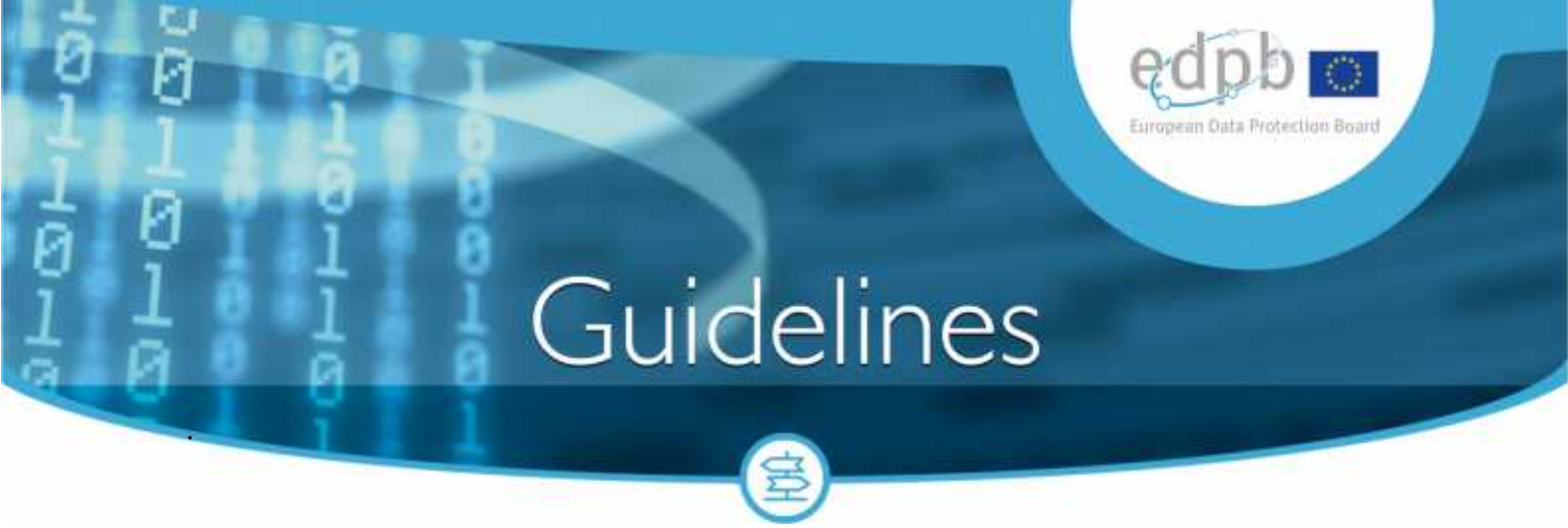

Guidelines 8/2020 on the targeting of social media users

Version 1.0

Adopted on 2 September 2020

The European Data Protection Board

Having regard to Article 70(1)(e) of Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

HAS ADOPTED THE FOLLOWING GUIDELINES

1 INTRODUCTION

1. A significant development in the online environment over the past decade has been the rise of social media. More and more individuals use social media to stay in touch with family and friends, to engage in professional networking or to connect around shared interests and ideas. For the purposes of these guidelines, social media are understood as online platforms that enable the development of networks and communities of users, among which information and content is shared.[1] Key characteristics of social media include the ability for individuals to register in order to create "accounts" or "profiles" for themselves, to interact with one another by sharing user-generated or other content and to develop connections and networks with other users.[2]

2. As part of their business model, many social media providers offer targeting services. Targeting services make it possible for natural or legal persons ("targeters") to communicate specific messages to the users of social media in order to advance commercial, political, or other interests.[3] A distinguishing characteristic of targeting is the perceived fit between the person or group being targeted and the message that is being delivered. The underlying assumption is that the better the fit, the higher the reception rate (conversion) and thus the more effective the targeting campaign (return on investment).

3. Mechanisms to target social media users have increased in sophistication over time. Organisations now have the ability to target individuals on the basis of a wide range of criteria. Such criteria may have been developed on the basis of personal data which users have actively provided or shared, such as their relationship status. Increasingly, however, targeting criteria are also developed on the basis of personal data which has been 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) to support ad-targeting options. In other words, the targeting of social media users involves not just the act of "selecting" the individuals or groups of individuals that are the intended recipients of a particular

[1] Additional functions provided by social media may include, for example, personalization, application integration, social plug-ins, user authentication, analytics and publishing. Social media functions may be a standalone offering of controllers or they may be integrated as part of a wider service offering.

[2] In addition to "traditional" social media platforms, other examples of social media include: dating platforms where registered users present themselves to find partners they can date in real life; platforms where registered users can upload their own videos, comment on and link to other's videos; or computer games where registered users may play together in groups, exchange information or share their experiences and successes within the game.

[3] Targeting has been defined as "the act of directing or aiming something at a particular group of people" and "the act of attempting to appeal to a person or group or to influence them in some way". https://www.collinsdictionary.com/dictionary/english/targeting.

message (the 'target audience'), but rather it involves an entire process carried out by a set of stakeholders which results in the delivery of specific messages to individuals with social media accounts.[4]

4. The combination and analysis of data originating from different sources, together with the potentially sensitive nature of personal data processed in the context of social media[5], creates risks to the fundamental rights and freedoms of individuals. From a data protection perspective, many risks relate to the possible lack of transparency and user control. For the individuals concerned, the underlying processing of personal data which results in the delivery of a targeted message is often opaque. Moreover, it may involve unanticipated or undesired uses of personal data, which raise questions not only concerning data protection law, but also in relation to other fundamental rights and freedoms. Recently, social media targeting has gained increased public interest and regulatory scrutiny in the context of democratic decision making and electoral processes.[6]

2 SCOPE

5. Targeting of social media users may involve a variety of different actors which, for the purposes of these guidelines, shall be divided into four groups: social media providers, their users, targeters and other actors which may be involved in the targeting process. The importance of correctly identifying the roles and responsibilities of the various actors has recently been highlighted with the judgments in *Wirtschaftsakademie* and *Fashion ID* of the Court of Justice of the European Union (CJEU).[7] Both judgments demonstrate that the interaction between social media providers and other actors may give rise to joint responsibilities under EU data protection law.

6. Taking into account the case law of the CJEU, as well as the provisions of the GDPR regarding joint controllers and accountability, the present guidelines offer guidance concerning the targeting of social media users, in particular as regards the responsibilities of targeters and social media providers. Where joint responsibility exists, the guidelines will seek to clarify what the distribution of responsibilities might look like between targeters and social media providers on the basis of practical examples[8].

7. The main aim of these guidelines is therefore to clarify the roles and responsibilities among the social media provider and the targeter. In order to do so, the guidelines also identify the potential risks for the rights and freedoms of individuals (section 3), the main actors and their roles (section 4), and tackles the application of key data protection requirements (such as lawfulness and transparency, DPIA, etc.) as well as key elements of arrangements between social media providers and the targeters.

---

[4] The messages delivered typically consist of images and text, but may also involve video and/or audio formats.

[5] Personal data processed in the context of social media may constitute 'special categories of personal data' pursuant to Article 9 GDPR, relate to vulnerable individuals, or otherwise be of a highly personal nature. See also Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP 248 rev. 01, p. 9.

[6] See, for example: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-03-13-statement-on-elections_en.pdf; https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/07/findings-recommendations-and-actions-from-ico-investigation-into-data-analytics-in-political-campaigns/; https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-data-protection-law-electoral-guidance-638_en.pdf; https://www.personuvernd.is/information-in-english/greinar/nr/2880.

[7] 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, ECLI:EU:C:2019:629.

[8] The present guidance is without prejudice to the EDPB Guidelines 07/2020 on the concepts of controller and processor under the GDPR adopted on 02 September 2020, concerning the distribution of responsibilities in other contexts.

3 RISKS TO THE RIGHTS AND FREEDOMS OF USERS POSED BY THE PROCESSING OF PERSONAL DATA

8. The GDPR underlines the importance of properly evaluating and mitigating any risks to the rights and freedoms of individuals resulting from the processing of personal data.[9] 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. These guidelines do not seek to provide an exhaustive account of the possible risks to the rights and freedoms of individuals. Nonetheless, the EDPB considers it important to point out certain types of risks and to provide a number of examples how they may manifest themselves.

9. Targeting of social media users may involve uses of personal data that go against or 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, this may result in personal data being used beyond their initial purpose and in ways the individual could not reasonably anticipate. The profiling activities that are connected to targeting might involve an inference of interests or other characteristics, which the individual had not actively disclosed, thereby undermining the individual's ability to exercise control over his or her personal data.[10] Moreover, 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.

10. A second type of risk concerns the possibility of discrimination and exclusion. Targeting of social media users may involve criteria that, directly or indirectly, have discriminatory effects relating to an individual's racial or ethnic origin, health status or sexual orientation, or other protected qualities of the individual concerned. For example, the use of such criteria in the context of advertising related to job offers, housing or credit (loans, mortgages) may reduce the visibility of opportunities to persons within certain groups of individuals. The potential for discrimination in targeting arises from the ability for advertisers to leverage the extensive quantity and variety of personal data (e.g. demographics, behavioral data and interests) that social media platforms gather about their users.[11] Recent research suggests that the potential for discriminatory effects exists also without using criteria that are directly linked to special categories of personal data in the sense of Article 9 of the GDPR.[12]

11. A second category of risk relates to potential possible manipulation of users. Targeting mechanisms are, by definition, used in order to influence the behavior and choices of individuals, whether it be in terms of their purchasing decisions as consumers or in terms of their political decisions as citizens

[9] According to Article 24 of the GDPR, the controller shall implement appropriate technical and organizational measures to ensure and be able to demonstrate that processing is performed in accordance with the GDPR, "taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons". See also Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP248 rev. 01, 4 October 2017.

[10] See also European Data Protection Supervisor, EDPS Opinion on online manipulation, Opinion 3/2018, 19 March 2018, p. 15 ("*The concern of using data from profiles for different purposes through algorithms is that the data loses its original context. Repurposing of data is likely to affect a person's informational self-determination, further reduce the control of data subjects' over their data, thus affecting the trust in digital environments and services.*").

[11] T. Speicher a.o., Potential for Discrimination in Online Targeted Advertising, Proceedings of the 1st Conference on Fairness, Accountability and Transparency, *Proceedings of Machine Learning Research* PMLR 81:5-19, 2018, http://proceedings.mlr.press/v81/speicher18a.html.

[12] Idem.

engaged in civic life.[13] Certain targeting approaches may however go so far as to undermine individual autonomy and freedom, e.g. by delivering individualized messages designed to exploit or even accentuate certain vulnerabilities, personal values or concerns. For example, an analysis of content shared through social media can reveal information about the emotional state (e.g. through an analysis of the use of certain key words). Such information could be used to target the individual with specific messages and at specific moments to which he or she is expected to be more receptive, thereby surreptitiously influencing his or her thought process, emotions and behaviour.[14]

12. Mechanisms to target social media users can also be used to unduly influence individuals when it comes to political discourse and democratic electoral processes.[15] While 'traditional' offline political campaigning intends to influence voters' behaviour via messages that are generally available and retrievable (verifiable), the available online targeting mechanisms enable political parties and campaigns to target individual voters with tailored messages, specific to the particular needs, interests and values of the target audience.[16] Such targeting might even involve disinformation or messages that individuals find particularly distressing, and are therefore (more) likely to stimulate a certain emotion or reaction by them. When polarising or untruthful (disinformation) messages are targeted at specific individuals, with no or limited contextualisation or exposure to other viewpoints, the use of targeting mechanisms can have the effect of undermining the democratic electoral process.[17]

13. In the same vein, the use of algorithms to determine which information is displayed to which individuals may adversely affect the likelihood of access to diversified sources of information in relation to a particular subject matter. This may in turn have negative consequences for the pluralism of public debate and access to information.[18] Targeting mechanisms can be used to augment the visibility of certain messages, while giving less prominence to others. The potential adverse impact may be felt at two levels. On the one hand, there are risks related to so-called 'filter-bubbles' where people are exposed to 'more-of-the-same' information and encounter fewer opinions, resulting in increased political and ideological polarisation.[19] On the other hand, targeting mechanisms may also create risks of "information overload", whereby individuals cannot make an informed decision because they have too much information and cannot tell if it is reliable.

14. The collection of personal data by social media providers may not be limited to the activities performed by individuals on the social media platform itself. The targeting of social media users on the basis of information concerning their browsing behaviour or other activities outside the social media platform can give individuals the feeling that their behaviour is systematically being monitored. This may have

[13] European Data Protection Supervisor, Opinion 3/2018, p. 18.

[14] See 'Experimental evidence of massive-scale emotional contagion through social networks', Adam D. I. Kramer, Jamie E. Guillory, and Jeffrey T. Hancock, PNAS June 17, 2014 111 (24) 8788-8790; first published June 2, 2014 https://doi.org/10.1073/pnas.1320040111, available at: https://www.pnas.org/content/111/24/8788 Adam D. I. Kramer Core Data Science Team, Facebook, Inc., Menlo Park, CA 94025.

[15] See also European Data Protection Board, Statement 2/2019 on the use of personal data in the course of political campaigns, 13 March 2019, p. 1.

[16] Information Commissioner's Office (ICO), *Democracy disrupted? Personal information and political influence*, 10 July 2018, p. 14.

[17] See also European Commission, Commission Guidance on the application of Union data protection law in the electoral context, A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018. See also L.M. Neudert and N.M. Marchal, Polarisation and the use of technology in political campaigns and communication, European Parliamentary Research Service, 2019, p. 22-24.

[18] See also European Parliament resolution of 3 May 2018 on media pluralism and media freedom in the European Union.

[19] European Data Protection Supervisor, Opinion 3/2018, p. 7.

a chilling effect on freedom of expression, including access to information.[20] Such effects may be exacerbated if targeting is also based on the analysis of content shared by social media users. If private messages, posts and comments are subject to analysis for commercial or political use, this may also give rise to self-censorship.

15. The potential adverse impact of targeting may be considerably greater where vulnerable categories of individuals are concerned, such as children. Targeting can influence the shaping of children's personal preferences and interests, ultimately affecting their autonomy and their right to development. Recital 38 of the GDPR indicates that 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.[21]

16. The EDPB recognizes that the increase in concentration in the markets of social media and targeting may also increase risks to the rights and freedoms of individuals. For example, certain social media providers may be able to combine, either alone or in connection with other companies, a higher quantity and diversity of personal data. This ability, in turn, may increase the ability to offer more advanced targeting campaigns. This aspect is relevant from both a data protection (more in-depth profiling of the persons concerned) and competition law viewpoint (the unrivalled insight capabilities provided by the platform may make it an *'unavoidable trading partner'* for online marketers). The degree of market and informational power, in turn, as the EDPB has recognised, "*has the potential to threaten the level of data protection and freedom enjoyed by consumers of digital services*".[22]

17. The likelihood and severity of the aforementioned risks will depend, inter alia, on the nature of the targeting mechanism and how and for which exact purpose(s) it is used. Elements which may affect the likelihood and severity of risks in the context of the targeting of social media users will be discussed in greater detail in section 7.

4 ACTORS AND ROLES

4.1 Users

18. Individuals make use of social media in different capacities and for different purposes (e.g. to stay in touch with friends, to exchange information about shared interests, or to seek out employment opportunities). The term "user" is typically used to refer to individuals who are registered with the service, i.e. those who have an "account" or "profile". Many social media services can, however, also be accessed by individuals without having registered (i.e. without creating an account or profile).[23] Such individuals are typically not able to make use of all of the same features or services offered to individuals who have registered with the social media provider. Both users and non-registered

[20] European Data Protection Supervisor, Opinion 3/2018, p. 9 and Committee of experts on media pluralism and transparency of media ownership (MSI-MED), Internet and Electoral Campaigns, Study on the use of internet in electoral campaigns, Council of Europe study DGI(2017)11, April 2018, p. 19-21.
[21] See also Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 6 February 2018, WP251rev.01, p. 29.
[22] Statement of the EDPB on the data protection impacts of economic concentration, available at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_economic_concentration_en.pdf
[23] The personal data and profiling information maintained by social media providers in relation to non-registered users are sometimes referred to as "shadow profiles".

individuals may be considered "data subjects" within the meaning of Article 4(1) GDPR insofar as the individual is directly or indirectly identified or identifiable.[24]

19. Whether or not individuals are expected to register with a real name or use a nickname or pseudonym may vary according to the social media service in question. It will generally still be possible, however, to target (or otherwise single out) the user in question even in the absence of a real name policy, as most types of targeting do not rely on user names but other types of personal data such as interests, sociographic data, behaviour or other identifiers. Social media providers often encourage users to reveal "real world" data, such as telephone numbers.[25] Finally, it is worth noting that social media providers may also enable targeting of individuals who do not have an account with the social media provider.[26]

4.2 Social media providers

20. Social media providers offer an online service that enables the development of networks and communities of users, among which information and content is shared. Social media services are typically offered through web browsers or dedicated apps, often after having requested the user to provide a set of personal data to constitute the user's "account" or "profile". They also often offer users associated account "controls", to enable them to access and control the personal data processed in the context of the use of their account.

21. The social media provider determines the functionalities of the service. This in turn involves a determination of which data are processed, for which purpose, under which terms, as well as how personal data shall be processed. This allows for the provision of the social media service but also likely the provision of services, such as targeting, that can benefit business partners operating on the social media platform or in conjunction with it.

22. The social media provider has the opportunity to gather large amounts of personal data relating to users' and non-registered users´ behaviour and interactions, which enables it to obtain considerable insights into the users' socio-demographic characteristics, interests and preferences. It is important to note that the 'insights' based on user activity often involve inferred or derived personal data. For example, where a user interacts with certain content (e.g. by "liking" a post on social media, or watching video content), this action can be recorded by the social media provider, and an inference might be made that the user in question enjoyed the content he or she interacted with.

23. Social media providers increasingly gather data not only from activities on the platform itself, but also from activities undertaken 'off-platform', combining data from multiple sources, online and offline, in order to generate further insights. The data can be combined with personal data that individuals actively disclose to the social media provider (e.g. a username, e-mail address, location, and phone number), alongside data which is "assigned" to them by the platform (such as unique identifiers).

[24] See also recital (26) ("singling out"). See also Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, 20 June 2007, WP 136, p. 12 and following.

[25] In some cases, social media providers ask for additional documentation to further verify the data provided, for example by requesting users to upload their ID cards or similar documentation.

[26] Such targeting may be rendered possible on the basis of online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them. See also recital (30) GDPR. Based on this recognition, targeted ads may be displayed on a website the individual visits.

4.3 Targeters

24. These 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.[27] What sets targeters apart from other users of social media is that they select their messages and/or their intended audience according to the perceived characteristics, interests or preferences of the individuals concerned, a practice which is sometimes also referred to as "micro-targeting".[28] Targeters can engage in targeting to advance commercial, political, or other interests. Typical examples include brands who use social media to advertise their products including to increase brand awareness. Political parties also increasingly make use of social media as part of their campaigning strategy. Charities and other non-profit organisations also use social media to target messages at potential contributors or to develop communities.

25. It is important to note that social media users can be targeted in different ways. For example, targeting might occur not only through displaying personalized advertisement (e.g. through a "banner" shown on the top or side of a webpage), but - as far as it is happening within the social media platform - also through display in a user's "feed", "timeline" or "story", where the advertising content appears alongside user-generated content. Targeting may also involve the creation of content hosted by the social media provider (e.g. via a dedicated "page" or other social media presence) or elsewhere (i.e. on third-party websites). Targeters may have their own websites and apps, where they can integrate specific social media business tools or features such as social plugins or logins or by using the application programming interfaces (APIs) or software development kits (SDKs) offered by social media providers.

4.4 Other relevant actors

26. 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. These actors are part of the complex and evolving online advertising ecosystem (which is sometimes known as "adtech") that collects and processes data relating to individuals (including social media users) by, for example, tracking their activities across websites and apps.[29]

27. Data brokers and data management providers are also relevant actors playing an important role in the targeting of social media users. Data brokers and DMPs differentiate themselves from other adtech companies to the extent that they not only process data collected by means of tracking technologies, but also by means of data collected from other sources, that can include both online and offline sources. In other words, data brokers and DMPs aggregate data collected from a wide variety of sources, which they then might sell to other stakeholders involved in the targeting process.[30]

28. While each of the other actors mentioned above can play an important role in targeting of social media users, the focus of the current guidelines is on the distribution of roles and data protection obligations

[27] Processing of personal data by a natural person in the course of a purely personal or household activity does not fall under the material scope of the GDPR (Art. 2(2)(c)).

[28] Simply sharing information on a social media page which is intended for the public at large (e.g. information about opening hours) without prior selection of the intended audience would not be considered as « targeting » for the purposes of these guidelines.

[29] On the description of the different actors, see WP29, Opinion 2/2010 on behavioural advertisement, at page 5. The Opinion is available at: https://ec.europa.eu/justice/Article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf

[30] See Consumer Policy Research Centre, "*A day in the life of data*", available at: http://cprc.org.au/publication/research-report-a-day-in-the-life-of-data/

of social media providers and targeters. Analogous considerations may apply, however, to the other actors involved in the online advertising ecosystem, depending on the role of each actor in the targeting process.

4.5 Roles and responsibilities

29. In order to clarify the respective roles and responsibilities of social media providers and targeters, it is important to take account of the relevant case law of the CJEU. The judgments in *Wirtschaftsakademie* (C-210/16), *Jehovah's Witnesses* (C-25/17) and *Fashion ID* (C-40/17) are particularly relevant here.

30. The starting point of the analysis is the legal definition of controller. According to Article 4(7) GDPR, a "'controller" means "*the natural or legal person […] which, alone or jointly with others, determines the purposes and means of the processing of personal data*".

31. In *Wirtschaftsakademie*, the CJEU decided that the administrator of a so-called "fan page" on Facebook must be regarded as taking part in the determination of the purposes and means of the processing of personal data. According to the submissions made to the CJEU, the creation of a fan page involves the *definition of parameters* by the administrator, which has an *influence* on the processing of personal data for the purpose of *producing statistics* based on visits to the fan page.[31] Using the filters provided by Facebook, the administrator can define the criteria in accordance with which the statistics are to be drawn up, and even designate the categories of persons whose personal data is to be made use of by Facebook:

> "*In particular, the administrator of the fan page can ask for — and thereby request the processing of — demographic data relating to its target audience, including trends in terms of age, sex, relationship and occupation, information on the lifestyles and centres of interest of the target audience and information on the purchases and online purchasing habits of visitors to its page, the categories of goods and services that appeal the most, and geographical data which tell the fan page administrator where to make special offers and where to organise events, and more generally enable it to target best the information it offers.*"

As the definition of parameters depends inter alia on the administrator's target audience "*and the objectives of managing and promoting its activities"*, the administrator also participates in determining the purposes of the processing of personal data.[32] The administrator was therefore categorised as a controller jointly responsible for the processing of personal data of the visitors of its 'page', together with the social media provider.

32. As further developed in section 9 of the present guidelines, controllers may be involved at different stages of the processing of personal data and to different degrees. In such circumstances, the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case:

> "*[T]he existence of joint responsibility does not necessarily imply equal responsibility of the various operators involved in the processing of personal data. On the contrary, those operators may be involved at different stages of that processing of personal data and to different degrees, so that the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case*."[33]

[31] Judgment in *Wirtschaftsakademie*, C-210/16, paragraph 36.
[32] Judgment in *Wirtschaftsakademie*, C-210/16, paragraph 39.
[33] Judgment in *Wirtschaftsakademie*, C-210/16, paragraph 43; Judgment in *Jehovah's Witnesses*, C-25/17, paragraph 66 and Judgment in *Fashion ID*, C-40/17, paragraph 70.

While concluding that the administrator of a page acts as a controller, jointly with Facebook, the CJEU also noted that in the present case, Facebook must be regarded as *primarily* determining the purposes and means of processing the personal data of users of Facebook and persons visiting the fan pages hosted on Facebook.[34]

33. In *Fashion ID*, the CJEU decided that a website operator can be a considered a controller when it embeds a Facebook social plugin on its website that causes the browser of a visitor to transmit personal data of the visitor to Facebook.[35] The qualification of the website operator as controller is, however, limited to the operation or set of operations in respect of which it actually determines the purposes and means. In this particular case, the CJEU considered that the website operator is only capable of determining, jointly with Facebook, the purposes and means of the collection and disclosure by transmission of the personal data of visitors to its website. As a result, the CJEU ruled that, for what concerns the embedding of a social plug-in within a website, the liability of the website operator is:

> "*limited to the operation or set of operations involving the processing of personal data in respect of which it actually determines the purposes and means, that is to say, the collection and disclosure by transmission of the data at issue.*"[36]

The CJEU considered that the website operator was not a controller for subsequent[37] operations involving the processing of personal data carried out by Facebook after their transmission to the latter, as the website operator was not in a position to determine the purposes and means of those operations by virtue of embedding the social plug-in:

> "*By contrast, in the light of that information, it seems, at the outset, impossible that Fashion ID determines the purposes and means of subsequent operations involving the processing of personal data carried out by Facebook Ireland after their transmission to the latter, meaning that Fashion ID cannot be considered to be a controller in respect of those operations [...]*".[38]

34. 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 particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14 GDPR.

35. The following sections clarify, by way of specific examples, the roles of targeters and social media providers in relation to different targeting mechanisms. Specific considerations are given in particular as to how the requirements of lawfulness and purpose limitation apply in this context. Next, the requirements concerning transparency, data protection impact assessments and the processing of special categories of data are analysed. Finally, the Guidelines address the obligation for joint

[34] Judgment in *Wirtschaftsakademie*, C-210/16, paragraph 30.
[35] Judgment in *Fashion ID*, C-40/17, paragraph 75 and following and paragraph 107.
[36] Judgment in *Fashion ID*, C-40/17, paragraph 107.
[37] Subsequent processing is any processing operation or set of processing operations which follows (i.e. takes place after) the data collection. In Fashion ID, the term is used to refer to processing operations carried out by Facebook after their transmission and for which Fashion ID should not be considered as a joint controller (because it does not effectively participate in determining the purposes and means of those processing).
Subsequent processing for a purpose other than that for which the personal data have been collected is only permissible insofar as Article 6(4) GDPR relating to further processing is complied with. For example, if an online retailer collects data relating to an individual's home address, a subsequent processing would consist in the storage or later deletion of this information. However, if this online retailer later decides to process this personal data to enrich the profile of the data subject for targeting purposes, this would amount to further processing within the meaning of Article 6(4) GDPR as it involves processing for a purpose other than that for which they were initially collected.
[38] Judgment in *Fashion ID*, C-40/17, paragraph 76.

controllers to put in place an appropriate arrangement pursuant to Article 26 GDPR, taking into account the degree of responsibility of the targeter and of the social media provider.

5 ANALYSIS OF DIFFERENT TARGETING MECHANISMS

5.1 Overview

36. Social media users may be targeted on the basis of provided, observed or inferred data, as well as a combination thereof:

a) **Targeting individuals on the basis of provided data** – "Provided data" refers to information actively provided by the data subject to the social media provider and/or the targeter.[39] For example:

- A social media user might indicate his or her age in the description of his or her user profile. The social media provider, in turn, might enable targeting on the basis of this criterion.
- A targeter might use information provided by the data subject to the targeter in order to target that individual specifically, for example by means of customer data (such as an e-mail address list), to be matched with data already held on the social media platform, leading to all those users who match being targeted with advertising[40].

b) **Targeting on the basis of observed data** – Targeting of social media users can also take place on the basis of observed data.[41] Observed data are data provided by the data subject by virtue of using a service or device.[42] For example, a particular social media user might be targeted on the basis of:

- his or her activity on the social media platform itself (for instance the content that the user has shared, consulted or liked);
- the use of devices on which the social media's application is executed (for instance GPS coordinates, mobile telephone number);
- data obtained by a third-party application developer by using the application programming interfaces (APIs) or software development kits (SDKs) offered by social media providers;
- data collected through third-party websites that have incorporated social plugins or pixels;
- data collected through other third parties (e.g. parties with whom the data subject has interacted, purchased a product, subscribed to loyalty cards, …); or

[39] Article 29 Data Protection Working Party, Guidelines on the right to data portability, WP 242 rev.01, 5 April 2017, p. 10.
[40] See for example the decision by the Administrative Court of Bayreuth (Germany), Beschluss v. 08.05.2018, B1 S 18.105, http://www.gesetze-bayern.de/Content/Document/Y-300-Z-BECKRS-B-2018-N-9586.
[41] In its Opinion 2/2010 on online behavioural advertising the WP29 noted that "*there are two main approaches to building user profiles: i) Predictive profiles are established by inference from observing individual and collective user behaviour over time, particularly by monitoring visited pages and ads viewed or clicked on. ii) Explicit profiles are created from personal data that data subjects themselves provide to a web service, such as by registering*" (Article 29 Data Protection Working Party, Opinion 2/2010 on online behavioural advertising, WP 171, p. 7).
[42] Article 29 Data Protection Working Party, Guidelines on the right to data portability, WP 242 rev.01, 5 April 2017, p. 10.

- data collected through services offered by companies owned or operated by the social media provider.

c) **Targeting on the basis of inferred data** – "Inferred data" or "derived data" are created by the data controller on the basis of the data provided by the data subject or as observed by the controller.[43] For example, a social media provider or a targeter might infer that an individual is likely to be interested in a certain activity or product on the basis of his or her web browsing behaviour and/or network connections.

5.2 Targeting on the basis of provided data

5.2.1 Data provided by the user to the social media provider

37. Individuals may actively disclose a great deal of information about themselves when making use of social media. The creation of a social media account (or "profile") involves disclosure of a number of attributes, which may include name, date of birth, gender, place of residence, language, etc. Depending on the nature of the social media platform, users may include additional information such as relationship status, interests or current employment. Personal data provided by social media users can be used by the social media provider to develop criteria, which enables the targeter to address specific messages at the users of the social media.

Example 1 :

Company X sells gentlemen's shoes and wishes to promote a sale of its winter collection. For its advertising campaign, it wishes to target men between the age of 30 and 45 who have indicated that they are single in their social media profile. It uses the corresponding targeting criteria offered by the social media provider as parameters to identify the target audience to whom its advertisement should be displayed. Moreover, the targeter indicates that the advertisement should be displayed to social media users while they are using the social media service between the hours of 5pm and 8pm. To enable targeting of social media users on the basis of specific criteria, the social media provider has previously determined which types of personal data shall be used in order to develop the targeting criteria and which targeting criteria shall be offered. The social media provider also communicates certain statistical information once the advertisements has been displayed to the targeter (e.g. to report on the demographic composition of individuals that interacted with the advertisement).

A. Roles

38. In Example 1, both the targeter and the social media provider participate in determining the purpose and means of the processing personal data. This results in the display of the advertisement to the target audience.

39. As far as the determination of *purpose* is concerned, Company X and the social media provider jointly determine the purpose of the processing, which is to display a specific advertisement to a set of individuals (in this case social media users) who make up the target audience.

40. As far as the determination of *means* is concerned, the targeter and the social media provider jointly determine the means, which results in the targeting. The targeter participates in the determination of the means by choosing to use the services offered by the social media provider, and by requesting it to target an audience based on certain criteria (i.e. age range, relationship status, timing of display).[44]

[43] *Idem.*

[44] See in this respect *Wirtschaftsakademie*, C-210/16, para. 39 - ECLI:EU:C:2018:388.

In doing so, the targeter defines the criteria in accordance with which the targeting takes place and designates the categories of persons whose personal data is to be made use of. The social media provider, on the other hand, has decided to process personal data of its users in such a manner to develop the targeting criteria, which it makes available to the targeter.[45] In order to do so, the social media provider has made certain decisions regarding the essential means of the processing, such as which categories of data shall be processed, which targeting criteria shall be offered and who shall have access (to what types of) personal data that is processed in the context of a particular targeting campaign.[46]

41. The joint control among the targeter and social media provider only extends to those processing operations for which they effectively co-determine the purposes and means. It extends to the processing of personal data resulting from the selection of the relevant targeting criteria and the display of the advertisement to the target audience. It also covers the processing of personal data undertaken by the social media provider to report to the targeter about the results of the targeting campaign. The joint control does not, however, extend to operations involving the processing of personal data at other stages occurring before the selection of the relevant targeting criteria or after the targeting and reporting has been completed, and in which the targeter has not participated in determining the purposes and means".[47]

42. The above analysis remains the same even if the targeter only specifies the parameters of its intended audience and does not have access to the personal data of the users that are affected. Indeed, joint responsibility of several actors for the same processing does not require each of them to have access to the personal data concerned.[48] The EDPB recalls that actual access to personal data is not a prerequisite for joint responsibility.[49]

B. Legal basis

As joint controllers, both parties (the social media provider and the targeter) must be able to demonstrate the existence of a legal basis (Article 6 GDPR) to justify the processing of personal data for which each of the joint controllers is responsible. The EDPB recalls that no specific hierarchy is made between the different lawful basis of the GDPR: the controller needs to ensure that the selected lawful basis matches the objective and context of the processing operation in question. The identification of the appropriate lawful basis is tied to principles of fairness and purpose limitation.[50]

43. Generally speaking, there are two legal bases which could theoretically justify the processing that supports the targeting of social media users: data subject's consent (Article 6(1)(a) GDPR) or legitimate

[45] See in the same vein also *Fashion ID*, C-40/17, para. 80: "*those processing operations are performed in the economic interests of both Fashion ID and Facebook Ireland, for whom the fact that it can use those data for its own commercial purposes is the consideration for the benefit to Fashion ID*".
[46] See Opinion 1/2010.
[47] See also Judgment in *Fashion ID*, C-40/17, para. 74 ("*[a] natural or legal person cannot be considered to be a controller, within the meaning of that provision, in the context of operations that precede or are subsequent in the overall chain of processing for which that person does not determine either the purposes or the means*") and paragraph 101.
[48] Judgment in *Wirtschaftsakademie*, C-210/16, para. 38 - ECLI:EU:C:2018:388; Judgment in *Jehovah's Witnesses*, C-25/17, para. 69 - ECLI:EU:C:2018:551.
[49] CJEU Judgment 10 July 2018 (C-25/17, para. 68 to 72).
[50] See paragraph 18, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, 8 October 2019, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf

interests (Article 6(1)(f) GDPR). A controller must always consider what the appropriate legal basis is under the given circumstances.

44. For what concerns the legitimate interest lawful basis, the EDPB recalls that in *Fashion ID*, the CJEU reiterated that in order for a processing to rely on the legitimate interest, three cumulative conditions should be met, namely[51] (i) the pursuit of a legitimate interest by the data controller or by the third party or parties to whom the data are disclosed, (ii) the need to process personal data for the purposes of the legitimate interests pursued, and (iii) the condition that the fundamental rights and freedoms of the data subject whose data require protection do not take precedence. The CJEU also specified that in a situation of joint controllership "*it is necessary that each of those controllers should pursue a legitimate interest […] through those processing operations in order for those operations to be justified in respect of each of them*".[52]

45. The EDPB recalls that in cases where a controller envisages to rely on legitimate interest, the duties of transparency and the right to object require careful consideration. Data subjects should be given the opportunity to object to the processing of their data for targeted purposes before the processing is initiated. 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.

46. With regard to Example 1, the targeter might consider its legitimate interest to be the economic interest of having an increased publicity for its goods through social media targeting. The social media provider could consider that its legitimate interest consists of making the social media service profitable by selling advertising space. Whether the targeter and the social media provider can rely upon Article 6(1)(f) GDPR as legal basis depends on whether all three cumulative conditions are met, as recently reiterated by the CJEU. Even if the targeter and the social media provider consider their economic interests to be legitimate, it does not necessarily mean that they will be able to actually rely on Article 6(1)(f) GDPR.

47. The second part of the balancing test entails that the joint controllers will need to establish that the processing is necessary to achieve those legitimate interests. "Necessary" requires a connection between the processing and the interests pursued. 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 interests 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.[53]

48. The third step in assessing whether the targeter and the social media provider can rely upon Article 6(1)(f) GDPR as legal basis for the processing of personal data, is the balancing exercise necessary to determine whether the legitimate interest at stake is overridden by the data subject's interests or fundamental rights and freedoms.[54]

[51] CJEU, Judgment in *Fashion ID*, 29 July 2019, C-40/17, para. 95 - ECLI:EU:C:2019:629.
[52] Idem, para 97.
[53] Article 29 Working Party Opinion 06/2014 on the concept of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP217, 9 April 2014, p. 29.
[54] When assessing the impact on the interests, fundamental rights and freedoms of the individual concerned, the following considerations are particularly relevant in the context of targeting directed to users of social media (i) the purposes of the targeting, (ii) the level of detail of the targeting criteria used (e.g., a broadly described cohort such as 'people with an interest in English literature', or more detailed criteria to allow segmentation and targeting on a more granular level), (iii) the type (and combination) of targeting criteria used (i.e. whether the

49. The outcome of the balancing exercise will also depend on the presence of additional controls and safeguards. 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. 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). If the balancing exercise points out that data subject's interests or fundamental rights and freedoms override the legitimate interest of the social media provider and the targeter, the use of Article 6(1)(f) is not possible.

50. For what concerns the consent lawful basis, the controller needs to keep in mind that there are clearly situations in which the processing would not be lawful without the valid consent of the individuals concerned (Article 6(1)(a) GDPR). For example, the WP29 has previously considered that it would be difficult for controllers to justify using legitimate interests as a legal basis for intrusive profiling and tracking practices for marketing or advertising purposes, for example those that involve tracking individuals across multiple websites, locations, devices, services or data-brokering.[55]

51. To be valid, the consent collected for the processing needs to fulfil the conditions laid out in Articles 4(11) and 7 GDPR. Generally speaking, 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. Consent must also be specific, informed and unambiguous and the data subject must be able to refuse or withdraw consent without detriment.[56]

52. Consent (Article 6(1)(a) GDPR) could be envisaged, provided that all the requirements for valid consent are met. The EDPB recalls that obtaining consent also does not negate or in any way diminish the controller's obligations to observe the principles of processing enshrined in the GDPR, especially Article 5 with regard to fairness, necessity and proportionality, as well as data quality. Even if the processing of personal data is based on consent of the data subject, this would not legitimize targeting which is disproportionate or unfair.[57]

53. Finally, the EDPB is of the opinion that the processing of personal data described in the Example 1 cannot be justified on the basis of Article 6(1)(b) by neither the social platform nor the targeter.[58]

---

targeting only focuses on a small aspect of the data subject, or is more comprehensive in nature), and (iv) the nature (sensitivity), volume and source of the data used in order to develop the targeting criteria. See Article 29 Working Party Opinion 06/2014 on the concept of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP217, 9 April 2014 https://ec.europa.eu/justice/Article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

[55] Article 29 Working Party, Opinion on profiling and automated decision making, WP 251, rev. 01, p. 15, see also Article 29 WP, Opinion on legitimate interest, p. 32 and 48: « Overall, there is an imbalance between the company's legitimate interest and the protection of users' fundamental rights and Article 7(f) should not be relied on as a legal ground for processing. Article 7(a) would be a more appropriate ground to be used, provided that the conditions for a valid consent are met ».

[56] See Article 29 Working Party, Guidelines on consent under Regulation 2016/679, WP259 rev.01.

[57] See Article 29 Working Party, Guidelines on consent under Regulation 2016/679, WP259 rev.01, p. 3-4.

[58] See Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, 8 October 2019, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf

5.2.2 Data provided by the user of the social media platform to the targeter

54. Targeting can also involve data provided by the data subject to the targeter, who then uses the data collected in order to target the data subject on social media. For example, "list-based" targeting occurs where a targeter uploads pre-existing lists of personal data (such as e-mail addresses or phone numbers) for the social media provider to match against the information on the platform. In this case, the social media provider compares the data uploaded by the targeter with user data that it already possesses, and any users that match are added to or excluded from the target audience (that is, the 'cluster' of persons to which the advertisement will be displayed on the social media platform). The social media provider may also allow the targeter to 'check' the list prior to finalising it, meaning that some processing takes place even before the audience has been created.

Example 2 :

Ms. Jones contacts Bank X to set up an appointment regarding a possible mortgage because she is buying a house. She contacts the bank via e-mail to set up the appointment. Following the appointment, Ms. Jones decides not to become a customer of the bank. The bank has nevertheless added the e-mail address of Ms. Jones to its customer e-mail database. 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.

Example 3 :

Mr. Lopez has been a customer at Bank X for almost a year. When he became a customer, he provided an e-mail address and was informed by Bank X, at the moment of collection, that: (a) his e-mail address would be used for advertising of offers linked to the bank services that he is already using; and (b) he may object to this processing at any time. The bank has added his e-mail address to its customer e-mail database. Afterwards, the bank uses its e-mail database to target its customers on the social media platform with the full range of financial services it has on offer.[59]

A. Roles

55. In these examples, the targeter, i.e. the bank, acts as a controller because it determines the purposes and means of the processing by actively collecting, processing and transmitting the personal data of the individuals concerned to the social media provider for advertising purposes. The social media provider, in turn, acts as a controller because it has taken the decision to use personal data acquired from the social media user (i.e. the e-mail address provided when setting up his or her account) in order to enable the targeter to display advertising to an audience of specific individuals.

56. Joint controllership exists in relation to the processing operations for which the social media provider and the targeter jointly determine the purposes and means, in this case, uploading unique identifiers

[59] In situations where e-mail addresses are used for direct marketing purposes controllers must also take into account the provisions of Article 13 ePrivacy Directive. The EDPB notes that in the situation where the advertisement would not be displayed on the social media platform, but would be directly sent via a push notification or a direct message to the data subject, Article 13 of the ePrivacy Directive would be applicable. However, in this specific example, consent would not be required, insofar as Article 13(2) states that the electronic contact details of an existing customer may be used by an entity for "*direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner*".

related to the intended audience, matching, selection of targeting criteria and subsequent display of the advertisement, as well as any reporting relating to the targeting campaign.[60]

57. In both examples the bank acts as the sole controller regarding the initial collection of the email address of Ms. Jones and Mr. Lopez respectively. The social media provider does not participate in any way to determine the means and purposes of this collection. The joint control begins with the transmission of the personal data and the collection of it by the social media provider and the following processing for the purpose of displaying targeted advertising (and until the deletion of the data).

58. The reason why the bank acts as sole controller when collecting the e-mail address from Ms. Jones and Mr. Lopez respectively, is because the collection of data occurs prior to (and is not inextricably linked to) the targeting campaign. Therefore, in this case one must distinguish between the initial set of processing operations for which only the bank is a controller and a subsequent processing for which joint control exists. The responsibility of the bank does not extend to operations occurring after the targeting and reporting has been completed and in which the targeter has not participated in the purposes and means and for which the social media provider acts as the sole controller.

B. Legal basis

59. In Example 2, Article 6(1)f GDPR does not provide an appropriate legal basis to justify the processing in this case, taking into account the context in which the personal data was provided. Indeed, Ms. Jones contacted the bank for the sole purpose of setting up an appointment, following which she communicated her intention not to make use of the services offered by the bank. Hence, one can consider that there is no reasonable expectation by Ms. Jones that her personal data shall be used for targeting purposes ('re-targeting'). Moreover, a compatibility test under Article 6(4) GDPR will lead to the outcome that this processing is not compatible with the purpose for which the personal data are initially collected.

60. In Example 3, the targeter might be able to rely on legitimate interest to justify the processing, taking into account inter alia that Mr. Lopez was: (a) informed of the fact that his e-mail address may be used for purposes of advertising via social media for services linked to the one used by the data subject; (b) the advertisement relates to services similar to those for Mr. Lopez is already a customer, and (c) Mr. Lopez was given the ability to object prior to the processing, at the moment where the personal data were collected by the bank. 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 Article 6 (1)(f). of GDPR.

[60] The determination of purposes and means of the processing of the targeter and social media provider is similar (albeit not identical) to Example 1. By uploading the list of email addresses and setting the additional targeting criteria, the targeter defines the criteria in accordance with which the targeting takes place and designates the categories of persons whose personal data is to be made use of. The social media provider likewise makes a determination as to whose personal data shall be processed, by allowing which categories of data shall be processed, which targeting criteria shall be offered and who shall have access (to what types of) personal data that is processed in the context of a particular targeting campaign. The shared purpose underlying these processing operations resembles the purpose identified in Example 1, namely the display a specific advertisement to a set of individuals (in this case: social media users) who make up the target audience.

5.3 Targeting on the basis of observed data

61. There are several ways in which social media providers may be able to observe the behaviour of its users. For example, observation is possible through the social media service itself or may also be possible on external websites by virtue of social plug-ins or pixels.

Example 4: Pixel-based targeting

Mr. Schmidt is browsing online in order to purchase a backpack. He visits the website "BestBags.com", views a number of items, but decides not to make a purchase. The operator of "BestBags.com" wishes to target social media users who have visited their website without making a purchase. To this end, it integrates a so-called "tracking pixel"[61] on its website, which is made available by the social media provider. After leaving the website of BestBags.com and logging into his social media account, Mr. Schmidt begins to see advertisement for the backpacks he was considering when browsing BestBags.com.

Example 5: Geo-targeting

Mrs. Michu has installed the application of a social media provider on her smartphone. She is walking around Paris during her holidays. The social media provider collects information regarding Mrs. Michu's whereabouts via the GPS functionalities of her smartphone on an ongoing basis[62], using the permissions that have been granted to the social media provider when the application was installed. Mrs. Michu is staying at a hotel that is located next to a pizzeria. The pizzeria uses the geo-targeting functionality offered by the social media provider to target individuals who are within 1km of its premises for the first time in the last 6 months. When opening the social media provider's application on her smartphone, Mrs. Michu sees an advertisement from the pizzeria, decides that she is hungry and buys a pizza via its website.

Example 6:

Mrs. Ghorbani creates an account on a social media platform. During the process of registration she is asked if she consents to the processing of her personal data to see targeted advertisement on her social media page, on the basis of data she directly provides to the social media provider (such as her age, sex and location), as well as on the basis of her activity on other websites outside of the social media platform using cookies. She is informed that this data will be collected via social media plug-ins or tracking pixels, the processes are clearly described to her, as well as the fact that targeting involves other entities who are jointly responsible for ensuring compliance with the GDPR. It is also explained to her that she can withdraw her consent at any time, and she is provided with a link to the privacy policy. Because Mrs. Ghorbani is interested in seeing targeted advertisement on her social media page, she gives her consent. No advertising cookies are placed or collected until Mrs. Ghorbani expresses here consent.

[61] Tracking pixels are comprised of small snippets of code that are integrated into the website of the targeter. When an individual accesses the targeter's website in their browser, the browser automatically sends a request to the social media provider's server to obtain the tracking pixel. Once the tracking pixel is downloaded, the social media provider is typically able to monitor the user's session (i.e. the individual's behaviour on the website(s) in question). The observed data can be used in order for example to add a social media user to a particular target audience.

[62] A social media provider may also be able to determine the whereabouts of their users on the basis of other data points, including IP address and WiFi information from mobile devices, or the user-derived data (e.g. if they place information about their location on the platform in a post).

Later on, she visits the website "Thelatesthotnews.com" that has a social media button integrated on it. A small but clearly visible banner appears on the right edge of the screen, asking Mrs. Ghorbani to consent to the transmission of her personal data to the social media provider using cookies and social media plug-ins. The website operator undertook technical measures so that no personal data is transferred to the social media platform until she gives her consent.

5.3.1 Roles

62. In Example 4, both the targeter and the social media provider participate in determining the purposes and means of the processing personal data, which results in the display of the advertisement to Mr. Schmidt.

63. As far as the determination of purpose is concerned, Bestbags.com and the social media provider jointly determine the purpose of the processing, which is to display a specific advertisement on the social media platform to the individuals who make up the target audience. By embedding the pixel into its website, Bestbags.com exerts a decisive influence over the means of the processing. The collection and transmission of the personal data of visitors of the website to the social media provider would not have occurred without the embedding of that pixel. The social media provider, on the other hand, has developed and offers the software code (pixel) that leads to the automatic collection, transmission and evaluation for marketing purposes of personal data to the social media provider. As a result, joint controllership exists in relation to the collection of personal data and its transmission by way of pixels, as well as in relation to the matching and subsequent display of the advertisement to Mr Schmidt on the social platform, and for any reporting relating to the targeting campaign. Joint controllership also exists, for similar reasons, in Example 6.

64. In Example 5, the pizzeria exercise a decisive influence over the processing of personal data by defining the parameters of the ad targeting in accordance with its business needs (for instance, opening hours of the pizzeria and geo-location of persons close to the pizzeria in this time-slot), and therefore must be regarded as taking part in the determination of the purposes and means of the data processing. The social media provider, on the other hand, has collected the information regarding Mrs. Michu's location (via GPS) for its purpose of enabling such location-based targeted advertising. As a result, joint control exists between the targeter and the social platform in relation to the collection and analysis of Mrs. Michu's location, as well as the display of the advertisement, in order to target her (as a person appearing within 1km of the pizzeria for the first time in the last 6 months) with the ad.

5.3.2 Legal basis

65. First of all, because Examples 4, 5 and 6 involve the use of cookies, requirements resulting from Article 5(3) of the ePrivacy Directive need to be taken into account.

66. In this regard, it should be noted that Article 5(3) of the ePrivacy Directive requires that users are provided with clear and comprehensive information, inter alia about the purposes of the processing, prior to giving their consent[63], subject to very narrow exceptions[64]. Clear and comprehensive information implies that a user is in a position to be able to determine easily the consequences of any consent he or she might give and ensure that the consent given is well informed.[65] As a result, the controller will have to inform data subjects about all the relevant purposes of the processing –

[63] Court of Justice of the European Union, Judgment in Planet 49 Gmbh, Case C-673/17, paragraph 73.
[64] See Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities. See also Court of Justice of the European Union, Judgment in Fashion ID, C-40/17, paragraphs 89-91.
[65] *Idem*, paragraph 74.

including any subsequent processing of the personal data obtained by accessing information in the terminal equipment.

67. To be valid, the consent collected for the implementation of tracking technologies needs to fulfil the conditions laid out in Article 7 GDPR.[66] For instance, consent is not validly constituted if the use of cookies is permitted by way of a checkbox pre-ticked by the service provider, which the user must deselect to refuse his or her consent.[67] Based on recital 32, 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 action: such actions may be difficult to distinguish from other activity or interaction by a user and therefore determining that an unambiguous consent has been obtained will also not be possible. Furthermore, in such a case, it will be difficult to provide a way for the user to withdraw consent in a manner that is as easy as granting it.[68]

68. Any (joint) controller seeking to rely on consent as a legal basis is responsible for ensuring valid consent is obtained. In *Fashion ID*, the CJEU emphasized the importance of ensuring the efficient and timely protection of the data subject rights, and that consent should not be given only to the joint controller that is involved later in the processing. Valid consent must be obtained prior to the processing, which implies that (joint) controllers need to assess when and how information should be provided and consent should be obtained. In other words, the question as to which of the joint controllers should be in charge of collecting the consent comes down to determining which of them is involved first with the data subject. In example 6, as the placement of cookies and processing of personal data occurs at the moment of account creation, the social media provider must collect her valid consent before the placement of advertisement cookies.

69. The EDPB also recalls that in a case where the consent sought is to be relied upon by multiple (joint) controllers or if the data is to be transferred to or processed by other controllers who wish to rely on the original consent, these organisations should all be named.[69] 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).

70. The EDPB emphasizes that the consent that should be collected by the website operator for the transmission of personal data triggered by its website (by embedding a social plug-in) relates only to the operation or set of operations involving the processing of personal data in respect of which the operator actually determines the purposes and means[70]. The collection of consent by a website operator, i.e. "Thelatesthotnews.com" in Example 6 for instance, does not negate or in any way diminish the obligation of the social media provider to ensure the data subject has provided a valid consent for the processing for which it is responsible as a joint controller[71], as well as for any subsequent or further processing it carries out for which the website operator does not jointly determine the purposes and means (e.g. subsequent profiling operations for targeting purposes).

[66] EDPB Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1, p. 6.
[67] Court of Justice of the European Union, Judgement in Planet 49, C-637/17, paragraph 57.
[68] EDPB Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1, p. 19.
[69] EDPB Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1, p. 16, paragraph 65.
[70] Judgment in *Fashion ID*, 29 July 2019, C-40/17, ECLI:EU:C:2019:629, paragraphs 100-101.
[71] This is all the more the case insofar as that for most targeting tools, it is the social media that carries out the read/write operations on the terminal of the user, because it collects the personal data for the purpose of targeted advertisement. Therefore, the social media provider is responsible for ensuring that valid consent is obtained.

71. In addition, any subsequent processing of personal data, including personal data obtained by cookies, social plug-ins or pixels, must also have a legal basis under Article 6 of the GDPR in order to be lawful.[72] For what concerns the legal basis of the processing in Examples 4, 5, and 6, the EDPB considers that legitimate interest cannot act as an appropriate legal basis, as the targeting relies on the monitoring of individuals' behavior across websites and locations using tracking technologies.[73]

72. Therefore, in such circumstances, the appropriate legal basis for any subsequent processing under Article 6 GDPR is also likely to be the consent of the data subject. Indeed, when assessing compliance with Article 6 GDPR, one should take into account that the processing as a whole involves specific activities for which the EU legislature has sought to provide additional protection.[74] Moreover, controllers must take into account the impact on data subjects' rights when identifying the appropriate legal basis in order to respect the principle of fairness.[75]

5.4 Targeting on the basis of inferred data

73. Inferred data refers to data which is created by the controller on the basis of the data provided by the data subject (regardless of whether these data were observed or actively provided by the data subject, or a combination thereof).[76] Inferences about data subjects can be made both by the social media provider and the targeter.

74. For example, by virtue of monitoring the behaviour of its users over a long period of time, both on and off the social media (e.g. pages visited, time spent on each page, number of reconnections to that page, words searched, hyperlinks followed, "likes" given), the social media provider may be able to infer information regarding the interests and other characteristics of the user of the social media. In the same vein, a targeter might also be able to infer data about specific individuals and use that knowledge when targeting him or her to display ads on his or her social media page.

Example 7:

Mrs. Delucca often "likes" photos posted by the Art Gallery "Beautifulart" by impressionist painter Pataolito on its social media page. Museum Z is looking to attract individuals who are interested in impressionist paintings in light of its upcoming exhibition. Museum Z uses the following targeting criteria offered by the social media provider: "interested in impressionism", gender, age and place of residence. Ms. Delucca subsequently receives targeted advertisement by Museum Z related to the upcoming exhibition of Museum Z on her social media page.

Example 8:

[72] Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, par. 41.

[73] Article 29 Working Party, Opinion on profiling and automated decision making, WP 251, rev. 01, p. 15, see also Article 29 WP, Opinion on legitimate interest, p. 32 and 48: «Overall, there is an imbalance between the company's legitimate interest and the protection of users' fundamental rights and Article 7(f) should not be relied on as a legal ground for processing. Article 7(a) would be a more appropriate ground to be used, provided that the conditions for a valid consent are met».

[74] Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, paragraph 41.

[75] European Data Protection Board, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, 8 October 2019, paragraph 1.

[76] See also Article 29 Data Protection Working Party, Guidelines on the right to data portability, WP 242 rev.01, 5 April 2017, p. 10.

Mr. Leon has indicated on his social media page that he is interested in sports. He has downloaded an application on his mobile phone to follow the latest results of his favorite sport games, has set on his browser the page www.livesportsresults.com as his homepage on his laptop, often uses his desktop computer at work to search for the latest sports results on the internet. He also visits a number of online gambling websites. The social media provider tracks Mr Leon' online activity across his multiple devices, i.e. his laptop, his cell mobile phone, and his desktop computer. Based on this activity and all the information provided by Mr. Leon, the social media provider infers that he will be interested in online betting. In addition, the social media platform has developed targeting criteria enabling companies to target people who are likely to be impulsive and have a lower income. The online betting company "bestpaydayloans" wishes to target users that are interested in betting and that are likely to be betting heavily. It therefore selects the criteria offered by the social media provider to target the audience to whom its advertisement should be displayed.

5.4.1 Roles

75. For what concerns the determination of the roles of the different actors, the EDPB notes the following: in Example 7, joint controllership exists between Museum Z and the social media provider concerning the processing of personal data for the purposes of 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 ("interested in impressionism") to the targeter fitting the purpose of finally displaying the advertisement.[77]

76. In Example 8, joint control exists between "bestpaydayloans" and the social media provider in relation to the processing operations jointly determined, in this case the selection of targeting criteria and subsequent display of the advertisement, as well as any reporting relating to the targeting campaign.

5.4.2 Legal basis

77. Targeting of social media users on the basis of inferred data for advertising purposes typically involves profiling[78]. The WP29 has previously clarified that according to the GDPR, profiling is an automated processing of personal data which aims at evaluating personal aspects, in particular to analyse or make predictions about individuals, adding that "*[t]he use of the word 'evaluating' suggests that profiling involves some form of assessment or judgement about a person*".[79] Profiling may be lawful by reference to any of the legal grounds in Article 6(1) GDPR, subject to the validity of this legal basis.

78. In Example 7, Article 5(3) of ePrivacy is applicable, insofar as the display of the advertisement on Mrs. Delucca's page related to the painter Pataolito requires a read/write operation to match this "like" with information previously held on her by the social media provider. Consent will therefore be required for these operations.

79. For what concerns Example 8, the EDPB recalls that in the case of automated decision-making which produces legal effects or similarly significantly affects the data subject, as set out in Article 22 GDPR data controllers may rely on the following exceptions:

- explicit consent of a data subject;

[77] As regards social media pages, joint controllership may also exist in relation to statistical information provided by the social media provider to the page administrator: see *Wirtschaftsakademie*.
[78] The EDPB notes that profiling may have occurred in previous examples as well.
[79] Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP251rev.01, p. 7.

- the necessity of the automated decision-making for entering into, or performance of, a contract; or
- authorisation by Union or Member State law to which the controller is subject.

80. WP29 has already stated that "*In many typical cases the decision to present targeted advertising based on profiling will not have a similarly significant effect on individuals (…). However, it is possible that it may do, depending upon the particular characteristics of the case, including:*

- *the intrusiveness of the profiling process, including the tracking of individuals across different websites, devices and services*;
- *the expectations and wishes of the individuals concerned;*
- *the way the advert is delivered; or*
- *using knowledge of the vulnerabilities of the data subjects targeted.*"[80]

Where the profiling undertaken by the social media provider is likely to have a "similarly significant [effect]" on a data subject, Article 22 shall be applicable. An assessment as to whether targeting will "similarly significantly [effect]" a data subject will need to be conducted by the controller (or joint controllers, as the case may be) in each instance with reference to the specific facts of the targeting.

81. In such circumstances as described in Example 8, the display of online betting advertisements may fall under the scope of Article 22 GDPR (targeting financially vulnerable persons that are interested in online betting which have the potential to significantly and adversely affect his financial situation). Therefore, in accordance with Article 22, explicit consent would be required. Furthermore, the use of tracking techniques triggers the applicability of Article 5(3) of the ePrivacy Directive, resulting in a requirement of prior consent. Finally, the EDPB recalls that for the processing to be lawful, the controller must conduct a case-by-case assessment, and that obtaining consent does not reduce other obligations to observe the requirements of fairness, necessity, proportionality and data quality, as stated in Article 5 GDPR.

6 TRANSPARENCY AND RIGHT OF ACCESS

82. Article 5(1)(a) GDPR states that personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. Article 5(1)(b) GDPR also states that personal data shall be collected for specified, explicit and legitimate purposes. Articles 12, 13 and 14 GDPR contain specific provisions on the transparency obligations of the data controller. Finally, recital 39 states that "*it should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed*".[81]

83. Information presented to data subjects in respect of the way in which their personal data are processed, should be, in all cases, concise, transparent, in an intelligible and easily accessible form, using clear and plain language.

[80] Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP251rev.01, p. 22.
[81] See also Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, WP260 rev.01, 11 April 2018, https://ec.europa.eu/newsroom/Article29/item-detail.cfm?item_id=622227

84. The EDPB recalls that the mere use of the word "advertising" would not be enough to inform the users that their activity is being monitored for the purpose of targeted advertising. It should be made transparent to individuals what types of processing activities are carried out and what this means for the data subject in practice. Data subjects should be informed in an easily understandable language if a profile will be built based on their online behaviour on the platform or on the targeter's website, respectively, by the social platform and by the targeter, providing information to the users on the types of personal data collected to build such profiles and ultimately allow targeting and behavioural advertising by targeters.[82] Users should be provided with the relevant information directly on the screen, interactively and, where appropriate or necessary, through layered notices.[83]

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

85. According to Article 26(1) GDPR, joint controllers "*shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects"*.

86. A further expression of the transparency principle is the obligation to make the essence of the joint controllership arrangement available to the data subject according to Article 26 (2) GDPR. Indeed, Article 26 GDPR requires joint controllers to take appropriate measures to ensure that data subjects are made aware of the allocation of responsibilities.

87. As a matter of principle, the information provided to the data subject must cover all aspects of the data processing operation(s) for which the joint controllers are jointly responsible. Indeed, the data subject is entitled to receive all information (including regarding envisaged subsequent processing where there is joint controllership) at the outset, so that the information is fair and appropriate. More precisely, this joint arrangement needs to ensure that the data subject will be provided information required by Articles 13 and 14 GDPR, including on their shared or closely linked purposes, storage periods, transmission to third parties etc., which need to be communicated to the data subject upon collection of the data or before the processing starts. The arrangement needs to make it clear where the responsibilities lie in this regard. To meet these requirements, such arrangement must contain (or reference) clear and comprehensive information in respect of the processing to which it relates with explanations, where appropriate, on the various phases and actors of the processing.[84]

88. Although both joint controllers are subject to the duty to inform where there is joint responsibility, they can mutually agree that one of them shall be tasked with providing the initial information to data subjects, especially in cases where only one of the controllers interacts with the users prior to processing, for example on its website[85]. This exchange of information to provide to the data subject should be an integral part of the joint arrangement (e.g. an appendix). 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

[82] Ref. to EDPB Guidelines on transparency under Regulation 2016/679.
[83] Article 29 Working Party, Guidelines on consent under Regulation 2016/679, WP259 rev. 01., para 24, 35.
[84] Opinion 1/2010 on the concepts of "controller" and "processor", WP 169, p. 28.
[85] CJEU *Fashion ID*, para 102, 105.

information to enable him to provide the data subject with full information in accordance with Articles 13 and 14 GDPR.

89. The EDPB notes that controllers are not directly responsible for providing the information required by Articles 13 and 14 GDPR in relation to further processing operations that do not fall under the scope of joint controllership. Therefore, the targeter is not directly responsible for providing the information relating to any further processing which will be carried out by the social media platform.

90. However, the EDPB emphasizes that the joint controller who intends to further use the personal data has specific obligations of information for this further processing where there is no joint responsibility, according to Article 14(4) of the GDPR, as well as obligations of compatibility of the further processing under Article 6(4).For example, the targeter and social media provider could agree that the targeter will provide certain information on behalf of the social media provider. The social media provider, however, remains ultimately responsible for ensuring that the data subject has been provided with the relevant information in relation to all the processing activities under its control.

> In Example 3 (Mr. Lopez being targeted for advertisement for Bank X on his social media page following the upload by the Bank of his email address to the social media provider), the Bank needs to inform Mr. Lopez that his email address will be used for advertising, via the social media provider, of offers linked to the bank services. Any further processing by the social media provider must be lawful and compatible with the purposes for which the Bank collected the data.
>
> In addition, to the extent that the social media provider intends to further process Mr. Lopez's email for another purpose, it must ensure that Mr. Lopez is provided with the information required by Article 14(4) GDPR prior to doing so.
>
> The social media provider and the Bank may agree that the Bank will provide Mr. Lopez with the relevant information on behalf of the social media provider. Even if that is the case, however, the social media provider remains ultimately responsible for ensuring that the data subject has been provided with the relevant information in relation to all the processing activities for which it is (alone) responsible. This obligation would not apply if Mr. Lopez has already been informed by the Bank of this processing, according to Article 14(5)(a) GDPR.
>
> These transparency obligations are to be considered without prejudice of the specific obligations applicable to legal basis considerations.

91. Each joint controller is responsible for ensuring that that the essence of the arrangement 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?".

6.2 Right of access (Article 15)

92. Data controllers must enable users to easily and fully exercise their data subjects' rights. An easy-to-use and efficient tool should be available for the data subject to ensure the easy exercise of all of their rights, at any time, in particular the right of erasure, objection, and the right of access pursuant to

Article 15 GDPR.[86] The following paragraphs focus on how and by whom the right of access should be accommodated in the context of targeting of social media users.[87]

93. In general, to fulfill the requirements of Article 15 (1) GDPR and to ensure full transparency, controllers may want to consider implementing a mechanism for data subjects to check their profile, including details of the information and sources used to develop it. The data subject is entitled to learn of the identity of the targeter, and controllers must facilitate access to information regarding the targeting, including the targeting criteria that were used, as well as the other information required by Article 15 GDPR.

94. As regards the kind of access to be provided to data subjects, recital 63 advises that *"[w]here possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data*." The specific features of social media providers - the online environment, the existence of a user account - suggest the possibility to easily grant the data subject with remote access to the personal data concerning him or her in accordance with Article 15 (1), (2) GDPR. Remote access in this case can be regarded as the most "appropriate measure" in the sense of Article 12(1) GDPR, also taking into account the fact that this is a typical situation "where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected" (see recital 58, which explicitly adds "online advertising" as concrete example). In addition, if requested, social media users who have been targeted should also be given a copy of the personal data relating to them in accordance with Article 15(3) GDPR.

95. According to Article 15(1)(c) GDPR, the user shall have access in particular to information on "*the recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations*". According to Article 4(9), the term "recipient" refers to a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether they are a third party or not. A targeter will not necessarily be a "recipient" of the personal data (see Example 1), as the personal data might not be disclosed to it, but it will receive statistics of the targeted customers in aggregated or anonymised form, e.g. as part of its campaign, or in a performance review of the same. Nevertheless, to the extent that the targeter acts as a joint controller, it must be identified as such to the social media user.

96. Although Article 15 GDPR is not explicitly identified in Article 26(1) GDPR, the wording of this Article refers to all "responsibilities for compliance" under GDPR, which includes Article 15 GDPR.

97. In order to enable data subjects to exercise their rights in an effective and easily accessible way, the arrangement between the social media provider and the targeter may designate a single point of contact for data subjects. Joint controllers are in principle free to determine amongst themselves who should be in charge of responding to and complying with data subject requests, but they cannot exclude the possibility for the data subject to exercise his or her rights in respect of and against each of them (Article 26 (3) of the GDPR). Hence, targeters and social media providers must ensure that a suitable mechanism is in place to allow the data subjects to obtain access to his or her personal data in a user-friendly manner (including the targeting criteria used) and all information required by Article 15 of the GDPR.

[86] Article 15 (1), (2) GDPR detail the information to be given to the data subject asking for access to her data. Article 15 (3), (4) GDPR regulate the right to obtain a copy.

[87] See EDPB, Guidelines on transparency under Regulation 2016/679, p. 35.

7 DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

98. In principle, prior to initiating the envisaged targeting operations, both joint controllers should check the list of processing operations "likely to result in a high risk" adopted at national level under Article 35(4) and recitals (71), (75) and (91) GDPR to determine if the designated targeting matches any of the types of processing operations subject to the requirement to conduct a DPIA. To assess whether the envisaged targeting operations are "likely to result in a high risk" and whether a DPIA is required, the criteria identified in the guidelines on DPIA should also be taken into account[88], as well as the lists that supervisory authorities have established of the kind of processing operations which are subject to the requirement for a data protection impact assessment (pursuant to article 35(4)).

99. In some cases, the nature of the product or service advertised, the content of the message or the way the advert is delivered might produce effects on individuals whose impact has to be further assessed. This might be the case, for example, with products which are targeted at vulnerable people. Additional risks may emerge depending on the purposes of the advertising campaign and its intrusiveness, or if the targeting involves the processing of observed, inferred or derived personal data.

100. In addition to the obligations specifically referred in Article 26 (1) GDPR, joint controllers should also consider other obligations when determining their respective obligations. As stated in the EDPB guidelines on DPIAs "When the processing operation involves joint controllers, they need to define their respective obligations precisely".

101. As a consequence, both joint controllers need to assess whether a DPIA is necessary. If a DPIA is necessary, they are both responsible for fulfilling this obligation. The EDPB recalls that the DPIA should tackle the entire processing of personal data, which means that in principle both joint controllers need to take part in the realization of the DPIA. 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".[89]

102. In practice, it is possible that joint controllers decide that one of them shall be tasked with carrying carries out the DPIA as such. This should then be specified in the joint arrangement, without prejudice to the existence of joint responsibility as such. It may indeed be that one of the controllers is better placed to assess certain processing operations. For example, this controller may, depending on the context, be the one with a higher degree of control and knowledge of the targeting process in particular on the back-end of the deployed system, or on the means of the processing.

103. Every DPIA must include measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data, and to demonstrate compliance with the GDPR taking into account the rights and legitimate interests of data subjects and other persons concerned. If the identified risks cannot be sufficiently addressed (i.e. the residual risks remain high), the joint controllers are each responsible for ensuring a prior consultation with the relevant supervisory authorities. If the targeting would infringe the GDPR, in particular because the risks have insufficiently been identified or mitigated, the targeting should not take place.

[88] See EDPB Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, wp248rev.0.
[89] *Idem*, page 8.

Example 9:

The political party "Letschangetheworld" wishes to encourage social media users to vote for a particular political candidate in the upcoming elections. They wish to target elderly people living in rural areas of the country, who regularly go to Church, and who have not travelled abroad in the past 2 years.

104. There is joint controllership between the social media platform and the political party, for the matching of the profile and the display of the targeted advertisement. The assessment of whether a DPIA is required needs to be carried out both by the Letschangetheworld political party and the social media platform. Indeed, in this example, they both have sufficient knowledge on the criteria that are being used to target the individuals in order to see that the processing is likely to result in a high risk.

105. If a DPIA is necessary, the joint arrangement should address the question of how the controllers should carry it and ensure that a relevant exchange of knowledge takes place. In this example, it may be that the social media platform is better placed to assess certain processing operations, insofar as the political party merely selects general targeting criteria.

8 SPECIAL CATEGORIES OF DATA

8.1 What constitutes a special category of data

106. The GDPR provides specific protection for personal data that are particularly sensitive in relation to individuals' fundamental rights and freedoms. Such data are defined in Article 9 GDPR as special categories of personal data and include data about an individual's health, racial or ethnic origin, biometry, religious or philosophical belief, political opinion, trade union membership, sex life or sexual orientation.

107. Controllers may only process special categories of data if they can meet one of the conditions set out in Article 9(2) GDPR, such as having obtained the data subject's explicit consent or the data have been manifestly made public by the data subject. In addition to the conditions in Article 9, processing of special categories of data must rely on a legal basis laid down in Article 6 and be carried out in accordance with the fundamental principles set out in Article 5.

108. Furthermore, the processing of special categories of personal data is relevant when assessing appropriate measures according to Articles 24, 25, 28 and 32 GDPR, but also to determine whether a DPIA must be carried out according to Article 35 GDPR, and whether a data protection officer must be appointed under Article 37 GDPR.

109. In the context of social media and targeting, it is necessary to determine whether the processing of personal data involves "special categories of data" and if such data are processed by the social media provider, the targeter or both. If special categories of personal data are processed, it must be determined whether and under what conditions the social media provider and the targeter can lawfully process such data.

110. If the social media provider processes the special category of data for targeting purposes, it must find a legal basis for the processing in Article 6 GDPR and rely on an exemption in Article 9(2) GDPR, such as explicit consent according to Article 9(2)(a) GDPR. If a targeter engages a social media provider and requests that the social media provider targets users based on this special category of data, the

targeter will be jointly responsible with the social media provider for the processing of the special category data.

111. The following legal analysis will explore different situations when such processing may take place and their legal implications.

8.1.1 Explicit special categories of data

112. At times, personal data being processed clearly falls within the definition of special categories of data, e.g. in case of a direct statement about a person being member of a certain political party or religious association.

> Example 10:
>
> Ms. Flora states explicitly in her social media profile that she is a member of the GreenestPlanet political Party. The environmental organisation "Long live the Earth" wants to target social media users that are members of the GreenestPlanet political party in order to address targeted messages to them.

113. In Example 10, the social media provider and the environmental organisation are acting as joint controllers.[90] Insofar as the environmental organisation requests the social media provider to target users based on their political opinion, both controllers contribute to the processing of special categories of data as defined by Article 9 GDPR. Processing of these data are in principle prohibited according to Article 9(1). Both the social media provider and the environmental organisation must therefore be able to rely on one of the exemptions in Article 9(2) for their processing. In addition to that, they must also both have a legal basis according to Article 6. Out of the exemptions in Article 9(2), it appears that the only applicable exemptions in this situation would be to obtain the data subject's explicit consent, under Article 9(2)(a) GDPR, or the exemption that Ms. Flora manifestly made the personal data public, under Article 9 (2)GDPR.

8.1.2 Inferred and combined special categories of data

114. Assumptions or inferences regarding special category data, for instance that a person is likely to vote for a certain party after visiting a page preaching liberal opinions, would also constitute a special category of personal data. Likewise, as previously stated by the EDPB, "*profiling can create special category of data by inference from data which is not special category of data in its own right, but becomes so when combined with other data. For example, it may be possible to infer someone's state of health from the records of their food shopping combined with data on the quality and energy content of foods".* [91]

115. For instance, the processing of a mere statement, or a single piece of location data or similar, which reveals that a user has (either once or on a few occasions) visited a place typically visited by people with certain religious beliefs will generally not in and of itself be considered as processing of special categories of data. However, it may be considered as processing of special categories of data if these data are combined with other data or because of the context in which the data are processed or the purposes for which they are being used.

> Example 11:
>
> The profile on Mr. Novak's social media account only reveals general information such as his name and domicile, but a status update reveals that he has visited the City Church frequently where he attended

[90] See the analysis in chapter 5.2.1.

[91] Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP251rev.01, page 15.

a religious service. Later on, the City Church wants to target its visitors with religious messages in order to encourage Christian people to join the congregation. In such circumstances, the use of personal data in Mr. Novak's status update for such a targeting purposes amounts to the processing of special categories of personal data.

116. If a social media provider or a targeter uses observed data to categorise users as having certain religious, philosophical or political beliefs - regardless of whether the categorization is correct/true or not - this categorisation of the user must obviously be seen as processing of special category of personal data in this context. As long as the categorisation enables targeting based on special category data, it does not matter how the category is labelled.

Example 12:

Mr. Sifuentes provides information in his social media profile in the shape of regular status updates, check-ins, etc., which indicate that he regularly takes part in activities arranged by the "Mind, Body and Spirit Movement". Even though no explicit statement on philosophical belief is provided, all updates, likes, check-ins and similar data provided by the user when collated, strongly indicate that Mr. Sifuentes has a certain philosophical belief.

Example 13:

A social media provider uses information actively provided by Ms. Allgrove on her social media profile page about her age, interests and address and combines it with observed data about the websites visited by her and her "likes" on the social media platform. The social media provider uses the data to infer that Ms. Allgrove is a supporter of left-wing liberal politics and places her in the "interested in left wing liberal politics" targeting category, and makes this category available to targeters for targeted advertising.

117. In Example 12, the vast information and the absence of measures to prevent targeting based on special category data implies that a processing of special categories of data is taking place. However, the mere fact that a social media provider processes large amounts of data which potentially could be used to infer special categories of data does not automatically mean that the processing falls under Article 9 GDPR. Article 9 will not be triggered if the social media provider's processing does not result in inference of special categories of data and the social media provider has taken measures to prevent that such data can be inferred or used for targeting. In any case, processing of a large amount of personal data about users may entail specific risks for the rights and freedoms of natural persons, which have to be addressed by implementing appropriate security measures, as prescribed under Article 32, and also by taking into account the outcome of the DPIA to be performed pursuant to Article 35 of the GDPR.

118. In Example 13, the offering as well as use of the targeting category "interested in left wing liberal politics" amounts to processing of special categories of data, as this category could easily be used as a proxy to target individuals who have left wing liberal political beliefs. By assigning an inferred political opinion to a user, the social media provider processes special categories of data. For the purpose of Article 9 GDPR, it is not relevant whether the user in fact is a supporter of left-wing liberal politics. Nor is it relevant that the targeting category is named "interested in…" and not "supporter of…", since the user is placed in the targeting category based on inferred political interests.

Example 14:

Mr. Svenson takes a career aptitude test developed, containing a psychological evaluation, by the company "YourPerfectJob" which is made available on a social media platform and makes use of the Application Programming Interface (API) provided by the social media provider. YourPerfectJob collects data about Mr. Svenson's education, employment status, age, hobbies, posts, email-address and connections. YourPerfectJob obtains the data through the API in accordance with the "permissions" granted by Mr. Svenson through his social media account. The stated purpose of the application is to predict what would be the best career path for a specific user.

Without the knowledge or approval of the social media provider, YourPerfectJob uses this information to infer a number of personal aspects, including his personality traits, psychological profile and political beliefs. YourPerfectJob later decides to use this information to target Mr. Svenson on behalf of a political party, using of the email-based targeting feature of the social media provider, without adding any other targeting criteria offered by the social media provider.

In Example 14, the targeter processes special categories of personal data, whereas the social media provider does not. Indeed, the assessment and identification of Mr. Svenson's political belief occurs without the involvement of the social media provider.[92] In addition to triggering the general prohibition of Article 9 GDPR, the targeting mentioned in Example 14 also constitutes an infringement of the requirements concerning fairness, transparency and purpose limitation. Indeed, Mr. Svenson is not properly informed of the fact that the personal relating to him will be processed for political targeting, which in addition, does not seem compatible with a career aptitude test.

119. While processing activities of the social media provider in Example 14 do not amount to processing of special categories of data within the meaning of Article 9 GDPR, the social media provider is responsible for integrating the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects in accordance with Article 24 and 25 GDPR.

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

120. Article 9(2)(e) of the GDPR allows processing of special category of data in cases where the data have been manifestly made public by the data subject. The word "manifestly" implies that there must be a high threshold for relying on this exemption. The EDPB notes that the presence of a single element may not always be sufficient to establish that the data have been "manifestly" made public by the data subject. In practice, a combination of the following or other elements may need to be considered for controllers to demonstrate that the data subject has clearly manifested the intention to make the data public, and a case-by-case assessment is needed. The following elements may be relevant to help inform this assessment:

[92] In Example 14, there is no joint controllership between the social media provider and YourPerfectJob at the moment of collection of personal data, because they do not jointly determine the purposes of the collection and subsequent or further processing of personal data for the purposes of Yourperfectjob at this stage of the processing. The EDPB would like to recall that the analysis on the roles and responsibilities needs to be done on a case by case basis, and that the conclusion on this specific example is without prejudice of any further work that can be carried out by the EDPB on APIs. The situation would of course be different if the social media provider, in addition to making the personal data available, also participated in the determination of purpose pursued by YourPerfectJob. In any event, joint controllership still exists between the targeter and the social media provider as regards the use of list-based targeting.

(i) the default settings of the social media platform (i.e. whether the data subject took a specific action to change these default private settings into public ones); or

(ii) the nature of the social media platform (i.e. whether this platform is intrinsically linked with the idea of connecting with close acquaintances of the data subject or creating intimate relations (such as online dating platforms), or if it is meant to provide a wider scope of interpersonal relations, such as professional relations, or microblogging, media sharing, social platforms to share online reviews, etc… ; or

(iii) the accessibility of the page where the sensitive data is published (i.e. whether the information is publically accessible or if, for instance, the creation of an account is necessary before accessing the information); or

(iv) the visibility of the information where the data subject is informed of the public nature of the information that they publish (i.e. whether there is for example a continuous banner on the page, or whether the button for publishing informs the data subject that the information will be made public…); or

(v) if the data subject has published the sensitive data himself/herself, or whether instead the data has been published by a third party (e.g. a photo published by a friend which reveals sensitive data) or inferred.

The EDPB notes that the presence of a single element may not always be sufficient to establish that the data have been "manifestly" made public by the data subject. In practice, a combination of these or other elements may need to be considered for controllers to demonstrate that the data subject has clearly manifested the intention to make the data public.

Example 15:

Mr. Jansen has opened an account on a microblogging social media platform. While completing his profile, he indicated that he is homosexual. Being a conservative, he chose to join conservative groups, knowing that he has been informed while subscribing that the messages he exchanges on the platform are public. A conservative political party wishes to target people who share the same political affiliations and sexual orientation as Mr. Jansen using the social media targeting tools.

121. Because members' sexual orientation is by default "private" and that Mr. Jansen has not taken any step to make it public, it cannot be considered as having been manifestly made public. In addition, the data relating to his political affiliation has not been made manifestly public, despite of (i) the nature of the microblogging social media platform, which is meant to share information with the wide public, and (ii) the fact that he has been informed of the public nature of the messages he publishes on the forums. In addition, although he has joined public forums relating to conservatism, he cannot be targeted on the basis of this sensitive data, because it is the social media platform that makes a deduction on Mr. Janssen's political affiliation, and it was not the specific intention of the data subject to make this data manifestly public, all the more that this deduction may turn out to be false. He cannot therefore be targeted on the basis of political affiliation data. In other words, the circumstances in each specific case have to be taken into account when assessing whether the data have manifestly been made public by the data subject.[93]

[93] The WP29 clarified in its Opinion on some key issues of the Law Enforcement Directive (WP 258, 29/11/2017, p. 10) that the expression "manifestly made public by the data subject" has to be interpreted to imply that the data subject was aware that the respective data will be publicly available which means to everyone, including authorities"; therefore, "[i]n case of doubt, a narrow interpretation should be applied…"

9 JOINT CONTROLLERSHIP AND RESPONSIBILITY

9.1 Joint controller arrangement and determination of responsibilities (Art. 26 GDPR)

122. Article 26 (1) GDPR requires joint controllers to determine – in a transparent manner – their respective responsibilities for compliance with the obligations of the GDPR in an arrangement, including, as explained above, the requirements for transparency.

123. In terms of scope, the EDPB considers that the arrangement between targeters and social media providers should encompass all processing operations for which they are jointly responsible (i.e. which are under their joint control). By concluding an arrangement that is only superficial and incomplete, targeters and social media providers would be breach of non-compliance with their obligations under Article 26 of the GDPR.

> For instance, in Example 4 the arrangement should cover the entire processing of personal data where there is joint controllership, i.e. from the collection of personal data in the context of the visit by Mr. Schmidt of the website "BestBags.com" with a tracking pixel, to the display of the advertisement on his social media page, as well as any eventual reporting relating to the targeting campaign.

124. In order to develop a comprehensive arrangement, both the social media provider and the targeter must be aware of and have sufficiently detailed information regarding the specific data processing operations taking place. The arrangement between the targeter and the social media provider should therefore contain (or refer to) all necessary information to enable both parties to comply with their obligations under the GDPR, including their duty to comply with the principles under Article 5(1) GDPR and their duty to demonstrate their compliance according to Article 5(2) GDPR.

125. If, for example, the controller is considering to rely on Article 6(1)(f) GDPR as a legal basis, it is necessary, among other things, to know the extent of the data processing in order to be able to assess whether the interest of the controller(s) are overridden by the interests or fundamental rights and freedoms of the data subjects. Without sufficient information concerning the processing, such an assessment cannot be performed. The importance of including or referencing the necessary information in the context of a joint arrangement cannot be overstated, especially in situations where one of the parties almost exclusive has the knowledge and access to the information necessary for both parties to comply with the GDPR.

> For instance, in Example 1, when Company X is assessing whether it can rely on the legitimate interest as a legal basis to target men between the age of 30 and 45 and who have indicated that they are single, it is necessary that it has access to sufficient information concerning the processing carried out by the social media platform, including for instance for what concerns the additional measures (such as the right to prior objection) put into place by the latter, to ensure that legitimate interests are not overridden by the data subject's interests or fundamental rights and freedoms.

126. In order to ensure that the rights of the data subject can be accommodated effectively, the EDPB takes the view that the purpose of the processing and the corresponding legal basis should be also reflected in the joint arrangement between targeters and social media providers who are joint controllers. Although the GDPR does not preclude joint controllers to use different legal basis for different processing operations they carry out, it is recommended to use, whenever possible, the same legal

basis for a particular targeting tool and for a particular purpose. Indeed, if each stage of the processing is processed on a different legal basis, this would render the exercise of rights impracticable for the data subject (e.g. for one stage there would be a right to data portability, for another there would be a right of objection).

As controllers the targeter and the social media provider are both responsible for ensuring that the principle of purpose limitation is complied with and should therefore incorporate appropriate provisions to that end within the joint arrangement.

> For example, if the targeter wishes to use personal data provided to it by the data subject in order to target on social media, it must take appropriate measures to ensure that the data provided shall not be further used by the social media provider in a manner that is incompatible with those purposes, unless the valid consent of the data subject has been obtained pursuant to Article 6(4) of the GDPR.
>
> In Example 3, the Bank X should ensure that there are appropriate provisions in the joint arrangement with the social media platform that Mr. Lopez' email address is not used for other purposes that advertising of offers linked to the bank services that he is already using without Mr. Lopez' consent.
>
> Likewise, the social media provider must ensure that use of data for targeting purposes by the targeters is in compliance with the principles of purpose limitation, transparency and lawfulness.

127. Other obligations that should be considered by the targeter and social media provider in the context of their joint arrangement include: other general data protection principles contained in Article 5 GDPR, security of processing, data protection by design and by default, notifications and communications of personal data breaches, data protection impact assessments, the use of processors and transfers to third countries.

> For instance, in Example 13, the joint arrangement should address the question of which of the controllers should carry a DPIA and ensure that a relevant exchange of knowledge takes place. In other words, the political party "Letschangetheworld" should ensure that it has a sufficient level of information, for instance on the security measures put into place by the social media platform, when a DPIA is carried out.

128. Finally, the joint arrangement between the social media provider and the targeter must contain specific information about how the obligations under the GDPR shall be fulfilled in practice. 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. Moreover, in such cases, both (joint) controllers will not have implemented appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR and therefore will have breached their obligations under Articles 5(2) and 24.

9.2 Levels of responsibility

129. The EDPB observes that targeters who wish to use targeting tools provided by a social media provider may be confronted with the need to adhere to pre-defined arrangements, without any possibility to negotiate or make modifications ('take it or leave it' conditions). The EDPB considers that such a

situation does not negate the joint responsibility of the social media provider and the targeter and cannot serve to exempt either party from its obligations under the GDPR. Both parties to the joint arrangement are also bound to ensure that the allocation of responsibilities duly reflects their respective roles and relationships vis-à-vis data the subjects in a practical, truthful and transparent manner.

130. It is important to stress that an arrangement pursuant to Article 26 GDPR cannot override the legal obligations incumbent upon a (joint) controller. While joint controllers shall, in accordance with Article 26 GDPR "*determine their respective responsibilities for compliance*" with the GDPR, each controller remains, as a matter of principle, responsible for the compliance of processing. This means that each controller is – *inter alia* – responsible for compliance with the principles set out under Article 5(1) GDPR, including the principle of lawfulness established under Article 5(1)(a) of the GDPR.

131. However, the degree of responsibility of the targeter and of the social media provider in relation to specific obligations may vary. In *Wirtschaftsakademie*, the CJEU noted that "*the existence of joint responsibility does not necessarily imply equal responsibility of the various operators involved in the processing of personal data. […] those operators may be involved at different stages of that processing of personal data and to different degrees, so that the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case"*. [94]

132. In other words, although joint controllers are both responsible for complying with the obligations under the GDPR, and although the data subject may exercise his or her rights as against each of the controllers, their level of responsibility must be assessed on their actual role in the processing. In *Google Spain*, the CJEU clarified that a controller must ensure, "*within the framework of its responsibilities, powers and capabilities*", that the processing of personal data meets the requirements of EU data protection law.[95]

133. When it comes to assessing the level of responsibility of targeters and social media providers, several factors may be relevant, such as the ability to influence the processing on a practical level, as well as the actual or constructive knowledge of each of the joint controllers. It is also important to be clear at what stage of the processing and to what extent or degree the targeter and the social media provider are responsible for the processing.

In Example 1, Company X sets up an advertising campaign so that users corresponding to specific targeting criteria may be shown advertisements for the company on the social media platform. However, although it sets the parameters for the advertising campaign, it does not collect or have access to any personal data, nor does it have any direct contact with the data subject. Each of these elements may be relevant when assessing the level (or "degree") or responsibility of the targeter and social media provider in case a violation of the GDPR is established (e.g. in case of lack of transparency towards the data subject or failure to ensure lawfulness of processing). As indicated earlier, notwithstanding, both parties are obliged to undertake appropriate measures in order to meet the requirements of the GDPR and protect the rights of data subjects against unlawful forms of processing.

In Example 3, which involved list-based targeting, the situation is slightly different than Example 1. In Example 3, the bank initially collected the personal data and shared it with the social media provider for targeting purposes. In that case, the targeter has voluntarily caused the collection and transmission stage of the data processing. Each of these elements should be taken into account

[94] CJEU judgment of 05 June 2018, Wirtschaftsakademie, C-210/16, para. 43.
[95] See also CJEU, C-131/12, Google Spain ("responsibilities, powers and capabilities").

when assessing the level of responsibility of each actor and should be duly reflected in the terms of the joint arrangement.

Similarly, in Example 4, in case of pixel-based targeting, it should be taken into account that the website operator enables the transmission of personal data to the social media provider. It is indeed the website "BestBags.com" that integrates a tracking pixel on its website so that it can target Mr Schmidt, although he has decided not to make a purchase[96]. The website is therefore actively involved in the collection and transmission of the data. As a joint controller, however, the social media provider is also under an obligation to undertake appropriate measures to meet the requirements of the GDPR and protect the rights of data subjects against unlawful forms of processing. In this case, if the data subject's consent is sought, the joint controllers should agree upon the way in which consent is collected in practice.

134. When it comes to assessing the level of responsibility of social media provider, the EDPB observes that several targeting mechanisms rely on profiling and/or other processing activities previously undertaken by the social media provider. It is the social media provider who decides to process personal data of its users in such a manner to develop the targeting criteria which it makes available to targeters. In order to do so, the social media provider has independently made certain decisions regarding the processing, such as which categories of data shall be processed, which targeting criteria shall be offered and who shall have access (to what types of) personal data that is processed in the context of a particular targeting campaign. Such processing activities must also comply with the GDPR, prior to the offering of any targeting services.

135. The examples mentioned in the preceding paragraphs indicate the importance of clearly allocating responsibilities in the joint controller arrangement between social media providers and targeters. Even though the terms of the arrangement should in any case mirror the level of responsibility of each actor, a comprehensive arrangement which duly reflects the role and capabilities of each party is necessary not only to comply with Article 26 of the GDPR, but also for complying with other rules and principles of the GDPR.

136. Finally, the EDPB notes that insofar as the terms of the joint arrangement between the social media provider and the targeter do not bind supervisory authorities, supervisory authorities may exercise their competences and powers in relation to either joint controller, as long as the joint controller in question is subject to the competence of that supervisory authority.

[96] In addition, as BestBags.com has integrated the social media tracking pixel on its website, it is also responsible for complying with ePrivacy requirements regarding this tool, which, given that the pixel also facilitates the processing of personal data, is also of importance when determining the level of responsibility.