Ecommerce Europe's contribution the EDPB Public Consultations - Comments to the Guidelines 8/2020 on the targeting of social media users

Introduction

Ecommerce Europe is the sole voice of the European Digital Commerce sector. It represents, via its 25 national associations, more than 100,000 companies selling goods and services online to consumers in Europe. Ecommerce Europe acts at European level to help legislators create a better framework for online merchants, so that their sales can grow further. We welcome the opportunity to provide our feedback to the recently published EDPB's Guidelines 8/2020 on the targeting of social media users.

General remarks

Within the e-commerce and online marketing environment, online retailers and social media platforms are two active performers. Following the outbreak of COVID-19 and the subsequent acceleration of digitalisation, a shift has taken place in which customer interactions have increasingly moved from an offline to an online environment. In that perspective, online advertising is essential for retail businesses to interact with consumers that no longer visit physical stores to the same extent as before. To be able to compete on a European and global market, the use of social media platforms is essential for online retail, as consumers increasingly find retail companies and their products/services via social media. Considering the above, the retail sector works very closely with social media platforms, especially when it comes to advertisement and the relationship with consumers. By using the targeting services and audience services offered by social media platforms, the retail sector can ensure that relevant advertisements and communication are presented to a customised target audience. In the view of Ecommerce Europe, it is important to understand the complete environment and the role of different parties within the supply chain involved in targeting social media users when developing guidelines on these subjects.

Given the importance of targeting for online and offline retailers, Ecommerce Europe welcomes the EDBP Guidelines 8/2020 on the targeting of social media users (hereafter referred to as "guidelines") and its efforts to clarify data protection issues related to the targeting on social media and the positive effect the guidelines will have on a common, uniform and harmonised interpretation of the GDPR within the Internal Market, thus stimulating cross-border trade.

Ecommerce Europe has identified great challenges for online retailers within the current online advertising and targeting environment. Clarifications on the role, responsibility and liability of each party involved in the processing of data within these services is therefore very much welcomed, especially in cases of joint-controllership, as is concluded by the EDPB for the relation between the targeting web shop and the targeting service provider.

However, it is important for Ecommerce Europe to emphasise that the advertising and targeting services offered by social media platforms and other actors like search engines, are offered to web shops and other retailers on a "take it or leave it" basis and that the factual influence of web shops on the targeting services offered by social media platforms and on the data processing that is conducted by them to offer these targeting services, is actually minimal or even completely absent. Most targeting services only allow web

shops to choose profiles they want to target, on the basis of categories and characters set and decided on solely by the targeting service provider. In that perspective, 'targeting online retailers' must be seen as customers of prefabricated products offered by social media services. Furthermore, targeting web shops do not have direct access to the personal data in the database of the targeting service and thus have no information on the identity of the data subjects included in the target audience of the targeting service provider. It is crucial to add that the majority of web shops using the targeting services of social media platforms are SMEs, while the targeting service providers are generally large companies with a substantial market power.

Although Ecommerce Europe acknowledges that the above facts cannot exempt online retail companies from their obligations under the GDPR, there is an imbalance in the relationship between the social media provider and the online retail company. In practice, the social media provider has the factual influence and decision-making power over its services and the way targeting is conducted, whereas SMEs and other online retailers often lack market power, knowledge, staff or resources, or are not able to influence or identify the main characteristics of the targeting service provided. In that perspective, online retailers, as users of a service that is unilaterally shaped and designed by the social media platforms, rely on the targeting service provider to shape the targeting process and the involvement of web shops in it. Moreover, as the Guidelines suggest, social media providers are "unavoidable trading partners" for targeters. The targeting service should provide relevant information to the targeting web shop as well as to the data subject and create balanced standard contracts (Article 26) to allow their clients to use their targeting services in a fair and GDPR compliant way. The responsibility and liability for the data processing should address the imbalance and be mainly allocated to the targeting service providers, which take the decisions on the goals and means of the processing, and only to a limited extent to the users of these services, which only have limited factual influence on the processing.

As we support fair competition and rules, the effect of market dominance of targeting service providers should also be taken into account by competition authorities when assessing potential unfair competition and abuse of market dominance by these providers in the field of targeting services.

In Ecommerce Europe's view, the above-mentioned reality must be duly reflected when determining the level of responsibility, and especially liability, between the parties in case of joint controllership.

Ecommerce Europe's five main messages for the EDPB:

1. When joint controllers do not have any or only minimal factual influence over the purpose and means of the data processing in targeting operations, they should not - or only to a limited extent - be held accountable for the joint data processing.[1] In that perspective, Ecommerce Europe would like to see more guidance from the EDPB on how these differences in factual influence and decision power affect the allocation of responsibility and liability.

2. As there is an unbalanced party relationship between the social media platforms and the targeting retailer, there is a great need for extra guidance on how these players should act when there are "take-it-or-leave-it" situations and online retailers are basically using a targeting service that was pre-set and shaped only by a targeting service provider.

[1] Guidelines 07/2020 on the concepts of controller and processor in the GDPR.

3. Supervision and assessment of GDPR compliance should basically be directed to the party that offers the targeting services and that has greater insights of and influence on these tracking operations, which would generally be the social media platform, thus assuring compliance in the most effective way of the online advertisement and tracking environment. Another issue related to enforcement is the fact that there are different interpretations of the guidelines and the legal framework by the national DPAs, as well as differences in means and resources national DPA's have. Ecommerce Europe would like to see better cooperation and coordination between the different Member States' DPAs, preferably in a harmonised and uniform way to secure the full potential of the Internal Market.

4. Ecommerce Europe believes that joint controllership should not lead to extra information obligations towards data subjects as they are already confronted with significant information obligations, which have led to information overkill and information fatigue. Joint controllership especially should not lead to double information obligations, and communication on the effects of joint controllership should preferably be possible in a layered and easily accessible way for the data subject. It also should be avoided that online retailers, as joint controller, have to inform data subjects about the targeting service provider's data processing that they do not have access to.

5. Ecommerce Europe believes that the examples in the guidance can be further improved to be more realistic and based on an assessment of the complexity of the targeting services that social media platforms offer to online and offline retailers.

Remarks on the Guidelines 8/2020 on the targeting of social media users

In this section you can find Ecommerce Europe's feedback on several paragraphs in the Guidelines.

❖ **Paragraph 5**

Although recent CJEU judgments state that the interactions between social media providers and other actors may give rise to joint controllership and joint responsibilities under EU data protection law, Ecommerce Europe is convinced that the protection of data subjects' rights is not strengthened by introducing joint controllership for targeting web shops. On the contrary, given the lack of factual influence and the lack of ability to exercise decision-making power, Ecommerce Europe strongly believes that controllership must primary be placed with the social media provider who solely determines how the targeting service is provided to advertisers, following the perspective that data subjects' rights will not be strengthened by creating a granular range of controllers with differing responsibilities for a data processing operation, where there is clearly only one controller that mainly decides on goals and means. In our view, this opinion is equally applicable to the Guidelines in paragraphs 19 and 20 of the EDPB's Guidelines 07/2020 on the concepts of controller and processor in the GDPR.

❖ **Paragraph 6**

As stated in this paragraph, the aim of these guidelines is to clarify the roles and responsibilities among the social media provider and the targeter. As such, Ecommerce Europe supports this aim, but wants to emphasise that the clarification of responsibilities among social media provider and targeter should also include the clarification on how to assess their respective share of responsibility and liability towards the data subject given the different level of influence on the shared data processing the involved parties have.

❖ **Paragraph 8**

In this paragraph, it is stated that "the mechanisms that can be used to target social media users, as well as the underlying processing activities that enable targeting, may pose significant risks". Ecommerce Europe wants to emphasise that the interpretation of what is considered a significant risk will differ between data subjects depending on *inter alia* their knowledge of the service, personal interests and their willingness to understand the services they use. Moreover, in practice, the younger generation of data subjects shows a more positive attitude towards data sharing. They have a greater understanding of the benefits directly linked to such data sharing and generally do not consider it as a significant risk. In that perspective, significant risk as such has to be assessed on a case-by-case base, taking into account the context of the specific targeting service, and it should be interpreted in a uniform way. In Ecommerce Europe's view, the guidelines should therefore clarify that social media targeting operations as such cannot *per se* be considered as posing a significant risk.

❖ **Paragraph 9**

In this paragraph, the guidelines define as one of risks to the rights and freedoms of users posed by the processing of personal data, that "targeting of social media users may involve uses of personal data that go beyond individuals' reasonable expectations and thereby infringes applicable data protection principles and rules. For example where a social media platform combines personal data from third-party sources with data disclosed by the users of its platform" which may result in personal data used beyond their initial purpose and in ways the data could not reasonably anticipate. Moreover, according to the guidelines, a lack of transparency regarding the role of the different actors and the processing operations involved may undermine, complicate or hinder the exercise of data subject rights.

Ecommerce Europe again wants to emphasise that the data subjects' reasonable expectations may vary depending on, *inter alia*, their age, sex, what website the data subject is operating on or whether he is a member of a company's loyalty program. The data subjects' reasonable expectations are also affected by the information about the processing of his personal data which is provided to the data subject (e.g. for a registration process to a loyalty program or a user account). In that perspective, it should be clarified that targeting as such is not *per se* considered as a risk to the rights and freedoms of users and that assessment of these risks should be done on a principle and case-by-case base, in the context of the specific targeting operation and taking into account the factual role of targeter and social media platform.

As regards to the lack of transparency regarding the role of the different actors in the targeting operation, Ecommerce Europe has a general concern that the extensive information requirements set out in various consumer protection legislation and GDPR has led to an information overload and information fatigue. This could cause consumers/data subjects to ignore their responsibility to actually read the information presented to them by the targeter or social media platform before engaging in social media services or online sales of services or goods. Although many retail companies invest large amounts in solutions to make the information more available and accessible to data subjects and to manage their reasonable expectations, it is a great challenge for retail companies to get data subjects to really and effectively take up the information that is provided in a compliant way. The lack of willingness to read the significant amount of obligatory information offered will naturally affect data subjects' perception of the data processing operations he will be subject to (i.e. targeted the advertisements) as a consequence of the use of the social media services or by engaging in an online sales. In that perspective, Ecommerce Europe welcomes further clarification and initiatives from the EDPB regarding information best practices, but also initiatives on how to educate data subjects concerning their responsibilities when using social media platforms and online services. Moreover, to avoid double information, we would welcome guidance on which joint controller,

given his decisive role in the specific targeting process, should be responsible for providing the relevant information about the targeting operation to the data subject concerned. This concerns in particular cases where social media platforms offer their targeting service on a "take it or leave it" base, with pre-set categories targeters can choose their custom target audience from and where online retailers have no factual influence or decision-making power on which data subjects will be included in the target audience.

❖ **Paragraphs 10, 11 and 12**

As regards to these paragraphs, Ecommerce Europe wants to emphasise that businesses in the online retail sector generally do not use social media services to specifically target vulnerable individuals nor do they engage in discrimination, exclusion or unduly political and electoral influencing of their customers. Although they do not have any intention to be non-compliant, online retailers generally have no insights into how and with which parameters or algorithms the social media platforms choose the targeted customer audience when entering into contract about targeted advertisement. Ecommerce Europe would therefore welcome clarifying guidelines on how to best protect vulnerable data subjects from targeting in an unethical manner, how to avoid discrimination and exclusion and what solutions need to be implemented in the services provided by social media platforms to ensure a level of data protection compliant with the GDPR.

❖ **Paragraph 13**

Ecommerce Europe wants to draw attention to the fact that especially in online commerce, data subjects may deliberately want to be exposed to "more of the same" information. For example, in online food supply, data subjects often appreciate that retailers predict their preferences and facilitate an individual grocery shopping experience based on their consumption profile. Moreover, Ecommerce Europe is convinced that the risk of unwanted filter bubbles within the retail sector is very low.

❖ **Paragraph 14**

Ecommerce Europe agrees with EDPB's statement that there is indeed a risk that individuals may feel that their behaviour is systematically being monitored when using online services. However, we strongly believe that this feeling can be reduced by educating the users on how the social media services work, how they can control access to their data (e.g. by using privacy tools in the social media service or by simply logging off from those social media platforms that systematically monitor their behaviour) when engaging in social media or when they are accepting targeting. In practice, most of the targeting practices are performed after the data subjects' acceptance of a service provider's terms of use or the data subjects' consent. Ecommerce Europe therefore believes there is, on the one hand, a need for education of data subjects on their rights and the consequences of their consent and, on the other hand, a need for effective enforcement guaranteeing GDPR compliant processing of their data by social media offering targeting services to third parties.

❖ **Paragraph 15**

Ecommerce Europe would like to point out that targeting children is not something that is common within the retail sector. However, at the same time, we notice that according to Member States' legal systems, minors are at considered capable to engage in legally binding contracts at different ages (e.g. at the age of 16) or that they are allowed to engage in legally binding contracts that are considered normal for their age (e.g. a 13 year old student buying a ticket for public transport to go to school). In the view of Ecommerce Europe, there should be no restrictions for minors that are legally capable to engage in online contracts in the same way as they are allowed to engage in offline contracts. It that perspective, targeted advertising, for instance on special deals and prices, can be very useful for them. It should therefore be carefully assessed what forms of targeted advertising are allowed for online retailers to minors. In the view of

Ecommerce Europe, the standards on advertising directed to minors and protection of minors as developed in offline retail should be the point of reference for online targeted advertising directed to minors.

❖ **Paragraph 18**

As regards to paragraph 18, Ecommerce Europe wants to emphasise that social media users that have an "account" or "profile" for the social media service often benefit from this registration (for instance loyalty members or very interactive members getting better deals and services). Also "paying with your data" for social media services is a more and more accepted concept (as for instance in the Directive (EU) 2019/770 on contract rules for the supply of digital content). In that perspective, the fact that individuals who did not register for the social media service will not be able to make use of all the features of the service like registered ones, should not be regarded as negative or discriminatory towards those individuals. Consequently, it should be regarded as normal practice, that individuals who decided to share data or to "pay" with their data should also get an advantage from doing this.

❖ **Paragraphs 22, 32 and 33**

Ecommerce Europe underlines the conclusion that in the relation between targeter and social media platform, it is generally the social media provider that has the opportunity to gather large amounts of data and to use it to offer standard targeting services to online retailers. It is especially important to consider that a targeter never has direct access to the personal data of the users of social media services. When using the social media services, the targeter has the opportunity to customise the target audience. However, this entails choosing from categories prefixed by the targeting service provider, the targeter has no factual influence and cannot exercise any decision-making power over the data processing other than the collection of personal data from the social media service and transfer of personal data to the social media provider. As set out in paragraph 32, joint controllers may be involved at different stages and to different degrees which makes it necessary to assess the level of responsibility, and liability, with regard to the targeting operation. As mentioned before, Ecommerce Europe wants to emphasise the importance of carefully considering the various stages of processing of personal data and the role of targeter and social media service when assessing their respective responsibility and liability. Ecommerce Europe would thus welcome concrete guidelines and more guidance from the EDPB on how and to what extent these differences in factual influence and decision power between social media service provider and targeter affect the allocation of responsibility and liability.

❖ **Paragraphs 26-28**

Paragraphs 28 to 28 clarify the scope of the Guidelines. They explain that targeters may directly use targeting mechanisms offered by social media providers or enlist the services of other actors, such as marketing service providers, ad networks, ad exchanges, demand-side and supply-side platforms, data management providers (DMPs) and data analytics companies (also known as adtech). Although it is recognized that each of the other actors mentioned can play an important role in targeting of social media users, the focus of the guidelines is on the distribution of roles and data protection obligations of social media providers and targeters. Ecommerce Europe would like to point out that the relationships between the other actors and the SMPs often enable much of the activity that is discussed in the Guidelines. We would therefore welcome further clarification on the relationships with and the allocation of responsibility for information and controllership towards the other actors.

❖ **Paragraphs 32 and 33**

As a general remark, Ecommerce Europe would like to state that, because of the fact that in social media targeting services multiple parties are engaged in different roles, be it (joint) controller, processor or sub-

processor, it is extremely difficult for both data subjects as well as online retailers - especially SMEs - to identify their role and rights and obligations when using standard targeting services offered by social media service providers on a “take it or leave it” basis. Data subjects and targeters generally lack sufficient insights in the complexity of the GDPR and they often do not have any staff or resources to carefully assess their and other participants’ role and responsibilities in the targeting process. Furthermore, there is a lack of transparency of the actual processing of personal data by social media service providers in the course of targeting operations. In that perspective, the concept of joint controllership does not contribute to better insight for the targeters and data subjects nor to less complexity of the targeting process. Most targeters are probably not aware of the fact that the CJEU decisions qualify them as joint controllers and rely on the social media service providers to provide them with relevant information and standard solutions to guarantee a compliant targeting process.

Ecommerce Europe would welcome guidelines on how to enhance transparency of the targeting process and on to what extent and for which processing of personal data, targeters, in their role as joint controller with a limited role in the targeting operation, have to fulfil the obligations of a controller. In assessing the responsibility for the GDPR obligations of the targeter, it should be taken into account to what extent the targeter is factually capable to perform the obligations, as practice shows that even when targeters are informed on their role and willing to be compliant with GDPR rules there is no practical way to comply available.

- **Paragraph 33**

Ecommerce Europe strongly supports the CJEU ruling that the liability of the targeter is limited to the operation(s) involving the processing of personal data where the targeter actually determines the purposes and means (i.e. the collection and disclosure of data by transmission of the data at issue). In our view, it is key for a well-functioning online system of targeted advertisement that the liability regime for targeters is limited to those processing activities where the targeter has factual control over purpose and means. In practice, these are very few activities, and usually stops after the data has been collected from a tracking device and then after is has been transferred to the social media platform. When the information has been transferred, the rest of the processing is in the decision-making- power of the social media platform.

- **Paragraphs 43 and 53**

In this paragraph, the EDPB states its opinion that the legal basis for processing of personal data in targeting operations can generally only be on consent (Article 6(1)(a) GDPR) or legitimate interest (Article 6(1)(f) GDPR) and cannot be justified on the basis of Article 6(1)(b) that allows processing when necessary for the performance of a contract to which the data subject is party. Since it is generally accepted that consumers can pay for digital content services with their data (as for instance in the upcoming Directive on contract rules for the supply of digital content) and since payment is a contractual obligation, Ecommerce Europe is convinced that the limitation to only consent and legitimate interest is not justified. In case the data subject allows the controller to process his data for certain purposes (e.g. for targeting) as a counter performance for the digital service or digital content offered by the controller (e.g. a social media service provider), it would be logical to allow this processing on the legal ground of Article 6(1)(b) as the allowed processing is the only means for parties involved to effectively “pay” or collect the “payment”. In that perspective, we ask the EDPB to provide guidance on how this payment can be seen in terms of performing the contract.

- **Paragraph 47**

In this paragraph, it is stated that the ‘necessity’ requirement is particularly relevant in the context of the application of Article 6(1)f, in order to ensure that processing of data based on legitimate interest does not

lead to an unduly broad interpretation of the necessity to process data. As in other cases, this means that it should be considered whether other less invasive means are available to serve the same end. In the view of Ecommerce Europe, this statement creates doubts that legitimate interest could ever apply as legal ground for processing data in the context of targeting. Ecommerce Europe would therefore welcome some clear examples where the necessity requirement still allows targeting operations on the basis of legitimate interest and where there is no unduly broad interpretation of the necessity to process data.

❖ **Paragraph 57**

This paragraph states that, for the mentioned examples, the joint controllership of the targeter and the social media service provider begins with the transmission of the personal data, the collection of it by the social media provider and the consequent processing for the purpose of displaying targeted advertising and until the deletion of the data. In the opinion of Ecommerce Europe, this statement is rather unclear as regards to the deletion of data and causes confusion about the end of joint controllership, as in many cases the data would be retained by the social media provider and used for other purposes and will not be deleted at all. If deletion of the data by the targetter is meant as end of the joint controllership, we recommend the EDPB to clearly mention this.

❖ **Paragraph 63**

Paragraph 63 states that joint controllership of the targeter covers the collection of personal data and its transmission by way of pixels, as well as the matching and subsequent display of the advertisement to the data subject on the social platform, and for any reporting relating to the targeting campaign. In the view of Ecommerce Europe, it is unclear why the targeter would be the controller for the matching process and actual targeting (e.g. based on an algorithm) as these are processes where the targeter usually has no insight and influence over. Specifically, where pixels are used (vs. an upload method where the targeter may select clear targeting criteria), the matching process and the actual targeting are generally not very transparent to targeters and they have no means to determine or influence how data is matched by the social media service. In that perspective, we would recommend revising the statement and limit the joint controllership of the targeter to those targeting operations of the social media service provider he has insights on and is able to influence.

❖ **Paragraph 67**

In this paragraph, the EDPB states that actions such as scrolling or swiping through a webpage or similar user activity will not under any circumstances satisfy the requirement of a clear and affirmative act and thus consent. In the view of Ecommerce Europe, this very restrictive approach of the EDPB is not justified by the requirements in the GDPR for a clear affirmative action needed to conclude for unambiguous consent. Ecommerce Europe, as the DPA of Member States such as Spain, is convinced that that scrolling and clicking on a webpage can be seen as a clear affirmative action signifying agreement to the processing of personal data when the requirements of Articles 4.11 and 7 GDPR are met. Although it might be difficult for controllers to meet these requirements, it is not absolutely impossible, as the EDPB states. As we are convinced that scrolling can be a valid way of obtaining consent from users, Ecommerce Europe would rather welcome suggestions and guidelines from the EDPB on the conditions that have to be fulfilled when obtaining consent from users by way of scrolling or clicking than an overall ban of this type of consent.

❖ **Paragraph 68**

This paragraph states, referring to example 6 that, as the placement of cookies and processing of personal data occurs at the moment of account creation, the social media provider must collect valid consent of the data subject before the placement of advertisement cookies. In the view of Ecommerce Europe, this

statement, presuming that the first party involved in the targeting process, mostly the social media service provider, gathers consent for data being collected via a pixel placed by the targeter, is very confusing and not in line with the current social media services practice (as in example 4 and 6), where the obligation to collect consent for placing a pixel or cookies on his website is always given to the targeter. In that perspective, Ecommerce Europe recommends a clear statement that it is the targeter, using pixels or cookies to audit his customers and to transfer personal data to the social media provider, that should seek consent of the data subject and not the social media service provider.

❖ **Paragraph 69**

Paragraph 69 states that insofar as not all joint controllers are known at the moment when the social media provider seeks the consent, the latter will necessarily need to be complemented by further information and consent collected by the website operator embedding the social media plugin (i.e. Thelatesthotnews.com in example 6). Referring to our comments above, Ecommerce Europe considers this statement very confusing as, in practice, the social media service provider only has to seek consent for its own data processing operations. It generally does not know which targeters will use their targeting service and therefore it does not know who the joint controller will be at the moment the data subject engages in the social media services. As joint controllership starts with the engagement of the targeter in the targeting service, Ecommerce Europe recommends a clear statement that it is the targeter, using pixels or cookies to audit his customers and to transfer personal data to the social media provider, that starts joint controllership and should seek for consent of the data subject and not the social media service provider.

❖ **Paragraph 70**

Paragraph 70 states that the social media provider has to ensure that the data subject has provided a valid consent for the processing for which it is responsible as a joint controller as well as for any subsequent processing it carries out for which the targeter does not jointly determine the purposes and means (e.g. subsequent profiling operations for targeting purposes). In the view of Ecommerce Europe, this statement is unclear and confusing as to which consent has to be ensured and seems to be in contradiction with paragraph 63, especially since the social media provider has to ensure consent of the data subject for any subsequent profiling operation at the moment the data subject engages in the social media services and before the targeter engages in the targeting operation. Ecommerce Europe therefore asks for more clarity and rewording of this paragraph.

❖ **Paragraph 75**

In this paragraph, referring to example 7, joint controllership is assumed for targeted advertising “taking into account the collection of these data via the ‘like’-functionality on the social media platform, and the ‘analysis’ undertaken by the social media provider in order to offer the targeting criterion (...) to the targeter fitting the purpose of finally displaying the advertisement.” Similar to comments above, it is unclear to Ecommerce Europe how the targeter can jointly control the 'analysis' (inference of the targeting criteria) as this is based on data collected and processed by the social media platform with means determined by the social media platform. In practice, the targeter has no insight into how the conclusions are being drawn. How can the targeter thus be responsible for this processing? As a consequence, the targeter would not be able to fulfil its obligations under the GDPR with regard to processing, such as explaining the processing activity in a record of processing activities, determining if a DPIA is necessary, providing information on the processing to data subjects, etc. as it cannot practically gain insights into this processing at all. Ecommerce Europe therefore strongly recommends to explicitly limit joint controllership of the targeter to those operations where he has factual insight and decision power on purposes and means of the processing.

❖ **Paragraph 80**

Paragraph 80 states that an assessment as to whether targeting will "similarly significantly [affect]" a data subject, will need to be conducted by the controller or joint controllers. Similar to comments above, it is unclear to Ecommerce Europe how a targeter can analyse whether the algorithms used by a social media platform to create target audiences or target audience criteria, would similarly significantly affect a data subject, as a targeter factually will never get insights in the methods used by a social media provider? As this statement seems to put a 'blind responsibility' on the targeter for operations he factually cannot analyse, Ecommerce Europe strongly recommends to explicitly limit joint controllership and obligations of the targeter to those operations he has factual insight and do not put burdens on targeters which they cannot fulfil.

❖ **Paragraph 88**

This paragraph describes that joint controllers can mutually agree that one of them shall be tasked with providing the initial information to data subjects and 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 to enable him to provide the data subject with full information in accordance with Articles 13 and 14 GDPR. For this statement, Ecommerce Europe wants to draw the attention of the EDPB on the fact that, in practice, responsibility for providing information is contractually (mostly a "take it or leave it" standard contract unilaterally decided on by the social media platform) almost always given to targeters who do not have insights into the targeting mechanisms. Moreover, it is even upon request for information to the social media provider almost impossible for a targeter to provide clear information about a social media platform's targeting mechanism. As this practice creates an imbalance and places more responsibility with the targeter than with the social media platform that mainly decides on purposes and means of the targeting operation, Ecommerce Europe would welcome more guidance on the validity of such contractual agreements shifting responsibility standard to the targeter.

❖ **Paragraph 91**

In this paragraph, it is stated that each joint controller is responsible for ensuring that the essence of the arrangement as meant in Article 26(1) GDPR is made available to the data subject. In practice, the essence of the arrangement should be directly available on the platform, referred to in its privacy policy, and also made directly accessible by a link, for example, in the targeter's page on the social media platform or in links such as "why am I seeing this ad?". Following the new guidance, many relationships might be re-qualified to joint controllership. In Ecommerce Europe's view, it will be in practice almost impossible to list all providers that might be having joint controllership for certain processing activities in the advertising value chain in a precise and concise manner. Therefore, it will also be a challenge to determine which actors will have the responsibility for ensuring that the essence of the arrangement as meant in Article 26(1) GDPR is made available to the data subject. Also, to avoid overkill of information, more guidance on how to practically apply and allocate this responsibility of all joint controllers involved, would be helpful.

❖ **Paragraphs 92-97**

Paragraphs 92 to 97 focus on how and by whom the right of access should be accommodated in the context of targeting of social media users. They describe that "data controllers must enable users to easily and fully exercise their data subjects' rights". Ecommerce Europe believes that data subject rights such as this "right to access" can often only be fulfilled by social media providers, in particular as targeters often do not have the required knowledge about the data subjects that were targeted by the social media providers.

Ecommerce Europe would welcome a further focus on such data subject rights as a core responsibility of the social media provider.

❖ **Paragraphs 101 and 104**

In these paragraphs, it is inter alia stated that, both joint controllers need to assess whether a DPIA is necessary and when a DPIA is necessary, they are both responsible for fulfilling this obligation. In the view of Ecommerce Europe, in practice, the targeter as joint controller will not be able to participate in or conduct such a DPIA, as social media platforms would never share how they infer data or create targeting criteria and thus make it impossible for targeters to effectively assess the impact of the data processing. In that perspective, Ecommerce Europe is convinced that DPIAs should generally be conducted by the social media platforms that have the relevant insights to do so, and urges the EDPB to come up with guidance on how to practically deal with this impossibility for targeters.

❖ **Paragraph 133**

Paragraph 133 states that if consent is sought, the joint controllers should agree upon the way consent is collected. As in previous comments, Ecommerce Europe wants to draw attention to the fact that the targeter in many instances would not exactly know what data is collected and how it is used to create targeting criteria and combined with other data. This section should note that for the actual creation of targeting criteria the social media provider has a higher level of responsibility and thus also as regards to the agreement upon the way consent is collected. Guidance on this issue and the role of targeter and social media in seeking consent would be welcome.