The Consumer Voice in Europe

BEUC'S COMMENTS ON THE EDPB'S GUIDELINES ON THE TARGETING OF SOCIAL MEDIA USERS

Contact: Ernani Cerasaro – Digital@beuc.eu

BUREAU EUROPÉEN DES UNIONS DE CONSOMMATEURS AISBL | DER EUROPÄISCHE VERBRAUCHERVERBAND
Rue d'Arlon 80, B-1040 Brussels • Tel. +32 (0)2 743 15 90 • www.twitter.com/beuc • www.beuc.eu
EC register for interest representatives: identification number 9505781573-45

Co-funded by the European Union

Ref: BEUC-X-2020-098 - 16/10/2020

Why matters to consumers

Social media plays a central role in the daily lives of consumers. Thanks to sophisticated algorithms and techniques that monitor and analyse how consumers use their services social media companies can create detailed profiles of consumers. These profiles are then used to offer products and services to consumers and target them with specific information and content based on their declared, observed or inferred commercial, political, or other interests. Having such intimate knowledge of consumers' preferences endangers their privacy and data protection right as well as their autonomy and freedom of choice. This can also have serious consequences for society at large. The information collected can be used to exploit consumers' vulnerabilities and unduly influence their choices and behaviour, for example by targeting sports betting ads towards people struggling with gambling addictions. It is necessary to ensure that social media companies respect the GDPR and do not use consumers' personal data in ways beyond their knowledge and control to target them and manipulate their behaviour.

An encouraging approach by the EDPB

BEUC welcomes and supports the guidelines of the European Data Protection Board (EDPB) and the efforts made by the Board to clarify key aspects for a respectful and legitimate use of consumers' personal data by social media platforms and targeters[1].

We consider that the Board provides a good general overview of the subject and the issues at stake. In particular, we welcome that the Board highlights that targeting criteria are not only developed through processing of personal data which has been proactively shared or provided by data subjects, but increasingly through the processing of personal data observed or inferred, either by the social media provider or by third parties, and collected/ aggregated by the platform or by other actors (e.g. data brokers) for purposes such as ad targeting. In this sense, BEUC supports the structure of the guidelines dividing the different processing activities (and related targeting) on the basis of the type of data collected (data provided by the user, observed or inferred). The Board has also rightfully clarified some roles and responsibilities in the complex ecosystem of the so-called 'AdTech' industry.

In addition to expressing our general support to the guidelines, BEUC wishes to comment on a series of points. We hope our comments will be of help and will be taken into consideration by the Board in view of the adoption of the final version of the guidelines.

Roles - Joint controllership

Although BEUC understands the need to tackle the specific issue of targeting of data subjects in the context of social media platforms, we are concerned that by focusing only on such platforms, the EDPB loses the opportunity to tackle the broader issue of profiling in the AdTech industry. What happens through and on social media platforms is only one example in the broader context of online targeting of consumers. In fact, the Board analyses the scenario where only two joint controllers (the platform and the advertiser/targeter) take part in the processing activities.

[1] The guidelines use the term 'targeter' to designate natural or legal persons that use social media services in order to direct specific messages at a set of social media users on the basis of specific parameters or criteria.

However, when it comes to the AdTech industry there will often be many joint controllers, as data is usually shared with other third and fourth parties. The "Out of Control" report, published earlier this year by the Norwegian Consumer Council, illustrates how popular social media apps are sharing personal data with numerous third parties, which operate as "data brokers" and have a business model based on the commercial surveillance of consumers. In this sense, the example number 3 of the guidelines is easily solved because there are only two controllers. But how would the sharing of responsibilities work in presence of many third/fourth parties downstream processing the personal data of the data subject? We hope that the Board will clarify this in the future.

Legal basis

Consent and legitimate interest are both described as a possible legal basis for processing the personal data of social media users. The Board also recalls that no specific hierarchy is made between the two different legal basis and that the controller needs to ensure that the selected legal basis matches the objective and context of the processing operation in question. Two considerations arise:

1. We recognise that it is not easy to obtain a specific, informed and unambiguous consent in the digital environment. As a result, when using consent as a legal basis in the context of targeting of social media users, consumers' personal data is systematically hoovered up and exploited. As also shown in the 'Out of Control' report by our Norwegian member, the extent of tracking often makes it impossible for consumers to make informed choices about how their personal data is collected, shared and used. More specifically, the way the ad-tech industry currently operates largely does not seem to meet the stringent requirements to allow for the obtention of valid consent as set forth in the GDPR. The system is therefore deprived of any meaningful individual choice and transparency, and personal data is transmitted to an enormous number of actors all operating with their own privacy policies. In this sense, we support the EDPB opinion that consent can only be an appropriate legal basis if a data subject is offered control and genuine choice. If consent is bundled up as a non-negotiable part of terms and conditions, it is presumed not to have been freely given.

2. Controllers can only rely on legitimate interests provided that all the safeguards are met. We stress that legitimate interest as a legal basis is subject to the strict and cumulative requirements individuated by the CJEU and well summarised by the Board in par. 44-50.

It is clear that both consent and legitimate interest have to pass through a strict and complex scrutiny before being lawfully used in the context of the targeting of data subjects on social media.

BEUC would welcome more clarity and nuance in relation to the identification of the appropriate legal basis in specific contexts and circumstances. Normally, consent should be the appropriate legal basis for processing personal data for the purpose of targeting social media users, given the impact that targeting practices can have on their fundamental rights and freedoms. In this sense, it must also be underlined that legitimate interests cannot be regarded as a fallback option in those cases where valid consent is simply difficult or impossible to obtain. As indicated by the Board in its Guidelines 05/2020, consent is the

appropriate legal base when the controller "wishes to engage in a processing operation that would be unlawful without the data subject's consent".

In order to provide clearer guidance, the Board could add examples showing where one legal basis is to be preferred to the other. For instance, clarifying what would be the appropriate legal basis in example 1 of the draft guidelines.

Additional comments

Targeting of children - Par. 15
In this paragraph the Board rightly recalls that pursuant to art. 38 of the GDPR specific protection should apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child.

The Board, however, does not explore this issue further. The Board had already endorsed that "organisations should, in general, refrain from profiling them for marketing purposes"[2]. Also the WP29 opinion on apps on smart devices[3] had stated that "data controllers should not process children's data for behavioural advertising purposes, neither directly nor indirectly, since this will be outside of the scope of the child's understanding and therefore exceed the boundaries of lawful processing". We think that it is of outmost importance that the Board provides more detail about what are the specific protections that should apply in the context of targeting of children. In particular, it is our opinion that, in light of the fairness principle, the processing of personal data to target children for marketing purposes should be considered unfair in principle and thus forbidden.

'Users' vs 'data subjects' - Par. 19
We would recommend reconsidering the use of the term '**user**'. This is a term which is only used in the context of social media platforms. We would suggest using 'data subjects'.

Exclusion of other actors - Par. 29
The exclusion of '**other actors**' such as data brokers minimise the impact of the guidelines (see point on joint controllership).

Right to object when data is inferred - Par. 45

"Data subjects should be given the opportunity to object to the processing of their data for targeted purposes before the processing is initiated". It would be good if the Board could clarify how this right to object can be exercised in practice when the processing is based on inferred data that the controller collects without the data subject knowing precisely what data is processed.

'Vulnerable people' - Par. 99
The Board refers to '**vulnerable people**'. We would highlight that microtargeting can make anyone vulnerable.

Purpose limitation when data is made public - Par. 113
It would be valuable if the Board could further explore and explain how purpose limitation applies in practice when "**manifestly making personal data public"**.

[2] WP29 Opinion Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, page 29.
[3] Adopted on 27 February 2013, page 26.

Inferred special categories of data - Par. 116 and 118

We strongly support the interpretation of the Board that inferred data can be "special category data" even if the inference is wrong. This is of particular importance as data controllers often – inaccurately – argue that inferred data is not "special category data".

-END-

This publication is part of an activity which has received funding under an operating grant from the European Union's Consumer Programme (2014-2020).