19 October 2020

EBF_042950

EBF response to the European Data Protection Board's consultation on the Guidelines 8/2020 on the targeting of social media users

Key points:

- The European Banking Federation (EBF) welcomes the opportunity to provide a response to the European Data Protection Board's consultation on the draft guidelines on the targeting of social media users.
- While we understand the risks identified by the EDPB, the current approach in the guidelines, which appears to make joint-controllership the default situation between Targeters and Social Media Providers, does not take into **consideration that the GDPR already contains all the guarantees that allow this type of processing to be properly managed**, **without it being necessary to establish a regime of co-responsibility** in this domain.
- We caution against extending the conclusions of the two specific CJEU cases the draft guidance refers to - Wirtschaftsakademie and FashionID –**to all situations of commercial activity that involves the processing of the data of the users of social networks in order to offer them products or services from third parties**. When these two cases do not apply, **the Targeter and the social media provider will often be independent controllers**, though this will vary according to the fact. This, and the parties' respective responsibilities, need to be assessed on a case by case basis.
- We recognise that all controllers need to adhere to the accountability principle. However, the final Guidance should place more emphasis **on ensuring that social media providers meet GDPR standards, as the entities with the greatest influence over the means and purpose of processing**, and the more direct relationship with the recipients of marketing material, rather than placing the responsibility on targetters.

EBF position:

The European Banking Federation (EBF) welcomes the European Data Protection Board (hereafter 'EDPB') draft guidelines on the targeting of social media users. You will find below some general and technical comments on the draft Guidelines.

European Banking Federation aisbl

Brussels / Avenue des Arts 56, 1000 Brussels, Belgium / +32 2 508 3711 / info@ebf.eu
Frankfurt / Weißfrauenstraße 12-16, 60311 Frankfurt, Germany
EU Transparency Register / ID number: 4722660838-23

www.ebf.eu

1. Introduction

Overall, we observe that in the draft Guidelines, joint-controllership appears to be the default situation for the relationship between the Targeter and the Social Media Provider. The two judgements of the Court of Justice of the European Union (CJEU) in Wirtschaftsakademie and FashionID[1] are in particular used to present and support this approach.

While we understand the risks identified by the EDPB, we think the current approach does not take into **consideration that the GDPR already contains all the guarantees that allow this type of processing to be properly managed**, **without it being necessary to establish a regime of co-responsibility** in this domain. Where a bank engages a Social Media Provider to promote its products, **each entity takes specific actions and engages in specific data processing, which bring specific responsibilities**. It would **add complexity without improving protection for individuals that the two controllers should be jointly responsible for the entirety of the processing, rather than each being responsible for its own decisions and processing.**

It is important to highlight that the Court of Justice **has limited co-responsibility to two very specific cases.[2] The conclusions should not, by default, apply to all situations of commercial activity that involve the processing of the data of the users of social networks in order to offer them products or services from third parties.** When these two cases do not apply, the **Targeter and the Social Media Provider will often be independent controllers, though this will vary according to the fact. This, and the parties' respective responsibilities, need to be assessed on a case by case basis.**

In our view it would be disproportionate for a beneficiary of the social media advertising to be always considered co-responsible, as the Social Media Provider is primarily responsible to define the purpose of the processing of the personal data of its users (e.g. obtaining consent for marketing communications from banking institutions). **This points to an issue we flag several times in our response – the imbalance regarding the negotiating power of the Targeters on one hand, and the Social Media Providers on the other.**

Regarding the scope, while the draft Guidance does mention data brokers very briefly in paragraphs 26 and 27, these actors participate heavily in this advertising ecosystem and we would welcome an explanation of why their role is not examined further.

Finally, we would also like to note that a six week timeframe for consultation on these draft Guidelines, together with the consultation on the draft Guidelines on the notion of controller and processor under the GDPR is very limited, and we would encourage the EDPB to consider longer consultation periods in the future.

[1] CJEU, Judgment in *Wirtschaftsakademie*, 5 June 2018, C-210/16, ECLI:EU:C:2018:388; CJEU, Judgment in *Fashion ID*, 29 July 2019, C-40/17,
[2] ibid

2. Actors and roles (Section 4)

4.5 Roles and responsibilities

Paragraph 34 notes that "*In case of joint controllership, pursuant to Article 26(1) GDPR, controllers* ***are required to put in place an arrangement which, in a transparent manner, determines their respective responsibilities*** *for compliance with the GDPR…"* In practice, social media providers often seek to apply standard contracts on a "take it or leave it" basis which, for example, provide limited control of onward processing or provide little or no right of recourse for damages sustained/liability incurred as a result of breaches or failures by the social media companies. This imbalance between the Targeter and the Social Media Provider is important to note and we welcome that this is discussed in section 9.2 of the Guidance. However, we recommend to also mention it in this section, perhaps by referring readers down to section 9.2. **as, in the view of EBF members, this is a key point to make up front (see also further comments below).**

We recognise that all controllers need to adhere to the accountability principle. **However, the guidance should place more emphasis on ensuring that social media providers meet GDPR standards, as the entities with the greatest influence over the means and purpose of processing, and the more direct relationship with the recipients of marketing material, rather than placing the responsibility on targetters**. The guidance should emphasise that social media platforms must provide adequate information to targetters to demonstrate they meet GDPR standards.

3. Analysis of Different Targeting Mechanisms (Section 5)

5.2.1 Targeting on the basis of provided data

Regarding the paragraphs on respective roles (38-42), even if the Social Media Provider and the Targeter have joint responsibility**, it should be acknowledged that the Targeter will in practice have to rely on the Social Media Provider for some elements of ensuring that there is a valid legal basis for processing**. **The Guidance should make clear that Social Media Providers have a key responsibility in this regard, which should be recognized in contracts with Targeters.**

Paragraph 45 (p.15) reads that "*Users of social media should not only be provided with the possibility to object to the display of targeted advertising when accessing the platform, but also be provided with controls that ensure the underlying processing of his or her personal data for the targeting purpose no longer* ***takes place after he or she has objected***." Targetters will never have the required insight to assess whether subjects have objected via social media opt-out controls. If an objection is received from its customers or users with the Social Media Provider, an opt-out solution should be provided on the targetter's side for direct marketing purposes (e.g. for compiling list-based or custom audiences) and the Social Media Provider should provide opt-out solutions for its users on the social media platform. In practice **targetters will have to rely on Social Media Providers removing data subjects that have objected prior to any campaign via the Social Media Provider's platform.**

In Paragraph 49 (p.16), the text notes that *"The Targeter seeking to rely on legitimate interest should, for its part, make it easy for individuals* ***to express a prior objection to its use of social media for targeting purposes.*** *However, insofar as the Targeter does not have any direct interaction with the data subject, the Targeter should at least ensure that the social media platform provide the data subject with means to efficiently express their right to prior objection."* Building on the comments made above, this seems to place the responsibility for Social Media Platform compliance on to Targetters. We accept that Targetters need to meet their obligations, including the accountability principle, **but the guidance should emphasise in the first instance that Social Media Platforms have an obligation to provide effective opt-out tools.**

Furthermore, Paragraph 49 also notes that *"**As joint controllers, the Targeter and Social Media Provider should clarify how the individuals' right to object** (as well as other rights) will be accommodated in the context of the joint arrangement (see section 6)."* This is an area where the Targeter is likely to have to rely on the Social Media Provider in practice. Although social media providers should explain to the targetter how it will enable data subjects' rights, the targetter will in practice not be able to control how objections are managed by the social media provider.

5.2.2. Data provided by the user of the social media platform to the Targeter

Regarding the Example under paragraph 54, members are concerned that, as it is currently worded, the Guidance seems to imply that banks only would like to target, with no regard for legislation. We would therefore recommend the following amendments:

> The bank **may consider** ~~**has nevertheless**~~ adde~~d~~ **ing** the e-mail address of Ms. Jones to **one of** its customer e-mail database**s**. **Since Ms. Jones showed interest in one of the products of the bank, Ms. Jones would be considered as a prospect for other banking products. E-mail addresses in this database are provided to the social media provider** ~~**Then, the bank uses its e-mail database, by allowing the social media provider**~~ to 'matching' the list of e-mail addresses it holds with those held by the social media platform, in order to target the individuals concerned with the full range of financial services on the social media platform.

Regarding paragraph 60 (p.18), we would recommend the Guidelines to expand on how Example 3 (p.17) would meet the Legitimate Interest Assessment test. The disclosure of the email address of the client can be based on legitimate interest if the client has been duly informed about it. Articles 13 and 14 GDPR help contribute to ensuring what happens with the data and that the client knows what his or her rights are (transparency). We fail to see the GDPR reasoning of EDPD that sustains the following statement: *"However, the mere fulfilment of information duties according to Article 13, 14 GDPR is not a transparency measure to be taken into consideration for the weighing of interests according to Article6(1)(f).of GDPR."* Is the intended meaning that provision of transparency information required under Articles 13 and 14 is not necessarily sufficient to ensure that the balancing of interests is satisfied?

5.4 Targeter's lawful basis for targeting on the basis of inferred data

Further clarity needs to be provided on Example 7 (p.22) as to how the Targeter could obtain consent for advertising on the basis of inferred data. In this example, the Targeter utilises targeting criteria offered by the Social Media Provider to display ads to users. The social media provider may obtain consent to the processing of users' data in order to display targeted advertising (including use of technologies that record information about users' online behaviour and for profiling using that information). The Targeter does not have a direct relationship with the users and so no opportunity to seek consent from the users. Paragraphs 68 and 69 indicate that consent for targeted advertising may be obtained by one joint controller (i.e. the social media provider) and relied on by multiple joint controllers, but all joint controllers seeking to rely on the consent must be named. **It would be impossible for the social media provider to specifically list all entities that might use its targeting criteria, nor would it be possible for a user to review and comprehend a list of hundreds of potential advertisers.** An indication of product categories could be sufficient.

The EDPB indicates that joint controllers, whenever possible, should rely on the same lawful basis for using a particular targeting tool and for a particular purpose. The key rationale for this is to enable data subjects to easily exercise their rights (paragraph 126). **However, data subjects' rights would be no less protected if the Targeter's lawful basis for targeting on the basis of inferred data was its legitimate interests and the social media provider's lawful basis was consent**. The Targeter could not provide transparency to a user directly but the parties could agree in the joint controller arrangement that the social media provider would be responsible for providing transparency. The Targeter would still have an obligation to ensure this transparency was sufficient, setting out appropriately the categories of data recipients, for example. The draft Guidance seems supportive of this division of responsibilities at section 9.1.

It would be helpful for this section of the guidance to clarify that legitimate interests can be an appropriate basis for processing for Targeters, subject to appropriate safeguards, even where the social media provider relies on (or must rely on) consent.

Lawful bases of Targeter and social media provider for 'lookalike advertising'

For completeness, it would be helpful if the guidance also addressed the very common practice of 'lookalike advertising', for example, where a Targeter provides a list of customers' email addresses to a social media provider and instructs the social media provider to target its customers (as in example 3) and to also target users who resemble the Targeter's customers. Targeting for lookalike advertising may be on the basis of data provided to the social media provider as well as observed/inferred data and will necessarily involve profiling. The social media provider and Targeter would have to assess whether they are independent or joint controllers in this case and determine the respective responsibilities accordingly. Provided sufficient transparency and an opportunity to object is provided to customers, it seems that the Targeter and social media provider may be able to rely on the lawful basis of legitimate interests for processing customers' data in

order to create a lookalike audience (as for targeting on the basis of provided data, see paragraph 45).

As to processing of data of the lookalike audience, it seems that the social media provider's lawful basis for processing data of the lookalike audience must be consent. It would be difficult for the Targeter to rely on that consent for the reasons identified above in relation to targeting on the basis of inferred data. As above, this problem would be solved with no downgrading of data subjects' rights if the Targeter could rely on legitimate interests for this processing.

3. Transparency and right of access (Section 6)

Essence of the arrangement and information to provide (Article 26(2) GDPR)

In paragraph 88 (p.25-26), the draft Guidelines note that "*In case one of the joint controllers does not have all information in detail because, for example, it does not know the exact technical execution of the processing activities, the other joint controller shall provide all necessary information…*" It would be useful for the Guidelines to acknowledge here that firms will need to be careful about not disclosing commercially sensitive information.

4. Data Protection Impact Assessments (DPIA) (Section 7)

In paragraph 101 (p.28), on fulfilling the DPIA, the draft Guidance writes that "*In this context, both controllers need to ensure that they have a sufficient level of information on the processing to carry out the required DPIA. This implies that* "***each data controller should express his needs and share useful information*** *without either compromising secrets (e.g.: protection of trade secrets, intellectual property, confidential business information) or disclosing vulnerabilities*". Depending on the nature of the processing**, it would not necessarily be proportionate for a full DPIA to be done before each marketing campaign by the targetter. It would be helpful for the guidance to mention that a DPIA could cover marketing in general, provided this is kept up to date**. It would also be helpful to make explicit that – where possible – generic information from the social media provider can be used, rather than requiring a bespoke disclosure for each marketing campaign.

5. Special categories of data (Section 8)

Inferred and combined special categories of data (SCPD)

We would recommend to further develop the examples provided in this section so as to illustrate more explicitly **that controllers can process large amounts of data from which inferences could in *theory* be drawn, but that this will not always imply SCPD are being processed.** It would therefore be helpful to have one example that illustrates specifically where SCPD are not being processed, despite large amounts of data being processed, and one where SCPD are considered to be processed, due to the intent of the Controller / the nature of the processing. We would also like to note that, in relation

to the recently closed consultation on the EDPB's draft guidance on the interplay between the GDPR and PSD2, that paragraph 117 takes a more pragmatic approach to SCPD than the former. **The greater emphasis on the controller's intentions in the social media guidance is welcome and should be reflected in the PSD2 guidance.**

More specifically, in paragraph 107 (p.29), the draft Guidance states that the processing of special categories of personal data "*must also rely on a legal basis laid down in Article 6*"; this in addition to the conditions provided in Article 9 (2). To ground the processing on both legal basis of Article 6 and 9[3] GDPR may be very burdensome for the data controller and it may also cause confusion and uncertainty on which legal ground the processing is based, infringing, as a consequence, the fundamental principles set forth in Article 5 GDPR[4].

Finally, regarding the structure of this section, we would recommend to place Example 12 (p.31) after paragraph 117 (p.31), as it does not seem to relate to paragraph 116 (p.31).

The Article 9(2) exception of special categories of data made manifestly public

Example 15 (p.33), as it is currently worded, is quite vague. We would therefore recommend amending the text by, for example, saying that "whilst Mr Jansen has included the information about his sexuality in his profile, he has not included it in any messages he has shared publicly."

6. Joint controllership and responsibility (Section 9)

Overall, members are of the view that **there is not necessarily a standard joint determination of the purposes and means of processing in Targetter-Social Media Provider relationships.** As set out above, and in our response to the draft guidance on the concepts of controller and processor, **this will depend on the details of each case, the situations covered in the two CJEU cases should not be assumed to be always applicable.**

If and when joint control of the data processing is established **it could be proposed to attach a joint data control agreement template to the Guidelines which could help to match the uneven balance between Marketers and Social Media Providers and set out the desired requirements in the joint data processing relationship**

[3] We note that grounding the processing on both legal basis (Articles 6 and 9), based on their national DPAs, is the approach taken in some jurisdictions.

[4] In addition, the statement of paragraph 107 is in conflict with the EDPB guidelines on Consent, where the former WP29 states that "the controller cannot swap between lawful bases. For example, it is not allowed to retrospectively utilise the legitimate interest basis in order to justify processing, where problems have been encountered with the validity of consent" (see Guidelines on Consent, paragraph 6). This principle is also recalled in the Guidelines 2/2019 on the processing of personal data under Art. 6(1)(b) GDPR in the context of the provision of online services to data subjects, where the EDPB confirms that, under the GDPR, it is not possible to swap from one lawful basis to another.

between Marketer and Social Media Providers. The use of this template would be voluntary.

It is also important to recognise the practicalities of the fact that, as the EDPB notes in paragraph 129, companies may be confronted with the need to adhere to pre-defined arrangements, with limited bargaining powers. **In situations where it is not possible to bargain or to gain access to further information on how the other party is going to process the data, we encourage the EDPB to make clear that the balance of responsibility and liability lies on the social media channel.**

Specifically on paragraph 125, including the example, (p.34), the EDPB seems to allocate more responsibility for compliance with the GDPR on the side of the Targeter than on the social media platform, who knows and has a relationship with the data subject, seeming to obviate the fact that the GDPR does not distinguish between data controllers. We encourage the guidance to emphasize that social media platforms must provide effective and sufficient information to the Targeter.

Finally, paragraph 128 (p.35) writes that *"If there is no clarity as to the manner in which the obligations are to be fulfilled, in particular in relation to data subject rights, **both the Targeter and the Social Media Provider** will be considered as acting in violation of Article 26(1) GDPR."* We would like to stress that responsibility is not split equally and reiterate that the social media provider needs to disclose enough information to the targetter to do effective due diligence.

ENDS

For more information:
Liga Semane
Policy Adviser – Data & Innovation
l.semane@ebf.eu

About the EBF

The European Banking Federation is the voice of the European banking sector, bringing together 32 national banking associations in Europe that together represent a significant majority of all banking assets in Europe, with 3,500 banks - large and small, wholesale and retail, local and international – while employing approximately two million people. EBF members represent banks that make available loans to the European economy in excess of €20 trillion and that reliably handle more than 400 million payment transactions per day. Launched in 1960, the EBF is committed to a single market for financial services in the European Union and to supporting policies that foster economic growth.

www.ebf.eu @EBFeu