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

To: European Data Protection Board

Vienna, 19.10. 2020

Subject: *noyb*'s comments on Guidelines 8/2020 on the targeting of social media users adopted on 2 September 2020 for public consultation

Dear Members of the EDPB,

noyb welcomes the opportunity to submit comments on the Guidelines 8/2020 published for consultation. We want to explicitly welcome the general approach the EDPB has taken in these guidelines and thank the members of the EDPB working groups for their work. We especially welcome:

- the clear position on the unlawful use of Article 6(1)(b) as a legal basis by some providers;
- the clear position that in most cases Article 6(1)(a) is the relevant legal basis;
- the clear position on the application of Article 9 when special categories of personal data are inferred or generated via the use of proxies and
- the highlight on the large footprint (from targeting of vulnerable groups to the use of micro-targeting for political manipulation) that GDPR violations in the area of social networks have.

In order to focus these submissions, we will, however, mainly concentrate on the elements that we feel may benefit from further input.

1. Pending Litigation

In the spirit of transparency, we want to highlight that *noyb* (or persons associated or supported by *noyb*) are currently engaged in litigation before the Irish DPC and before the Austrian Civil Courts that partly overlaps with issues raised in these Guidelines.

At the same time, we invite the EDPB to request the documents in the cases before the Austrian, Belgian, German and Irish DPAs (DPC Case numbers C-18-5-5, C-18-5-6 and C-18-5-7) to get first hand input on the legal arguments put forward by some Social Media Providers. We are equally happy to provide the relevant documents in the case 3 Cg 52/14k - 91 before the Vienna Regional Civil Court (LGfZRS), which partly overlaps with the subject matter of these guidelines.

In light of experience derived from these pending cases, we hope to add helpful practical points to the work of the EDPB.

Finally, for the avoidance of doubt and in light of arguments made in litigation in Ireland, Germany, Belgium and Austria, we want to mention that an omission to comment on individual parts of the Guidelines may not be interpreted as agreeance to these parts by *noyb*.

2. General Comments

2.1. Wording throughout the Guidelines

As a general matter and being fully aware of the delicate process of drafting EDPB Guidelines, we would encourage the EDPB to take even clearer positions on some issues in order to arrive at guidelines that go beyond the first red lines set by the recent CJEU judgements on Facebook.

This is especially in light of our experience that social media providers, in particular, have so far aggressively used even the slightest uncertainty in EDPB guidelines to depart from their obvious meaning. Lack of clear guidelines in practice opens the door to deliberate misinterpretation by controllers, which in turn leads to the abuse of data subject rights, to lengthy procedures before DPAs, or even costly litigation.

In this regard , we want to highlight that many *factual* descriptions in the Guidelines (like "*Personal data provided by social media users can be used by the social media provider…*" in § 37) will likely be used out of context by controllers to claim that the EDPB takes the view that these practices are actually *legal*. While some factual descriptions are clearly found to be illegal in other parts of the Guidelines, other practices are not further analysed, but merely described.

We therefore strongly encourage the EDPB to limit general factual descriptions of services and to use language that distinguishes between factual descriptions (of partly illegal practices) and the later legal analysis more clearly.

2.2. "Upstream" processing

While we are aware that this may be outside of the scope of the Guidelines, it seems striking that processing operations that take place before any "upstream" operations (i.e. processing operations for advertisement) are not mentioned in the Guidelines. This seems to be relevant in at least two aspects:

First, we wanted to draw attention to the fact that, under C-101/01 *Lindqvist*, users of social networks may themselves be controllers for the initial processing operations (such as public micro-blogging or their personal messages or emails). There is often no red line between consumers and active users of social media service and even private parties often run public pages on such platforms. In practice, the click of a button that makes others' data public or the mere intent to use a page for commercial purposes can make a user a "controller" as in *Lindqvist* or C-210/16 *Wirtschaftsakademie*.

Should the social media provider use data that it gathered as a processor (e.g. when Google provides Cloud Storage or Gmail) in violation of the instructions by the user, it would violate Articles 28 and 29 and other parts of the GDPR.

Second, Article 2(2)(c) GDPR and Recital 18 GDPR makes the, often unlimited, uploading, sharing and storing of personal data of others ("friends") legal, only if these activities fall under the household exception. Limitless further processing of such "privileged" data for commercial purposes would make the household exception a backdoor that would allow commercial actors to outsource data gathering to private persons. Recital 18 explicitly mentions that social media providers are (in relation to these processing operations) processors that fall under the GDPR, even if the user can make use of the household exception and therefore does not fall under the GDPR. Some controllers may interpret the factual description of this process in the Guidelines as an accepting of this practice as legal.

Third, the Guidelines mention, for example in §§ 9 and 18, that data is generated and shared for private ("household") purposes. As these are clearly not compatible purposes with the purpose of commercial data gathering for advertisements, this begs the question of whether a social media provider may simply engage in "secondary use" of such (often very personal and private data) under Article 6(4) GDPR. It seems to *noyb* that such a "secondary use" of personal data would for example require the consent of the data subject under Article 6(4) GDPR – in addition to the requirement for consent under Article 6(1) GDPR, which the Guidelines already discuss in detail.

While the EDPB may decide against including a legal analysis of these "upstream" processing operations as part of the Guidelines, we would strongly encourage to explicitly limit the Guidelines to processing operations from a certain point onwards and mention that the EDPB does at least not take a position on the legality of the described data gathering process.

The current factual descriptions in the Guidelines, according to which data is taken from many sources (be it maps, email services or chat apps) and further used, could be misinterpreted to mean that the EDPB agrees that the massive and global harvesting and aggregation of data on every individual (euphemistically called "social graph") is generally legal - independent of the purpose or controllership of the original processing operation.

2.3. Differentiation of "targeting mechanism"

In general, we consider that all data, whether inferred, observed or actively provided by the users, should be processed under the same conditions by the social media providers, in compliance with all relevant data protection laws. Whereas we see the interest of the distinction made by the EDPB in its guidelines for didactic purposes, such categories may not be that easy to delineate in the context of social media. For example, the Guidelines consider that the "like" button would constitute inferred data, whereas one could easily argue that this data is merely observed because the "like" button clearly indicates a preference actively provided by the user.

i) Transparency implications

The requirement for transparent and informed consent[1] relating to observed data and inferred data should be more clearly detailed. Users are not always aware that their personal data are collected even when they are merely, in their subjective opinion, "interacting" with the social media but not actively providing information to the social media or to a third party.

For example, "liking" a post of a friend or "friending" someone provides information to the social media, but, in the subjective view of many users, this might be providing information to the friend but

[1] See below on why consent under Article 6(1)(a) GDPR is usually the relevant legal basis. If the EDPB takes a different view, the same transparency considerations apply to Article 6(1)(f) GDPR.

not actively to the social media platform, unlike a user uploading their profile photo. Moreover, in such contexts, it can be difficult to prove that a social media provider actually processes observed or inferred data when there is a lack of information given by the social media provider and the targeters.

Therefore, it is crucial that the EDPB clarifies that any new categorization of data resulting from observation or inference, such as "*users interested in online betting*", "*people likely to be impulsive*", "*people likely to be betting heavily*" and "*people with lower income*", are made transparent and clear to the users. Without such transparency clarifications, the recommendations of the EDPB will remain a dead letter – any such categories will not be communicated to the users who will thus remain unaware of the various profiling types used by social media providers and targeters.

ii) <u>Data shared by other users</u>

Linked to the comment above, we want to highlight that when the Guidelines mention types of targeting mechanisms on page 12 and onwards, it seems they do not mention personal data that was provided by *other* users, like "friends" or even strangers to the user. Larger company groups (such as Facebook or Google) often aggregate data via the main service or a network of services and apps used by third party users. Typical examples are data uploads (e.g. data from phone books) or functionalities like free email accounts, which allow scanning of data from incoming emails by others. While it seems irrelevant for the later analysis of the Guidelines, this is another element where the clear limit in the scope of the Guidelines to "upstream" data gathering methods is unclear to us and could be addressed.

3. Roles of the different controllers

While we do not think that *noyb* is in the best position to comment on the sections of the Guidelines that refer to the different roles of controllers, it seems to us that the Guidelines seem to further stretch the concept joint controllership to situations that seem to be clearly separate operations. It is for example hardly understandable how an advertiser would be a "controller" for the delivery of an advertisement when this is wholly done by a social media platform.

We are aware that form an enforcement perspective, joint controllerships open many additional options for data subjects and DPAs, it seems in some parts more accurate to focus on the CJEU's concept of distinct "stages" (see §§ 70 and 72 in C-490/17 *Fashion ID*) and individual processing operations to get a clearer picture of the responsibilities. In practice, joint controllerships are extremely complex and hardly understandable for data subjects. We therefore fear that data subjects will be lost in a web of "responsibility shifting" exercises.

In this relation, we welcome the comments by the EDPB that in many cases the "joint controllers" are anything but equal partners. In previous experiences, large social media providers have simply unilaterally assigned rights and responsibilities on others. While the EDPB highlights in § 136 of the Guidelines that the DPAs are not bound by such declarations, it seems important to explicitly name these agreements as one-sided declarations that do not constitute these roles and rights. Consequently these declarations are not only non-binding on DPAs, but any outside party – including the data subjects, if they take the view that controllers misrepresent their actual roles in these documents.

4. Principles (Article 5)

We would like to further highlight that the Guidelines mention the principles in Article 5 GDPR throughout the document, but often do not apply them to each processing operation. As some examples, we would like to demonstrate this in the following cases:

4.1. Purpose Limitation (Article 5(1)(b))

As mentioned before, Paragraphs 9 and 18 of the Guidelines mention that personal data is shared by users for purposes other than advertisement. This begs the question of whether a large part of the originally collected data is not being used in violation of the purpose limitation principle.

> Practical Example:
>
> WhatsApp has dropped the €1 annual fee and instead uses the traffic and contact data from WhatsApp for advertisement on other services like Facebook or Instagram. To do so, WhatsApp scans the phone books of its users. The phone books include information about other data subjects (and which was likely collected without informing these data subjects that their data will be shared with third parties and maybe even without their consent) under the "household exception" for the purpose of private communication. The result is that a user may share his/her private phone number at a club with a date only to find out that his/her data ended up being used by Facebook for targeted advertising.

In a similar way, the Guidelines seem to lack an analysis of the purpose in the context of special categories of data in Paragraphs 106 to 121, especially when special categories of data are made public. When a person e.g. takes part in a demonstration (no matter if a "pro-life" demonstration or gay pride), this is done for the purpose of political engagement and under the umbrella of the freedom to free speech and the freedom to assembly. If such information were used for targeted advertising towards the user, there would be an obvious breach of purpose limitation.

It seems that including these elements would be helpful as a further strong line of reasoning to arrive at the conclusions in the Guidelines.

4.2. Data Minimization (Article 5(1)(c))

It is striking, moreover, that the Guidelines describe the vast amounts of data that social media harvests for the purpose of personalized advertisement, but lack a clear position on whether it would be proportionate to use all the available data for the mere purpose of advertisement.

In comparison to the example of WhatsApp metadata being used for Facebook advertisement above, the judgments by the CJEU on data retention come to mind. In these cases, the CJEU even found the use of such data for national security purposes to be disproportionate. While even the most remote information can theoretically be used to target advertisement, it seems clear that most data is neither "adequate", "relevant" nor "necessary" within the meaning of Article 5(1)(c) read in the light of the Charter. It seems problematic if the Guidelines describe these actions by the industry, without further analysis under the principle of data minimization.

While we understand that the Guidelines may be limited in scope, it again seems crucial to at least name these issues or explicitly limit the scope of the Guidelines to avoid the possibility of controllers misusing the Guidelines to legitimize their actions.

5. Legal Basis (Article 6 to 9)

5.1. General Remarks

While we believe that the elements below are not relevant for a strict legal analysis, it seems that the Guidelines are partly relying or at least describing certain elements that may need further context. We would therefore like to add some general remarks before an analysis under Article 6(1):

5.1.1. Business model of social media providers

The Guidelines state that "*as part of their business model, many social media providers offer targeting services*" (see §2). Some social media providers allege that targeted advertising and the processing of personal data is necessary in order to be able to provide their services for free.[2]

However, no evidence supports this conclusion: targeted advertising is possible without personal data. For example, targeting advertising can have the following forms:

- Geographical targeting (based on the first digits of an IP address);
- Language targeting (based on browser language);
- Contextual targeting (based on the content of the page);[3]
- Technical targeting (based on the terminal device, e.g. mobile/stationary);
- Time targeting (based on daily schedule or season).

It therefore seems problematic to mirror the broad-brush industry argument that there is only data driven "targeted advertisement" and not to differentiate between the many forms of targeted advertisement that have very different impacts on users' rights.

Moreover, according to the Guidelines, targeted advertising would lead to believe that the *"better the fit, the higher the reception rate (conversion) and thus the more effective the targeting campaign (return on investment)"* (see §2 of the Guidelines). Such a conclusion has already been challenged by recent studies, according to which targeted advertising was not much more profitable for publishers and advertisers. For instance, one estimate even suggested that the only increase in profit-targeted advertising brought was $0.00008 per advertisement.[4]

In any case, the business model chosen by social media providers – and even the mere aim of increasing profits from advertisement further – cannot be a relevant element under the GDPR to allege that the processing of personal data is necessary to provide a free service to the users, and therefore should not be permitted under the GDPR (see below).

We would therefore suggest rethinking such descriptions, which may be used by the industry to legitimize processing operations that are found to be unlawful in other parts of the Guidelines.

---

[2] See *e.g.* Snapchat Privacy Policy: *"Because most of our services are free, we also use some information about you to try and show you ads you'll find interesting"*; see Facebook Terms: *"Instead of paying to use Facebook and the other products and services we offer, by using the Facebook Products covered by these Terms you agree that we can show you ads that business and organizations pay us to promote on and off the Facebook Company Products. We use your personal data, such as information about your activity and interests, to show you ads that are more relevant to you"*.

[3] The search engine DuckDuckGo has been profitable since 2014 and earns more than $25 million annually using contextual advertising.

[4] See *e.g.* Veronica MAROTTA and others, *Online Tracking and Publishers' Revenues: An Empirical Analysis*, https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_38.pdf.

5.1.2. The determination of the service by the social media provider

While social media platforms are free to decide upon the functionalities of their services, this can self-evidently only happen within the limits of the law. Therefore, social media providers do not have total liberty to design their products and determine their business models. Implementing the GDPR at the design phase of a product or service is even an explicit requirement under Article 25 GDPR.

We welcome the fact that the EDPB makes a distinction between a social media service (provided to the users) and the provision of services such as targeting, based on the processing of data (provided to the targeters). That clarifies that one should reject the idea – supported by some social media providers – that "personalized ads" are also provided to the users as part of the service to them, leading to the inclusion of "targeting services" into their contractual terms with the users.[5]

This raises the fundamental question of the definition of a social service. According to the EDPB, the "key characteristics" of social media include the ability to register in order to create accounts or profiles, to interact with one another by sharing user-generated or other content, and to develop connections and networks with other users (see §1 of the Guidelines). We welcome this clarification from the EDPB.

The definition of the scope of the services provided to the users raises indeed two important questions:

- Some social media providers make it difficult to understand precisely what service they provide to users.[6] The terms and other contractual documents give the impression that they are either commercials for the service or at best a description of the how personal data are processed or recommendations for the use of personal data on the platform, rather than clauses or conditions about the service provided and the respective rights and obligations attached to it. Some social media providers simply do not describe the service provided to their users.[7]
- Some social media providers consider that the provision of advertising is part of the service to the users.[8] However, as already noted by the EDPB in the past, this goes beyond what is necessary to perform the contract (see below) and such reasoning is rightfully expressly rejected by the EDPB.

---

[5] See Facebook Terms: *"By using our Products, you agree that we can show you ads that we think will be relevant to you and your interests. We use your personal data to help determine which ads to show you."*

[6] See for example Instagram Terms of Use. Under the section "The Service we provide", one can find the following statements, describing vaguely the "service" provided: Offering personalized opportunities to create, connect, communicate, discover, and share; Fostering a positive, inclusive, and safe environment; Developing and using technologies that help us consistently serve our growing community; Ensuring a stable global infrastructure of our Service; Providing consistent and seamless experiences across other Facebook Company Products; Connecting you with brands, products, and services in ways you care about; Research and innovation.

[7] See Commission Des Clauses Abusives, Avis n°38 sur les conditions générales des sites de réseaux sociaux, p. 24 : *"Certains sites de réseaux sociaux ne définissent pas l'objet de leurs prestations de services. Bien que la plupart des utilisateurs savent parfaitement à quoi s'attendre, il est malgré tout indiqué d'expliquer à l'utilisateur ce qu'il peut précisément attendre du site internet (et ce que le site de réseau social d'autre part ne peut pas lui offrir)"* (available on https://economie.fgov.be/sites/default/files/Files/About-SPF/avis-cob-cca/Avis-38-Commission-Clauses-Abusives.pdf).

[8] See *e.g.* Instagram Terms of use: *"**Connecting you with brands, products, and services in ways you care about.** We use data from Instagram and other Facebook Company Products, as well as from third-party partners, to show you ads, offers, and other sponsored content that we believe will be meaningful to you. And we try to make that content as relevant as all your other experiences on Instagram".*

5.2. Concrete Legal Basis

We welcome the clarification from the EDPB according to which the processing for targeting purposes could take place primarily on the basis of consent and not in the form of an alleged "contract". At the same time, while theoretically possible, we have doubts as to the availability of "legitimate interests" in practical examples of processing on social media platforms.

5.2.1. The processing of personal data cannot be based on Article 6 (1)(b) GDPR

The EDPB already stated: *"For applicability of Article 6(1)(b), it is required that the processing is objectively necessary for a purpose that is integral to the delivery of that contractual service to the data subject"* (see EDPB Guidelines 2/2019, §30). As already mentioned, processing the data of the users to provide targeted advertising is not necessary to provide the social media service.

In this respect, we refer to the "economic necessity" alleged by the social media providers: such an argument also has to be rejected. Any business that derives profit from unlawful processing of personal data could otherwise make this "economic necessity" argument. Neither the GDPR, nor any other area of law or the economy, supports the "economic necessity" argument in order to make otherwise illegal business practice legal. In other words: an illegal practice does not become legal simply because it employs the person breaking the law.

Moreover, even if such *economic* necessity was proven, it should be not be confused with the *legal* necessity underlying Article 6(1)(b) GDPR.[9]

The EDPB already considered that, "*[a]s a general rule, behavioural advertising does not constitute a necessary element of online services. Normally, it would be hard to argue that the contract had not been performed because there were no behavioural ads. This is all the more supported by the fact that data subjects have the absolute rights under Article 21 to object to processing of their data for direct marketing purposes"* (Guidelines 2/2019, §47).

In the same vein, the mere reference by social media providers to the processing of data in their contractual terms (or privacy policy) cannot be sufficient to consider that the processing is necessary to perform the contract. Neither does the agreement to a processing operation under Article 6(1)(a) become a "contract" in the context of social media service, nor can processing without an objective link to the core contract be "necessary".

We therefore ask the EDPB to clarify that the mere inclusion of a consent clause in contractual terms or the privacy policy does not make such processing "*necessary for the performance of the contract*". Similarly, agreeing to a processing operation under Article 6(1)(a) does not result in a "contract" in the context of a social media service, and processing without an objective link to the core contract can also not be considered as "necessary".

[9] "*The processing must be necessary to perform the contract with this particular person. If the processing is instead necessary to maintain your business model more generally, or is included in your terms for other business purposes beyond delivering the contractual service, this lawful basis will not apply and you should consider another lawful basis, such as legitimate interests".* (see *Legal basis for processing* on the website of the ICO).

Practical Example:

Facebook Group has switched from consent under Article 6(1)(a) GDPR to an alleged "contract" as the main basis for all data processing under Article 6(1)(b) GDPR. This "contract" includes an alleged request by the data subject to have all personal data processed for many different purposes, including advertisement. This switch happened at the stroke of midnight on 25.5.2018 in an obvious attempt to bypass the protections of the GDPR on consent.[10] When we had 1.000 Austrian Facebook users questioned by the Gallup Institute, only 1.6% understood the relevant page to be such an alleged "contract" with the right to advertisement, while 64% interpreted it as (unlawful) consent. Others could not attribute any meaning to the page under Article 6(1) GDPR.[11]

The Gallup Study shows that Article 6(1)(b) must not only be rejected from a legal perspective, but that it is also rejected by about 98% of the users based on common sense. We hope that this position will also be embraced by all DPAs, as we have experienced that the Irish DPA has explicitly rejected the positions of the EDPB on this very issue in pending cases.[12]

The EDPB already confirmed that *"[m]erely referencing or mentioning data processing in a contract is not enough to bring the processing in question within the scope of Article 6(1)(b). Where a controller seeks to establish that the processing is based on the performance of a contract with the data subject, it is important to assess what is objectively necessary to perform the contract. This is also clear in light of Article 7(4), which makes a distinction between processing activities necessary for the performance of a contract, and terms making the service conditional on certain processing activities that are not in fact necessary for the performance of the contract. 'Necessary for performance' clearly requires something more than a contractual condition.* (see EDPB Guidelines 2/2019, § 27)*".*[13]

We therefore welcome the existing clarification in the Guidelines and ask the EDPB to further clarify that, where consent is requested in the context of a contract, such consent must be assessed on the basis of Article 6(1)(a), and not in light of Article 6(1)(b) GDPR.

5.2.2. Consent

The EDPB already stated in its Guidelines on consent that *"Article 7(4) seeks to ensure that the purpose of personal data processing is not disguised nor bundled with the provision of a contract of a service for which these personal data are not necessary"* (see EDPB Guidelines 5/2020, §3.1.2).

In practice this seems to be the only legal basis that would allow a controller to overcome other protections in the GDPR, such as:

(1) the purpose limitation principle, when data that was used for private communication is used for advertisement (see Article 5(1)(b) and Article 6(4) GDPR) or,

[10] Position of Facebook in litigation 3 Cg 52/14k - 91 before the Vienna Regional Civil Court and before the DPC.
[11] See https://noyb.eu/sites/default/files/2020-05/Gallup_Facebook_EN.pdf.
[12] See Letter to the EDPB of 25.5.2020, https://noyb.eu/sites/default/files/2020-05/Open%20Letter_noyb_GDPR.pdf.
[13] See EDPS Opinion 4/2017, p. 14: *"The fact that the purposes of the processing is covered by contractual clauses drafted by the supplier will not automatically mean that the processing is necessary for the performance of the contract"*; see also *Le contrat: dans quels cas fonder un traitement sur cette base légale ?* on the website of the CNIL : *"En pratique, la condition de nécessité s'apprécie concrètement au regard de l'objectif du contrat et des attentes mutuelles des parties quant à cet objectif. Elle n'est en revanche pas déterminée par la formalisation de ce contrat : le respect de cette condition ne doit pas être évalué au vu de ce qui est permis ou écrit dans le contrat proposé par le responsable du traitement".*

(2) situations where the user processes data as a controller (likely under the household exemption) and needs to "instruct" the processor to use such data under Article 29 GDPR.

We appreciate that the EDPB is consistent and restates in these Guidelines published for consultation that if consent is bundled up as a non-negotiable part of terms and conditions, it should be deemed to be not freely given (see § 51).

We also welcome the clarification made by the EDPB that, even if based on consent, the processing must always be proportionate and fair (see § 52). Indeed, the condition of proportionality is inherent to all processing operations, as enshrined in Article 5 GDPR.

5.2.3. Legitimate interest

We welcome that the Guidelines clarify that the data subject should always be given the opportunity to object to the processing of their data on the basis of legitimate interest. Such a possibility is not always given to the user prior to the use of their data for targeted advertising purposes. This must be possible on a case-by-case basis for each type of processing, as social media providers combine vast types of processing on one platform (spanning from micro-blogging to photo storage, email or even GDS tracking of another person). Currently most providers follow a "take it or leave it" approach and thereby undermine the free will and the informational self-determination of the users.

Regarding the three cumulative conditions to be met according to the *Fashion ID* decision of the CJEU (see § 44 of the Guidelines), we submit the following observations:

i) On the existence of a legitimate interest

The Guidelines could be read to mean that making the social media enterprise (more) profitable by using personal data to sell advertising space for a higher price is a legitimate interest.

As most private businesses are by definition striving to increase their profits, it seems hard to see how other controllers should not claim a "*legitimate interest*" in basically any form of squeezing the last cent out of personal data (no matter if consumers', employees' or competitors' personal data). To make the most profit from personal data is in itself <u>not</u> a legitimate interest – otherwise any struggling industry sector would have a "*legitimate interest*" to interfere with the right to personal data. There is nothing about social media companies, the advertisement industry or publishers that would give such a special status to these industry sectors.

ii) On the necessity to achieve the legitimate interest

Even where solely making a profit would be considered a legitimate interest and doing it via personalized advertising would be effective (see section above that personalised advertising is not more efficient than contextual advertising without processing personal data) this would not automatically make it "necessary":

As stated in the EDPB Guidelines (see § 47), it should be considered whether other less invasive means are available to meet the same end. For many sectors, such alternative means are clearly available.

Practical examples:

WhatsApp was profitable by charging € 1 per year, however Facebook now uses the service to gather even more data for its social networks. It cannot be claimed that it was "necessary" to transfer the meta-data of all communication to Facebook to make a profit, when it was clearly profitable by charging a tiny fee.

Equally, when a publisher gains an increase of $0.00008 per advertisement,[14] it can hardly be "necessary" to disclose the data of all visitors of a webpage to third parties to finance that webpage. Targeted advertising may be slightly more profitable than other forms of advertisement, but it is hardly "necessary" make a platform with a stable business model profitable.

We also draw attention to the assessment of the Article 29 Working Group, according to which the balance could not favour the controller where there are no alternatives to the service where no personal data are processed.[15] In such cases, consent would be the only appropriate legal basis.

We therefore submit that, in principle, targeted (personalised) advertising is not necessary to meet the interest of the social media platform (making the social media profitable), when other, more privacy friendly, means are available that can achieve the same objective of profitability.

iii) On the balancing test

Should the two prior requirements be met, one must still determine whether the legitimate interest at stake is overridden by the data subject's interests or fundamental rights and freedoms.

We welcome the statement of the EDPB in its Guidelines (see § 50) according to which intrusive profiling and tracking practices for marketing and advertising purposes would *a priori* not be permitted under such a balancing test.

At the same time, it seems that the extremely broad collection of personal data from countless sources and the combination of such data, as most social media providers do ("social graph"), is an exceptionally severe interference with the right to data protection and should be explicitly mentioned, for example, in § 48 of the Guidelines. This extreme interference with the right to data protection has to be contrasted with the rather trivial interest of improving targeted advertising.

In comparison to the CJEU judgments on data retention (with e.g. 6 months of meta data for national security purposes) it seems unthinkable that limitless collection of meta and content data for the purpose of "more targeted advertisement" could even be remotely considered as meeting the balancing test under Article 6(1)(f) GDPR or be "proportionate" in the light of Article 52 CFR.

Absent user consent (when the user is simply giving up the right to privacy and data protection) it seems unthinkable that Article 8 CFR would allow an interpretation of the GDPR that would lead to the result that (1) general and long-term gathering and central storage of personal data (2) from countless private and commercial sources (3) without the knowledge of the user for (4) the mere aim to slightly increase profits of a commercial actor (by selling more targeted advertisement) could be generally legitimized by the GDPR, without at the same time violating Article 8 of the Charter.

[14] See *e.g.* Veronica MAROTTA and others, *Online Tracking and Publishers' Revenues: An Empirical Analysis*, https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_38.pdf.

[15] See Opinion 6/2014 of the Article 29 Working Group on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, p.

iv) Transparency

However, even when legitimate interest is relied upon by the social media provider, the test is often not transparent: social media providers rarely mention which specific legitimate interests they pursue, despite the requirements of Articles 13 (1) (d) and 14 (2) (b) GDPR.[16] Under these circumstances, it is impossible for the data subject to assess whether, and how, the conditions mentioned above are met.

We therefore recommend that the Guidelines make clear that:

- merely increased profitability is not a legitimate interest.
- processing large amounts of personal data on users for the merely more targeted advertisement can – in the light of the CJEU judgements – never meet the balancing test under Article 6(1)(f) GDPR and Article 52 CFR.
- the legitimate interests envisaged by the social media providers as the legal basis for the processing of personal data in the context of targeted advertising is clearly and explicitly communicated to the users.[17]

6. Right to Access (Article 15)

noyb has (unfortunately) gained substantial experience in the lack of compliance with Article 15 GDPR by many platforms.[18] While we generally agree that online solutions ("tools") to access and correct personal data are in many cases the easiest and most practical solutions, we need to highlight that these tools are, in every case that we have so far analysed, deliberately complicated and wholly incompliant with the requirements of the GDPR.

> Practical examples:
>
> Facebook named up to ten tools[19] in ongoing litigation to provide access to different parts of the users' data. Facebook explicitly does not provide a stable copy of all personal data to the user. Users must "screenshot" or "print" the pages to get a stable copy according to Facebook.
>
> The "access" to ad targeting data was argued to be granted by having the user click on a button on each individual advertisement on Facebook the second it is shown. When doing so, however, the user was blocked for clicking too often after clicking on about ten advertisements in a row. Also, when an advertisement is not visible anymore, the user has no option to get access to the data.
>
> Facebook, Netflix and Google (among many other controllers) say that information under Article 15(1), (2) and (4) is granted by a link to their generic privacy policies, which say e.g. that data may be disclosed to others, without saying if, when and what data was *in fact* disclosed to whom.

[16] See *e.g.* Instagram and Facebook Data Policy: *"we collect, use and share the data that we have in the ways described above: […] as necessary for our (or others') legitimate interests, including our interests in providing an innovative, personalized, safe, and profitable service to our users and partners, unless those interests are overridden by your interests or fundamental rights and freedoms that require protection of personal data".*

[17] See Opinion 6/2014 of the Article 29 Working Group, section III.3.5.

[18] See e.g. https://noyb.eu/en/netflix-spotify-youtube-eight-strategic-complaints-filed-right-access.

[19] Facebook for example argues that users get access by combining the information in the (1) „Download your Information" tool, a separate (2) „Access your Information" tool, an additional (3) "Off Facebook Activity" tool, a supplementary (4) "Activity Log", the (5) "Control Center", the (6) "Why do I see this Advertisement?" function with each individual advertisement, a (7) "Privacy Check-Up", the (8) "About Facebook Advertisement" tool, the (9) "Advertisement Preferences" tool and (10) settings on the users' mobile devices – list taken from page 19 of Facebook's submissions in 3 Cg 52/14k from 1.9.2020.

As some of the most common problems that turn the right to access in a time-consuming hunt for partial access to the users' own personal data, we would like to highlight the following phenomena:

i) Mere access to the platform, not to personal data

There is a trend that social media platforms argue that mere access to the platform and some "tools" gives users "access" to the data, without ever providing an actual *copy* (a stable, reproducible and concentrated format) of personal data and without providing the data that is held in the background of the services. In our ongoing litigation in Austria, Facebook even argued that providing all personal data that is used for advertisement would be too complicated for users and is therefore not available. In practice this means that "tools" are often not even designed to provide all information and data under Article 15 GDPR.

Equally, as the data of third parties (that may neither have an account with the provider nor even have access to the internet) can be shared on social media platforms by other users, it follows that while online "tools" may be useful for many standard settings, they cannot be the sole form of access to data on social media.

ii) Reference to the privacy policy

In addition, instead of providing accurate data under Articles 15(1), (2) and (4) GDPR, controllers refer to the generic privacy policy that was written "ex-ante" under Article 13 or 14 GDPR.

A privacy policy however only reflects the planned processing that was drawn up in the office of a lawyer. The lack of any real-life "ex-post" information which data was actually processed in an individual case, makes it impossible to verify whether the controller has complied with its plans from the privacy policy or indeed with the GDPR. Referring to a privacy policy inherently blocks data subjects from exercising their rights, as they are only informed about processing "as planned" and not "as in reality".

iii) Lack of relationships between data and additional information

This comes in combination with the lack of links between the actual data categories, the purposes for which data was processed, the storage period for them or the legal basis that the controller has used for each processing operation. In the end, data subjects are only informed that *any* data may have been use for *any* purpose, for *any* time and on *any* of the named legal bases.

Referring to a privacy policy may be accurate in many "smaller" processing operations, like when a newsletter was factually sent as described in the privacy policy and the question does not arise which data was used under which legal basis for what purpose. However, it is inherent in social media platforms that the countless option for users and providers to use these platforms lead to different processing for each data subject. This must be reflected when answering access requests.

We therefore call on the EDPB to highlight that increased complexity and ever-larger data flows, require increased transparency and accuracy – not more generic information by social media platforms. This includes individualized, ex-post information as to the actual processing, as well as a clear link between the elements in Article 15(1), (2) and (4) GDPR to allow a data subject to determine what data was used for what purpose. To comply with the requirement of a "copy" in Article 15(3) and the requirements of Article 12 GDPR, an access tool must offer a centralized, stable and reproducible download.

7. Automated decision-making

We welcome the reference to Article 22 GDPR in cases where the automated decision-making would have a significant impact on the data subjects.

However, we consider that the example of the profiling used to target "*users interested in betting and likely to be betting heavily*" in Example 8 of the Guidelines is applicable to many more instances where profiling takes place for targeted (personalised) advertising. Advertisement is by its very nature meant to manipulate the decision process of the recipient (to e.g. buy a product or vote for another political party). The fact that it is a massive industry shows that it is often enough effective.

The criteria referred to by the Guidelines (see § 80) are indeed applicable to many more situations of targeted advertising (and not only to the one of a low income person likely to bet online, and not only based on inferred data):

- the intrusiveness of the profiling process is always high in the context of social media targeted advertising, considering the resources, the powerful tools, and amount of highly personal data used to create profiles on the user and his soundings that are then used to target different messages to each individual. In analogue terms, collecting such information would require multiple private investigators to sift through the daily life, friends and private communication of a user;
- individuals usually do not expect to be profiled on the basis of data that they were not even aware that someone was collecting, and they are unaware of the immense capabilities and potential consequences of profiling (e.g. as evidenced by the Cambridge Analytica scandal);
- the way the advertising is delivered in always intrusive, since ads typically appear directly as a type of content on the page of the user or on multiple third party pages, at the time which is selected by the targeter, to a specific profile, and with a direct link to the product or service;
- social media providers and targeters are in the best position to nudge users to engage with the advertised product or service, knowing their preferences and their shopping habits, and which users are more impulsive than others.

Therefore, the conclusion reached in the context of Example 8 in the Guidelines should be extended to many other situations where targeted advertising is performed. For example, many providers permit the targeting of people that are likely to buy products (in other terms: impulsive persons). Thereby, targeters may decide to target shopping addicts who are already financially over extended and using consumer credit (such as credit cards or consumer loans) to finance their purchase.

For these reasons, we recommend that the EDPB confirms that automated decision-making in the context of targeted advertising will usually be subject to the condition of Article 22, and that automated decision-making and Article 22 is applicable to all situations where data are processed, whether on the basis of data actively provided, inferred data or observed data.