

Opinion of the Board (Art. 64)



Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms

Adopted on 17 April 2024

Executive summary

The Dutch, Norwegian and German (Hamburg) supervisory authorities requested the EDPB to issue an opinion on the question of under which circumstances and conditions 'consent or pay' models relating to behavioural advertising can be implemented by large online platforms in a way that constitutes valid, and in particular freely given, consent, also taking into account the judgment of the Court of Justice of the European Union (CJEU) in C-252/21. The scope of this opinion is indeed limited to the implementation by large online platforms (which are defined for the purposes of this opinion) of 'consent or pay' models where users are asked to consent to processing for the purposes of behavioural advertising.

In this respect, the EDPB highlights the need to comply with all the requirements of the GDPR, in particular those for valid consent, while assessing the specificities of each case. Of particular importance is the principle of accountability. The EDPB recalls that obtaining consent does not absolve the controller from adhering to all the principles outlined in Article 5 GDPR, as well as the other GDPR obligations. It is key to comply with the principles of necessity and proportionality, purpose limitation, data minimisation, and fairness.

In most cases, it will not be possible for large online platforms to comply with the requirements for valid consent if they confront users only with a binary choice between consenting to processing of personal data for behavioural advertising purposes and paying a fee.

The offering of (only) a paid alternative to the service which includes processing for behavioural advertising purposes should not be the default way forward for controllers. When developing the alternative to the version of the service with behavioural advertising, large online platforms should consider providing data subjects with an 'equivalent alternative' that does not entail the payment of a fee. If controllers choose to charge a fee for access to the 'equivalent alternative', controllers should consider also offering a further alternative, free of charge, without behavioural advertising, e.g. with a form of advertising involving the processing of less (or no) personal data. This is a particularly important factor in the assessment of certain criteria for valid consent under the GDPR. In most cases, whether a further alternative without behavioural advertising is offered by the controller, free of charge, will have a substantial impact on the assessment of the validity of consent, in particular with regard to the detriment aspect.

With respect to the requirements of the GDPR for valid consent, first of all, consent needs to be 'freely given'. In order to avoid detriment that would exclude freely given consent, any fee imposed cannot be such as to effectively inhibit data subjects from making a free choice. Furthermore, detriment may arise where non-consenting data subjects do not pay a fee and thus face exclusion from the service, especially in cases where the service has a prominent role, or is decisive for participation in social life or access to professional networks, even more so in the presence of lock-in or network effects. As a result, detriment is likely to occur when large online platforms use a 'consent or pay' model to obtain consent for the processing.

Controllers also need to evaluate, on a case-by-case basis, whether there is an imbalance of power between the data subject and the controller. The factors to be assessed include the position of the large online platform in the market, the existence of lock-in or network effects, the extent to which the data subject relies on the service and the main audience of the service.

The element of conditionality, i.e. whether consent is required to access goods or services, even though the processing is not necessary for the fulfilment of the contract, is another criterion to

evaluate whether consent is 'freely given'. The CJEU has stated in the *Bundeskartellamt* judgment that users who refuse to give consent to particular processing operations are to be offered, 'if necessary for an appropriate fee, an equivalent alternative not accompanied by such processing operations'. In doing so, controllers will avoid an issue of conditionality. In any case, the other criteria for 'freely given' consent still need to be fulfilled as well.

An 'equivalent alternative' refers to an alternative version of the service offered by the same controller that does not involve consenting to the processing of personal data for behavioural advertising purposes. The Opinion provides elements that can help ensuring the alternative is genuinely equivalent. If the alternative version is different only to the extent necessary as a consequence of the controller not being able to process personal data for behavioural advertising purposes, it can be in principle regarded as equivalent.

In respect of the imposition of a fee to access the 'equivalent alternative' version of the service, the EDPB recalls that personal data cannot be considered as a tradeable commodity, and controllers should bear in mind the need of preventing the fundamental right to data protection from being transformed into a feature that data subjects have to pay to enjoy. Controllers should assess, on a case-by-case basis, both whether a fee is appropriate at all and what amount is appropriate in the given circumstances, taking into account possible alternatives to behavioural advertising that entail the processing of less personal data as well as the data subjects' position. Controllers should ensure that the fee is not such as to inhibit data subjects from making a genuine choice in light of the requirements of valid consent and of the principles under Article 5 GDPR, in particular fairness. The accountability principle is key in this regard. Supervisory authorities are tasked with enforcing the application of the GDPR, which may also relate to the impact of any fee on the data subjects' freedom of choice.

Another condition is granularity: when presented with a 'consent or pay' model, the data subject should be free to choose which purpose of processing they accept, rather than being confronted with one consent request bundling several purposes.

Valid consent also needs to be 'specific', i.e. given for one or more specific purposes, and amount to an unambiguous indication of wishes: in 'consent or pay' models it is especially important for controllers to attentively design how data subjects are asked to provide their consent. Users should not be subject to deceptive design patterns.

For consent to be 'informed', the information process built by controllers should enable data subjects to have a full and clear comprehension of the value, the scope and the consequences of their possible choices, taking into account the complexity of processing activities related to behavioural advertising.

The EDPB also provides clarifications on the withdrawal of consent and advises controllers to carefully assess how often consent should be 'refreshed'.

Table of contents

1	Introduction.....	6
1.1	Summary of facts.....	6
1.2	Admissibility of the request for an Article 64(2) GDPR opinion.....	7
2	Definitions and scope of the opinion	8
2.1	Definitions	8
2.1.1	Definition of ‘consent or pay’ models.....	9
2.1.2	Definition of ‘behavioural advertising’	9
2.1.3	Definition of ‘large online platforms’ in the context of this Opinion	10
2.2	Scope of the Opinion.....	12
3	Legal Context.....	12
3.1	Relevant provisions of the GDPR.....	12
3.2	Further legal instruments.....	13
3.3	Summary of the <i>Bundeskartellamt</i> judgment.....	15
3.4	Existing EDPB guidance	16
4	Assessment of the EDPB.....	16
4.1	Principles and general observations	16
4.2	Requirements for valid consent	18
4.2.1	Freely given consent.....	19
4.2.2	Informed consent	32
4.2.3	Specific consent.....	35
4.2.4	Unambiguous indication of wishes	35
4.3	Additional elements	36
4.3.1	Withdrawal of consent.....	36
4.3.2	Refreshing consent.....	38
5	Conclusions.....	39

The European Data Protection Board

Having regard to Article 63 and Article 64(2) of the 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 (hereinafter ‘GDPR’),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to Article 10 and Article 22 of its Rules of Procedure,

Whereas:

(1) The main role of the European Data Protection Board (hereafter the ‘Board’ or the ‘EDPB’) is to ensure the consistent application of the GDPR throughout the European Economic Area (‘EEA’). Article 64(2) GDPR provides that any supervisory authority (‘SA’), the Chair of the Board or the Commission may request that any matter of general application or producing effects in more than one EEA Member State be examined by the Board with a view to obtaining an opinion. The aim of this opinion is to examine a matter of general application or which produces effects in more than one EEA Member State.

(2) The opinion of the Board shall be adopted pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the Rules of Procedure within eight weeks from when the Chair and the competent supervisory authorities have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION

1 INTRODUCTION

1.1 Summary of facts

1. On 17 January 2024, the Dutch supervisory authority (NL SA), acting also on behalf of the Norwegian supervisory authority (NO SA) and the German (Hamburg) supervisory authority (DE Hamburg SA), together referred to as the ‘requesting SAs’, requested the EDPB to issue an opinion pursuant to Article 64(2) GDPR in relation to the so-called ‘consent or pay’ models (‘the request’).
2. The Chair of the Board and the NL SA considered the file complete on 25 January 2024. On the same date, the file was broadcast by the EDPB Secretariat.

¹ References to ‘Member States’ made throughout this opinion should be understood as references to ‘EEA Member States’.

3. The request concerns, in short, the circumstances under which so called ‘consent or pay’ models² can be implemented by large online platforms which attract large amounts of users in the European Economic Area (‘EEA’) when data is processed for behavioural advertising purposes, in a way that satisfies the requirement for a valid, and in particular freely given, consent³.
4. The requesting SAs recall the ‘EDPB Guidelines 05/2020 on consent under Regulation 2016/679’, hereinafter ‘EDPB guidelines on consent’, and highlight that it is important to assess if data subjects that are faced with ‘consent or pay’ models are ‘able to exercise a real choice’, taking into account the ‘risk of deception, intimidation, coercion or significant negative consequences’ or if ‘there is any element of compulsion, pressure or inability to exercise free will’⁴.
5. The requesting SAs further mention that the above questions should be addressed by taking into account the Court of Justice’s *Bundeskartellamt* judgment⁵.
6. Finally, in their reasoning for the request, the requesting SAs point out that ‘several EDPB Members have already provided guidance regarding ‘consent or pay’ models at national level, for instance in relation to media outlets’ and that, while this national guidance is ‘valuable and providing a good starting point’, it is ‘usually aimed at smaller controllers’⁶. Thus, the requesting SAs argue that there is the need to provide an answer to the specific questions raised by the implementation of ‘consent or pay’ models by large online platforms, in order to ensure a consistent interpretation and application of the GDPR.

1.2 Admissibility of the request for an Article 64(2) GDPR opinion

7. Article 64(2) GDPR provides that, in particular, any SA may request that any matter of general application or producing effects in more than one Member State be examined by the Board with a view to obtaining an opinion.
8. The requesting SAs specify in the request that ‘from a data protection perspective there is, at the moment, no consistent European answer to the above-mentioned question⁷ regarding the validity of consent in relation to ‘consent or pay’ models’⁸. They further stress that this ‘is a cause for concern as

² See definition in Section 2.1.1 of this Opinion.

³ Request for an opinion pursuant to Article 64(2) GDPR (hereinafter, the ‘Request’), Section I (‘Introduction’), p. 1.

⁴ Request, Section II (‘Background and reasoning of this request’), A. Legal framework regarding the fundamental concept of consent, p. 2. In this regard, see the EDPB Guidelines 05/2020 on consent under Regulation 2016/679, adopted on 4 May 2020 (hereinafter, ‘EDPB Guidelines on consent’), paragraph 24.

⁵ Request, Section II (‘Background and reasoning of this request’), B. The relation between consent and ‘consent or pay models’, p. 3. See Judgment of the Court of Justice of the European Union of 4 July 2023, *Meta Platforms Inc. v Bundeskartellamt*, C-252/21, EU:C:2023:537 (hereinafter, ‘CJEU *Bundeskartellamt* judgment’). More specifically, the requesting SAs recall paragraphs 143-144, 148-150 of the CJEU *Bundeskartellamt* judgment.

⁶ Request, Section II (‘Background and reasoning of this request’), C. Current developments and the need for clarity, p. 4. More specifically, the requesting SAs submit with the request national guidance providing general criteria for ‘consent or pay’ models issued by the German (Hamburg), Austrian and French supervisory authorities.

⁷ See paragraph 3 of the present Opinion.

⁸ Request, Section II (‘Background and reasoning of this request’), C. Current developments and the need for clarity, p. 4.

this issue is [...] inextricably linked to the interpretation of the concept of consent and therefore a matter of general application regarding a key concept from the GDPR⁹.

9. The request relates to the consistent interpretation of the concept of consent, and more specifically to the circumstances under which consent collected by large online platforms processing personal data for behavioural advertising purposes and implementing ‘consent or pay’ models, can be considered valid. As a consequence, the Board considers that the request concerns a ‘matter of general application’ within the meaning of Article 64(2) GDPR. In particular, the matter relates to questions related to the practical implementation of key provisions of the GDPR and in relation to which, at the moment, there is no consistent interpretation at EU level. It can therefore be argued that a general interest exists in assessing this question in the form of an EDPB opinion, in order to ensure the uniform application of the GDPR. The implementation of ‘consent or pay’ models by large online platforms raises specific issues: as highlighted by the requesting SAs ‘this lack of a uniform approach is particularly pressing when it comes to large online platforms which attract millions of data subjects in Europe. It can be argued that, especially when it comes to such large online platforms, a uniform approach is required in relation to any questions of general application related to this type of controllers, taking into account that these platforms are active in all EU and EEA Member States and any ‘consent or pay’ model implemented by controllers operating this type of large online platform will affect millions of European data subjects’¹⁰.
10. The request includes written reasoning on the background and reasons for submitting the question to the Board, including on the relevant legal framework, on the relation between the consent and ‘consent or pay’ models, as well as on the current developments in the CJEU jurisprudence and need for clarity and consistent interpretation¹¹. Therefore, the Board considers that the request is reasoned in line with Article 10.3 of the EDPB Rules of Procedure¹².
11. According to Article 64(3) GDPR, the EDPB shall not issue an opinion if it has already issued an opinion on the matter¹³. As further explained in Section 3.4 below, the EDPB has not issued an opinion on the same matter and it has not yet provided replies to the questions arising from the request.
12. For these reasons, the Board considers that the request is admissible and the questions arising from it should be analysed in this opinion (the ‘Opinion’) adopted pursuant to Article 64(2) GDPR.
13. The following Section provides a definition of ‘consent or pay’ models, ‘behavioural advertising’ and ‘large online platforms’ in the context of this Opinion, as well as a description of the scope of the Opinion.

2 DEFINITIONS AND SCOPE OF THE OPINION

2.1 Definitions

⁹ Request, Section II (“Background and reasoning of this request”), C. Current developments and the need for clarity, p. 4.

¹⁰ Request, Section II (“Background and reasoning of this request”), C. Current developments and the need for clarity, p. 5.

¹¹ Request, Section II (“Background and reasoning of this request”), pp. 1-5.

¹² Article 10.3 of the EDPB Rules of procedure states: “Requests shall be provided with reasoning pursuant to Article 64 (2) GDPR”.

¹³ Article 64(3) GDPR and Article 10.4 of the EDPB Rules of Procedure.

2.1.1 Definition of ‘consent or pay’ models

14. ‘Consent or pay’ models¹⁴ can be defined as models where a controller offers data subjects a choice between at least two options in order to gain access to an online service that the controller provides: the data subject can 1) consent to the processing of their personal data for a specified purpose, or 2) decide to pay a fee and gain access to the online service without their personal data being processed for such purpose. This Opinion will focus on models in which consent can be given to the processing of personal data for behavioural advertising purposes.
15. Under the first option mentioned above, the data subjects get access to the service only if they consent to being tracked and targeted with behavioural advertising by the controller. In this case, the controller’s business model is usually financed through online advertising based on users’ behaviours.
16. Under the second option, the data subjects pay a fee (which can be, for instance, a weekly, monthly, or annual subscription, as well as a one-off payment)¹⁵ and are allowed to access a version of the service that does not include the processing of the user’s personal data for behavioural advertising purposes. However, one should note that, while this second option may entail that the data subjects are not tracked at all, it might also entail that data subjects would be still tracked for different purposes, e.g. in order to analyse the use of a website to improve its functionalities. In any event, the EDPB recalls that such purposes must be legitimate, specific and processing must be based on a lawful ground pursuant to the GDPR. Moreover, cookies or tracking technologies might still be used, under the paid version of the service, for purposes other than behavioural advertising. If any technology used involves access or storage of information in terminal equipment, this is subject to compliance with the GDPR and Article 5(3) of the ePrivacy Directive where applicable.
17. While under ‘consent or pay’ models discussed in the present Opinion, a data subject is usually denied access to the service if they neither consent to the processing of personal data for behavioural advertising purposes nor pay a fee, the EDPB highlights that a further alternative without behavioural advertising, free of charge, can be offered to data subjects as further described below in Section 4.2.1.1.

2.1.2 Definition of ‘behavioural advertising’

18. The EDPB notes that mechanisms allowing the provision of personalised online advertisements to data subjects have proliferated over time. Their sophistication has also increased. Users can be targeted with personalised advertising on the basis of different criteria and techniques, including on the basis of information related to their behaviour online and offline.
19. Behavioural advertising, which entails the development of detailed profiles of data subjects, has become a key feature of certain business models in today’s online environment. In the Article 29 Working Party (WP29) Opinion 2/2010 on online behavioural advertising, ‘behavioural advertising’ is

¹⁴ See also in this regard documents adopted at national level, such as (i) Austrian SA (DSB), *FAQ zum Thema Cookies und Datenschutz*, 20 December 2023, (ii) French SA (CNIL), *Cookie walls: la CNIL publie des premiers critères d’évaluation*, 16 mai 2022, and (iii) the Conference of the Independent Data Protection Authorities of Germany (DSK), *Beschluss - der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom*, 22 March 2023.

¹⁵ In these cases, the paid subscription may also differ based on the services that the user accesses, e.g., a basic service for the first subscription level, an additional one for additional/complementary services or functionalities.

defined as ‘advertising that is based on the observation of the behaviour of individuals over time’¹⁶. The Article 29 Working Party has also underlined that behavioural advertising ‘seeks to study the characteristics of this behaviour through their actions (repeated site visits, interactions, keywords, online content production, etc.) in order to develop a specific profile and thus provide data subjects with advertisements tailored to match their inferred interests’¹⁷.

20. As explained in the above-mentioned WP29 Opinion, behavioural advertising is based on data that is collected through observing the users’ activity over time (e.g. from the pages they visit, the amount of time they spend on a page displaying a certain product, the number of reconconnections to a page, the likes given or their location). In these cases, the monitoring of users takes place through the use of cookies or other similar tracking technologies (e.g., social plug-ins or pixels). Users can be tracked across different websites by various players (e.g., platforms and data brokers)¹⁸. The data collected, which may, in certain cases, be aggregated with data actively provided by the user (e.g., when they create an account online or when they log-in on a website), or with offline data, allows businesses to infer information about the user and draw conclusions on their preferences, tastes and interests¹⁹. Several processing activities take place when controllers process personal data for behavioural advertising purposes. These include monitoring of data subjects’ behaviour, gathering personal data and analysing them for the purpose of creating and developing users’ profiles, sharing personal data with third parties as part of the creation and development of users’ profiles or to connect advertisers with publishers, serving data subjects with ads personalised on the basis of the resulting profile, and analysing the users’ interaction with the advertisements displayed based on their profile.
21. For this reason, behavioural advertising is considered a particularly intrusive form of advertising, as it can provide controllers with a very detailed picture of individuals’ personal life. In addition, as recalled by the EDPB in its Guidelines 8/2020 on the targeting of social media users, it raises significant risks for the fundamental rights and freedoms of data subjects including the possibility of discrimination and exclusion and the possible manipulation of users²⁰.

2.1.3 Definition of ‘large online platforms’ in the context of this Opinion

22. This Opinion focuses on ‘consent or pay’ models implemented by ‘controllers of ‘large online platforms’ which attract large amounts of users in the EEA’²¹. It is important to identify the type of platforms that fall under the scope of this Opinion.
23. The EDPB recalls that ‘online platforms’ are not defined in the GDPR. It is therefore appropriate to specify the meaning of this concept. For the purposes of the present Opinion, the concept of ‘online

¹⁶ Article 29 Working Party, Opinion 2/2010 on online behavioural advertising, WP 171, adopted on 22 June 2010 (hereinafter, ‘WP29 Opinion on online behavioural advertising’), p. 4.

¹⁷ WP29 Opinion on online behavioural advertising, p. 4.

¹⁸ EDPB Guidelines 8/2020 on the targeting of social media users, Version 2.0, adopted on 13 April 2021 (hereinafter, ‘EDPB Guidelines on targeting’), paragraph 3.

¹⁹ WP29 Opinion on online behavioural advertising, p. 7 (‘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. Both approaches can be combined. Additionally, predictive profiles may be made explicit at a later time, when a data subject creates login credentials for a website).

²⁰ EDPB Guidelines on targeting, paragraphs 9-18.

²¹ Request, Section I (‘Introduction’), p. 3.

platforms' may cover, but is not limited to, 'online platforms' as defined under Article 3(i) Digital Services Act²².

24. In the following paragraphs, the EDPB highlights certain elements to be assessed, on a case-by-case basis, to determine whether a controller is to be considered as a 'large online platform' for the purposes of this opinion. Taking into account that certain elements may be more relevant for certain controllers than for others, this list of elements is not an exhaustive one nor a list of cumulative requirements; rather, this list of elements aims to provide an indication of aspects that may lead to considering a controller as a 'large online platform' for the purposes of this Opinion.
25. First of all, large online platforms are platforms that attract a large amount of data subjects as their users.
26. The position of the company in the market is another element that may be relevant to assess whether the controller can be considered as a 'large online platform'.
27. Another element to consider in order to assess if a controller qualifies as a 'large online platform' is whether it conducts 'large scale' processing. The EDPB recalls that the GDPR does not define what constitutes large scale processing, although Recital 91 GDPR provides some guidance. However, the Article 29 Working Party has given guidance (endorsed by the EDPB) as to the meaning of 'large scale' processing in the context of Article 37(1)(b) and (c) GDPR, and more specifically on the factors that should be considered when determining whether the processing is carried out on a large scale. These factors are also relevant for the purposes of the present Opinion. They include, for instance, the number of data subjects concerned, the volume of data and the geographical extent of the processing activity²³.
28. The definition may cover, among others, certain controllers of 'very large online platforms', as defined under the DSA²⁴ and 'gatekeepers', as defined under the DMA²⁵.

²² Article 3(i) of the Digital Services Act defines 'online platform' as 'a hosting service that, at the request of a recipient of the service, stores and disseminates information to the public, unless that activity is a minor and purely ancillary feature of another service or a minor functionality of the principal service and, for objective and technical reasons, cannot be used without that other service, and the integration of the feature or functionality into the other service is not a means to circumvent the applicability of this Regulation'.

²³ See, in this regard, Article 29 Data Protection Working Party Guidelines on Data Protection Officers ('DPOs'), WP 243 rev.01, as last revised and adopted on 5 April 2017, endorsed by the EDPB on 25 May 2018, pp. 7-8, and Article 29 Data Protection Working Party Guidelines 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, as last revised and adopted on 4 October 2017, endorsed by the EDPB on 25 May 2018, p. 10.

²⁴ Under Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (hereinafter, 'DSA'), Article 33(1), VLOPs are 'online platforms which provide their services to a number of average monthly active recipients of the service in the Union equal to or higher than 45 million' and which are designated' as VLOPs by the European Commission under Article 33(4) DSA. According to Article 3(i) DSA, an online platform is a hosting service that, at the request of a recipient of the service, stores and disseminates information to the public.

²⁵ Under Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (hereinafter, 'DMA'), Article 3(1), gatekeepers are companies that fulfil the following three cumulative requirements: (i) they have a significant impact on the internal market; (ii) they provide a core platform service, which is an important gateway for business users to reach end users; (iii) they enjoy an entrenched and durable position, in their operations, or it is foreseeable that they will enjoy such a position in the near future. Under Article 2(2), core platform services include the following: (a) online intermediation

2.2 Scope of the Opinion

29. The Board agrees with the requesting SAs that, from a data protection perspective, ‘consent or pay’ models raise fundamental questions, in particular with regard to the interpretation and application of the concept of consent, referred to in Article 8 of the Charter of Fundamental Rights of the European Union and in Articles 4, 5, 6 and 7 of the GDPR.
30. While it should be recalled that the concept of consent in the GDPR applies to any controller seeking to rely on this legal basis, this Opinion focuses on the specific questions that arise in connection to the validity of consent sought by large online platforms deploying ‘consent or pay’ models, as identified in the request. These platforms may be uniquely situated in respect of some of the criteria for valid consent, e.g. in respect of the existence of an imbalance of power. The use of the term ‘controller(s)’ in this Opinion should be understood as covering large online platforms as defined in Section 2.1.3 above.
31. In light of the above, the present Opinion concerns, and is limited to, the assessment of the validity of consent when used as a legal basis to process personal data for behavioural advertising purposes in the context of ‘consent or pay’ models deployed by large online platforms. The factors highlighted in this Opinion will typically apply to large online platforms, but not exclusively. Some of the considerations expressed in this opinion may prove useful more generally for the application of the concept of consent in the context of ‘consent or pay’ models.
32. The EDPB recalls that, in accordance with Article 51(1) GDPR, supervisory authorities are ‘responsible for monitoring the application of [the GDPR], in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union’²⁶. In addition, pursuant to Article 51(2) GDPR, ‘Each supervisory authority shall contribute to the consistent application of [the GDPR] throughout the Union’. It is therefore within the competence of supervisory authorities to assess the validity of consent used as a legal basis for the processing of personal data, including when such consent is collected in the context of ‘consent or pay’ models where personal data is processed for behavioural advertising purposes.
33. In line with the above, this Opinion provides a framework for controllers and SAs to assess the validity of consent in ‘consent or pay’ models by addressing in turn each of the requirements that make up consent under the GDPR. It is of note that a case-by-case assessment of the criteria remains necessary.

3 LEGAL CONTEXT

3.1 Relevant provisions of the GDPR

34. For the purposes of this Opinion, the EDPB considers that the main relevant provisions of the GDPR include Articles 4, 5, 6 and 7, as well as Recitals 32, 42 and 43.

services; (b) online search engines; (c) online social networking services; (d) video-sharing platform services; (e) number-independent interpersonal communications services; (f) operating systems; (g) web browsers; (h) virtual assistants; (i) cloud computing services; (j) online advertising services, including any advertising networks, advertising exchanges and any other advertising intermediation services, provided by an undertaking that provides any of the core platform services listed in points (a) to (i).

²⁶ See also Article 57(1) GDPR listing the tasks of supervisory authorities.

35. Article 4(11) GDPR defines consent as ‘any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her’. The provision of consent by the data subject is one of the lawful grounds for processing of personal data, specified in Article 6(1)(a) GDPR²⁷.
36. In addition, it is also important to recall the requirements for controllers to process personal data in line with all applicable provisions of the GDPR, and in particular with the data protection principles laid down in Article 5 GDPR²⁸ and with the principle of data protection by design and by default in Article 25 GDPR²⁹.
37. Article 7 and Recitals 32, 42 and 43 GDPR provide additional requirements and guidance regarding how controllers need to comply with the main elements of the consent requirements.
38. In particular, Article 7 GDPR sets the conditions for consent to be valid and stipulates, first, that ‘where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data’. This is also connected to the principle of accountability set by Article 5(2) GDPR.
39. Article 7(2) GDPR provides that ‘If the data subject’s consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language’ and that ‘Any part of such a declaration which constitutes an infringement of [the GDPR] shall not be binding’.
40. Paragraph 3 of Article 7 highlights the data subject’s right to withdraw his or her consent at any time. In this respect, the ‘withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal’. The data subject shall be informed about this prior to giving consent. The GDPR also specifies that it ‘shall be as easy to withdraw as to give consent’.
41. Article 7(4) GDPR states that ‘When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract’.

3.2 Further legal instruments

42. The EDPB is aware that certain aspects of ‘consent or pay’ models might also fall under the scope of other EU legal instruments which, although considered outside of the scope of this opinion, it is useful to recall.

²⁷ More specifically, Article 6 GDPR states, under paragraph 1(a), that ‘Processing shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes’.

²⁸ See also EDPB Guidelines on targeting, paragraph 58, ‘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.’ See also EDPB Guidelines on consent, paragraph 5.

²⁹ See the EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, Adopted on 20 October 2020 (hereinafter, ‘Guidelines on Data Protection by Design and by Default’).

43. The EDPB recalls that the concept of ‘consent’ under the GDPR is also relevant for the purpose of the application of the ePrivacy Directive³⁰ and implementing national laws³¹. Article 2(f) of the ePrivacy Directive further provides that consent by a user or subscriber corresponds to the data subject's consent in the GDPR. While this Opinion focuses on the interpretation of consent as a legal basis for processing of personal data under Article 6(1)(a) GDPR, its considerations on the notion of consent are therefore also relevant for the ePrivacy Directive as *lex-specialis*³².
44. The EDPB notes that some aspects of the issue raised by the request are also relevant to consumer and competition law, and may also be addressed under legal instruments such as, among others, Directive 2005/29/EC on Unfair Commercial Practices Directive³³. Even if this Opinion does not relate to these other fields of law or legal instruments, it may refer to their concepts or rules to build relevant criteria of analysis and foster a coherent application of EU law.
45. The EDPB is aware that the Directive 2019/770 on certain aspects concerning contracts for the supply of digital content and digital services (the ‘Digital Content Directive’)³⁴ may also be relevant.
46. The EDPB further notes that certain provisions of the Digital Markets Act (‘DMA’)³⁵, such as Article 5(2), lay down specific rules for so-called ‘gatekeepers’ processing personal data³⁶, and that Article 5(2) DMA refers to the concept of consent under the GDPR.
47. In addition, the EDPB notes that the Digital Services Act (‘DSA’) lays down specific obligations for providers of online platforms, as well as for providers of very large online platforms³⁷. This Opinion refers to relevant provisions of the DMA and the DSA insofar as necessary to foster a coherent application of EU law³⁸.

³⁰ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) as amended by Directive 2006/24/EC and Directive 2009/136/EC.

³¹ See Recital 173 GDPR clarifying the *lex specialis-lex generalis* relationship between Directive 2002/58/EC and the GDPR.

³² E.g. Article 5(3) ePrivacy Directive, which requires consent for access or storage of information in terminal equipment, unless an exception applies. See EDPB 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 Adopted on 12 March 2019, paragraph 40.

³³ Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (‘Unfair Commercial Practices Directive’). Other legal instruments relevant from a consumer law perspective include, for instance, Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights and Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts.

³⁴ Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services (the ‘Digital Content Directive’).

³⁵ Regulation (EU) 2022/1925 (Digital Markets Act).

³⁶ Relevant in this regard are also Recitals 36 and 37 of the DMA.

³⁷ In particular, Article 33(1) DSA provides that ‘This Section [5 DSA] shall apply to online platforms ... which have a number of average monthly active recipients of the service in the Union equal to or higher than 45 million, and which are designated as very large online platforms ... pursuant to paragraph 4’.

³⁸ Settled CJEU case law provides that, where two EU legal acts of the same hierarchical value do not establish priority of one over the other, they should be applied in a compatible manner, which enables a coherent application of them. See e.g. Judgment of the General Court of 3 May 2018, Malta v Commission, T-653/16, ECLI:EU:T:2018:241, paragraph 137.

48. Taking into account that competition law and consumer protection law are relevant in respect of certain aspects of ‘consent or pay’ models, the EDPB sought input from national and EU regulators in these fields of law on the topic of ‘consent or pay’ models.

3.3 Summary of the *Bundeskartellamt* judgment

49. The CJEU addressed several questions in its judgment issued on 4 July 2023, which arose from a request for a preliminary ruling. The first of the questions posed to the Court asked whether, when investigating a potential abuse of a dominant position under competition law, a competition authority could examine whether the undertaking in question had engaged in behaviour that did not comply with the GDPR³⁹. In its reply the Court highlighted the duty of sincere cooperation between competition authorities and data protection supervisory authorities⁴⁰. Further questions related to the interpretation of Article 9 GDPR⁴¹ and Article 6(1) GDPR (letters b, d, e, f)⁴².
50. As a last question, as recalled by the requesting SAs, the *Bundeskartellamt* judgment concerned the question of whether ‘consent given by the user of an online social network to the operator of such a network may be regarded as satisfying the conditions of validity laid down in Article 4(11) of [the GDPR], in particular the condition that consent must be freely given, where that operator holds a dominant position on the market for online social networks’⁴³.
51. The CJEU recalled, first of all, the definition of consent in Article 4(11) GDPR as well as Article 7(4) and Recitals 42 and 43 GDPR⁴⁴. As noted in the request, the CJEU stated that the existence of a dominant position of a provider of online social networks ‘does not, as such, preclude the users of such a network from being able validly to consent, within the meaning of Article 4(11) of [the GDPR], to the processing of their personal data by that operator’⁴⁵.
52. However, the CJEU clarified that a dominant position is ‘an important factor in determining whether the consent was in fact valid and, in particular, freely given, which is for that operator to prove’⁴⁶. This is because this circumstance ‘is liable to affect the freedom of choice of that user, who might be unable to refuse or withdraw consent without detriment’⁴⁷ and ‘may create a clear imbalance ... between the data subject and the controller’⁴⁸.
53. In addition, although not central to the Court’s determination, the CJEU mentioned that, where it appears that certain processing operations are not necessary for the performance of a contract⁴⁹, ‘users must be free to refuse individually, in the context of the contractual process, to give their

³⁹ CJEU *Bundeskartellamt* judgment, paragraphs 36-63.

⁴⁰ CJEU *Bundeskartellamt* judgment, paragraph 53.

⁴¹ A question relating to the interpretation of Article 9(1) GDPR is tackled by the Court in paragraphs 64-85 of the CJEU *Bundeskartellamt* judgment.

⁴² More specifically, paragraphs 86-139 of the CJEU *Bundeskartellamt* judgment. Paragraphs 86 and 97-126 of the CJEU *Bundeskartellamt* judgment relate to Article 6(1)(b) and Article 6(1)(f) GDPR. Paragraphs 127-139 of the CJEU *Bundeskartellamt* judgment relate to Article 6(1)(d) and Article 6(1)(e) GDPR.

⁴³ Request, Section II (‘Background and reasoning of this request’), B. The relation between consent and ‘consent or pay models’, p. 3 referring to paragraph 140 of the CJEU *Bundeskartellamt* judgment.

⁴⁴ CJEU *Bundeskartellamt* judgment, paragraphs 142-145.

⁴⁵ See CJEU *Bundeskartellamt* judgment, paragraph 154.

⁴⁶ See CJEU *Bundeskartellamt* judgment, paragraph 154.

⁴⁷ CJEU *Bundeskartellamt* judgment, paragraph 148, referring to Recital 42 GDPR.

⁴⁸ CJEU *Bundeskartellamt* judgment, paragraph 149, referring to Recital 43 and Article 7(4) GDPR.

⁴⁹ In this respect, the Court also makes reference in paragraph 149 to the paragraphs 102-104 above.

consent to [them], without being obliged to refrain entirely from using the service offered by the online social network operator, which means that those users are to be offered, if necessary for an appropriate fee, an equivalent alternative not accompanied by such data processing operations.⁵⁰

54. The CJEU also highlighted that as consent ‘is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case’ referring to Recital 43 GDPR. It further identified the ‘scale of the processing of the data’ and the ‘significant impact of that processing on the users of that network’, as well as the reasonable expectations of the users, as being particularly important factors in the case at hand. Having done this, the CJEU returned the cases to the referring court, stating that it should ascertain whether users had the possibility to give separate consent for the processing of data relating to their conduct within the social network and of data collected ‘off-platform’⁵¹.

3.4 Existing EDPB guidance

55. Various guidelines adopted by the EDPB are relevant for this Opinion⁵². In this regard, EDPB Guidelines 05/2020 on consent⁵³ are particularly relevant. They address the conditions for freely given consent from the data subjects, along with the other elements of valid consent. However, Guidelines 05/2020 do not fully tackle the question submitted to the EDPB by the requesting SAs, as they do not explain how the general EDPB guidance on consent should be applied in the context of ‘consent or pay’ models implemented by large online platforms which attract large amounts of users in the EEA and process their personal data for behavioural advertising purposes on the basis of consent⁵⁴. Therefore, it is appropriate for the EDPB to reply to the question raised in the request by issuing an EDPB Opinion under Article 64(2) GDPR.
56. As this Opinion aims at providing a framework against which ‘consent or pay’ models implemented by large online platforms can be assessed, each of the cumulative requirements that make up consent under the GDPR will be addressed in turn.

4 ASSESSMENT OF THE EDPB

4.1 Principles and general observations

57. Article 5 GDPR sets out the principles for processing of personal data. In this respect, the EDPB already clarified that obtaining consent does not absolve the controller from adhering to all the principles outlined in Article 5 GDPR⁵⁵ (as well as the other obligations foreseen by the GDPR). **Even if the**

⁵⁰ Request, Section II (‘Background and reasoning of this request’), B. The relation between consent and ‘consent or pay’ models, p. 3 referring to CJEU *Bundeskartellamt* judgment, paragraph 140.

⁵¹ CJEU *Bundeskartellamt* judgment, paragraph 151.

⁵² These include EDPB Guidelines on consent, as well as EDPB Guidelines on targeting.

⁵³ EDPB Guidelines on consent.

⁵⁴ In the EDPB Guidelines on consent, the EDPB clarified its position on the so-called ‘cookie walls’, where data subjects have the choice between consenting to the storing of information in their terminal equipment or not accessing the service. This is an example of a situation where the consent provided by data subjects cannot be considered ‘freely given’.

⁵⁵ EDPB Guidelines on consent, paragraph 5 (‘Furthermore, 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’).

processing is consent-based, it does not justify collecting personal data beyond what is necessary for the specified purpose or in a manner that is unfair to the data subjects⁵⁶.

58. The processing should respect the principles of **necessity and proportionality⁵⁷**. Respecting the principles of **purpose limitation and data minimisation⁵⁸** is of crucial importance. Pursuant to the purpose limitation principle, personal data must be collected for specified, explicit and legitimate purposes⁵⁹. Controllers have the responsibility to clearly define the purposes of processing, including with respect to processing carried out for behavioural advertising purposes⁶⁰. Additionally, controllers have to ensure compliance with the principle of data minimisation⁶¹, according to which personal data are to be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed, and which gives expression to the principle of proportionality⁶². In this regard, controllers should first of all determine whether they even need to process personal data for their relevant purposes, and **verify whether the relevant purposes can be achieved by less intrusive means, or by processing less personal data**, or having less detailed or aggregated personal data⁶³. Section 4.2.1.1 below is relevant in this regard.
59. The EDPB notes that behavioural advertising may entail gathering and compiling as much personal data as possible about individuals and their activities, potentially monitoring their entire life, on- and offline⁶⁴. The EDPB considers that the magnitude and intrusiveness of the processing have to be taken into account while assessing compliance with the principle of data minimisation. Excessive tracking, which includes the combination of various sources of data across different websites, is thus harder to reconcile with the principle of data minimisation than, for example a system of personalized advertising in which users themselves actively and consciously determine their own preferences.
60. Processing activities should always respect the **fairness** principle⁶⁵. Key elements of the fairness principle include, among others, the need for the processing to correspond with data subjects' reasonable expectations, the need for the controller to not unfairly discriminate against data subjects or exploit their needs or vulnerabilities, the need to avoid or account for power imbalances, and the need to avoid any deceptive or manipulative language or design⁶⁶. In this respect, the EDPB recalls the need to avoid deceptive design patterns⁶⁷. Additionally, the controller should take into account the processing's wider impact on individuals' rights and dignity, and grant the highest degree of autonomy

⁵⁶ EDPB Guidelines on consent, paragraph 5 ('Even if the processing of personal data is based on consent of the data subject, this would not legitimise collection of data, which is not necessary in relation to a specified purpose of processing and be fundamentally unfair').

⁵⁷ EDPB Guidelines on consent, paragraph 5 ('Furthermore, 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 of the GDPR with regard to fairness, necessity and proportionality, as well as data quality').

⁵⁸ Article 5(1)(b) and 5(1)(c) GDPR.

⁵⁹ EDPB Guidelines on Data Protection by Design and Default, section 3.4.

⁶⁰ EDPB Guidelines on Data Protection by Design and Default, paragraph 72 (referring to the elements of 'predetermination' and 'specificity' of the purposes as part of the purpose limitation principle).

⁶¹ EDPB Guidelines on Data Protection by Design and Default, sections 3.4 and 3.5.

⁶² CJEU, Judgment of the Court in Case C-439/19 (*Latvijas Republikas Saeima*), paragraph 98.

⁶³ EDPB Guidelines on Data Protection by Design and Default, paragraphs 51 and 74.

⁶⁴ See above Section 2.1.2.

⁶⁵ Article 5(1)(a) GDPR.

⁶⁶ EDPB Guidelines on Data Protection by Design and Default, paragraph 70.

⁶⁷ EDPB Guidelines 3/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them, Version 2.0, adopted on 14 February 2023 (hereinafter, 'EDPB Guidelines on deceptive design patterns').

possible to data subjects⁶⁸. This is key for controllers to bear in mind especially whenever the processing they engage in is particularly intrusive. The EDPB also notes that fairness can act as an easily-understandable touchstone or reference point for controllers when evaluating a ‘consent or pay’ model. In this regard, it is important that controllers are able to demonstrate why they consider certain choices are in line with the principle of fairness as described in the previous paragraph. This is particularly important if the controller narrows down the data subject's range of choices (e.g. by not providing a Free Alternative Without Behavioural Advertising, as described below in Section 4.2.1.1) or which may risk unduly influencing the data subject's choice (e.g. by charging a fee that is such to effectively inhibit data subjects from making a free choice).

61. Controllers are also expected to respect the principle of **transparency**. In application of this principle, controllers should enable data subjects to easily understand how their choice will affect the processing of their personal data⁶⁹. In respect of consent, this is further described below in Section 4.2.2.
62. In line with Article 25 (1) GDPR, the controller shall respect the principle of **data protection by design**. This means they shall implement appropriate technical and organisational measures which are designed to implement the data protection principles and to integrate the necessary safeguards into the processing in order to meet the requirements and protect the rights and freedoms of data subjects⁷⁰.
63. Additionally, in line with Article 25 (2) GDPR, the controller shall respect the principle of **data protection by default**. This means that they should choose and be accountable for implementing default processing settings and options in a way that only processing that is strictly necessary to achieve the set, lawful purpose is carried out by default. This means that by default, the controller shall not collect more data than is necessary, they shall not process the data collected more than is necessary for their purposes, nor shall they store the data for longer than necessary⁷¹.
64. Children benefit from specific protection, especially in relation to profiling and marketing purposes⁷². In particular, **children** should not be subject to behavioural advertising⁷³, and by extension, should not be confronted with ‘consent or pay’ models seeking consent for such processing.
65. Of particular importance in this regard is the principle of **accountability** in Article 5(2) GDPR, which states that the controller is responsible for and must be able to demonstrate its compliance with the other principles of Article 5 GDPR⁷⁴. In relation to consent, Article 7(1) explicitly states that the controller must be able to demonstrate that the data subjects have consented to the processing where they rely on consent as a legal basis. As the CJEU pointed out in the *Bundeskartellamt* judgment⁷⁵, the controller must be able to demonstrate that the data subject’s consent was freely given in light of the circumstances of the processing situation, and that all other conditions for valid consent were met.

4.2 Requirements for valid consent

⁶⁸ EDPB Guidelines on Data Protection by Design and Default, paragraph 70.

⁶⁹ Recital 39 GDPR; WP29 Guidelines on Transparency, paragraph 4; EDPB Guidelines on Data Protection by Design and Default, paragraph 66.

⁷⁰ EDPB Guidelines on Data Protection by Design and Default, paragraph 7.

⁷¹ EDPB Guidelines on Data Protection by Design and Default, paragraph 42.

⁷² Recital 38 GDPR.

⁷³ See also Article 28(2) DSA.

⁷⁴ See, in this regard, CJEU, Judgment of the Court in case C-175/20, *SIA 'SS' v Valsts ieņēmumu dienests*, ECLI:EU:C:2022:124, paragraph 77.

⁷⁵ CJEU *Bundeskartellamt* judgment, paragraph 152.

66. In order to reply to the question of under which circumstances and conditions 'consent or pay' models relating to behavioural advertising can be implemented by large online platforms in a way that constitutes valid and, in particular, freely given consent, this Opinion will address in turn each of the cumulative requirements that make up consent under the GDPR.

4.2.1 Freely given consent

67. The criterion of 'freely given consent' is central to the understanding of consent as a legal basis for processing of personal data. The distinct character of consent as a legal ground for processing is that it is the data subject's decision ('unambiguous indication of the data subject's wishes'), and crucially their freedom of choice to make that decision, which determines the legality of the processing.
68. Controllers must ensure that data subjects have a real freedom of choice when asked to consent to processing of their personal data, and they may not limit data subjects' autonomy by making it harder to refuse rather than to consent⁷⁶. This is also supported by one of the main purposes of the GDPR, which is to provide data subjects with control over their personal data⁷⁷. For consent to be freely given, the data subjects must be able to determine themselves if the processing can take place, without inappropriate influence from the controller or others⁷⁸, and be provided with appropriate information about the processing⁷⁹.
69. The EDPB has previously stated that the word 'free' implies real choice and control for data subjects' and that under the GDPR, 'if the data subject has no real choice, feels compelled to consent or will endure negative consequences if they do not consent, then consent will not be valid'⁸⁰. As highlighted by the EDPB on multiple occasions, consent can only be valid if the data subject is able to exercise a real choice, and there is no risk of deception, intimidation, coercion or significant negative consequences if the data subject does not consent. Consent will not be free in cases where there is any element of compulsion, pressure or inability to exercise free will⁸¹.
70. The GDPR provides several criteria that should be used to assess whether the context and circumstances where the data processing takes place provide the data subjects with sufficient autonomy for their consent to be considered 'freely given'. As explained by the EDPB in its Guidelines on consent, the main criteria to be taken into account when assessing whether consent is valid are whether the data subject suffers detriment by not consenting or withdrawing consent; whether there is an imbalance of power between the data subject and the controller; whether consent is required to access goods or services, even though the processing is not necessary for the fulfilment of the contract (conditionality); and whether the data subject is able to consent to different processing operations (granularity)⁸². The CJEU also stated in the *Bundeskartellamt* judgment that these are the main considerations on whether a data subject's consent is valid⁸³.

⁷⁶ The same also applies to withdrawing consent, see Article 7 (2) GDPR.

⁷⁷ See Recitals 7, 42 and 43 GDPR. The principle of transparency and the rights of data subjects in Chapter III of the GDPR are further examples of rules that seek to strengthen the data subjects' control of their personal data.

⁷⁸ See in this regard EDPB Guidelines on Deceptive Design Patterns, given that as mentioned in their paragraph 3 "deceptive design patterns" can hinder data subjects' ability to give an informed and freely given consent.

⁷⁹ In this regard, the considerations made in Section 4.2.2 on informed consent are relevant and should be taken into account.

⁸⁰ EDPB Guidelines on consent, paragraph 13.

⁸¹ EDPB Guidelines on consent, paragraph 24.

⁸² EDPB Guidelines on consent, paragraphs 13-54.

⁸³ CJEU *Bundeskartellamt* judgment, paragraphs 143 – 146.

71. One must consider whether the criteria are met on a case-by-case basis in relation to the specific processing situation. Controllers should be able to demonstrate that consent was freely given. In this regard, while the criteria are interrelated, each one must be respected at the time when a data subject consents to the processing. For instance, if a controller takes steps to avoid any conditionality, but not consenting would entail detriment to the data subject, consent will not be freely given.

4.2.1.1 The provision of a free alternative without behavioural advertising

72. As described in the previous section, data subjects should enjoy a real and genuine freedom of choice when asked to consent to the processing of their personal data. In such a context, the freedom of choice that the data subject enjoys also depends on the options that users are offered.

73. **The offering of (only) a paid alternative to the service which includes processing for behavioural advertising purposes should not be the default way forward for controllers.** On the contrary, when developing the alternative to the version of the service with behavioural advertising, **controllers should consider providing data subjects with an ‘equivalent alternative’ that does not entail the payment of a fee**, such as the Free Alternative Without Behavioural Advertising as described below in this section.

74. **Should controllers decide to provide data subjects with an ‘equivalent alternative’ which involves the payment of a fee**, the EDPB highlights that particular attention should be paid to the elements contained in this Opinion, such as the ones included in section 4.2.1.4.1 and 4.2.1.4.2. In such cases, in order to ensure genuine choice and to avoid presenting users with a binary choice between paying a fee and consenting to processing for behavioural advertising purposes, **controllers should consider also offering a further alternative free of charge** (‘Free Alternative Without Behavioural Advertising’).

75. This alternative must entail no processing for behavioural advertising purposes and may **for example** be a version of the service **with a different form of advertising involving the processing of less (or no) personal data**, e.g. contextual or general advertising or advertising based on topics the data subject selected from a list of topics of interests. This is also linked to the principle of data minimisation as recalled in Section 4.1: controllers should ensure that only personal data that is necessary for the purpose of placing such advertisement would be processed. Controllers should in any event bear in mind the need to comply with Article 6 GDPR and Article 5(3) of the ePrivacy Directive when applicable.

76. While there is no obligation for large online platforms to always offer services free of charge, making this further alternative available to the data subjects **enhances their freedom of choice**. This makes it **easier for controllers to demonstrate that consent is freely given**.

77. In the opinion of the EDPB, whether or not a Free Alternative Without Behavioural Advertising is provided is a **particularly important factor to consider when assessing whether data subjects can exercise a real choice** and therefore whether consent is valid. As stated in its reply to the Commission’s initiative for a cookie pledge, the EDPB considers among others relevant whether a user is offered, in addition to a service using tracking technology and a paid service, another type of service, such as one that includes a less intrusive form of advertising, when assessing the validity of consent and whether the data subject is able to exercise a real choice⁸⁴.

⁸⁴ EDPB reply to the Commission’s Initiative for a voluntary business pledge to simplify the management by consumers of cookies and personalised advertising choices, adopted on 13 December 2023, p. 5 of the Annex: ‘When assessing whether consent is valid, the EDPB considers it among others relevant whether in addition to a service using tracking technology and a paid service, another type of service is offered, for example a service

78. The Free Alternative without Behavioural Advertising offered as a further alternative would play a **relevant role to remove, reduce or mitigate the detriment** that may arise for non-consenting users from either having to pay a fee to access the service or not being able to access it.
79. Additionally, as previously observed by the EDPB, where a clear imbalance of power exists, consent can only be used in ‘exceptional circumstances’ and where the controller, in line with the accountability principle, can prove that there are no ‘adverse consequences at all’ for the data subject if they do not consent, notably if data subjects are offered an alternative that does not have any negative impact⁸⁵. In the context of this Opinion, such an alternative could be the offering of the Free Alternative Without Behavioural Advertising.
80. Whether controllers offer a Free Alternative Without Behavioural Advertising may also be relevant in assessing other aspects of freely given consent, such as whether a situation of conditionality exists, as explained in Section 4.2.1.4 of this Opinion.
81. When various options are presented to data subjects, controllers should also ensure that the data subjects fully understand what each option entails in terms of data processing and their consequences. In this regard, the considerations made in Section 4.2.2 on informed consent are relevant and should be taken into account. The **clarity of the different options to choose from** should also be reflected in the design of the interface, as deceptive or manipulative design should be avoided in line with the principle of fairness⁸⁶.
82. Also, the EDPB recalls that controllers that are gatekeepers pursuant to the DMA and/or VLOPs under the DSA should take their respective requirements into account when developing alternative options for the user⁸⁷.

4.2.1.2 Detriment

83. Pursuant to Recital 42 GDPR, for consent to be regarded as freely given, the data subject needs to have a genuine choice and be able to refuse or withdraw their consent without detriment, which means without experiencing harm or damage⁸⁸. The possibility to refuse or withdraw consent without detriment needs to be demonstrated by the controller⁸⁹.

with a less privacy intrusive form of advertising, such as contextual advertising, and whether the data subject is able to exercise a real choice.’

⁸⁵ EDPB Guidelines on consent, paragraph 22 and Example 5.

⁸⁶ See the EDPB Guidelines on Data Protection by Design and by Default, paragraph 70. See also the EDPB Guidelines on Deceptive Design Patterns.

⁸⁷ See Article 5(2) DMA. In addition, see Recital 36 of the DMA: ‘[t]o ensure that gatekeepers do not unfairly undermine the contestability of core platform services, gatekeepers should enable end users to freely choose to opt-in to such data processing and sign-in practices by offering a less personalised but equivalent alternative, and without making the use of the core platform service or certain functionalities thereof conditional upon the end user’s consent.’ Recital 37 of the DMA adds that: ‘[t]he less personalised alternative should not be different or of degraded quality compared to the service provided to the end users who provide consent, unless a degradation of quality is a direct consequence of the gatekeeper not being able to process such personal data or signing in end users to a service’. See also Article 38 of the DSA ‘[...] providers of very large online platforms and of very large online search engines that use recommender systems shall provide at least one option for each of their recommender systems which is not based on profiling as defined in Article 4, point (4), of Regulation (EU) 2016/679’.

⁸⁸ EDPB Guidelines on consent, paragraphs 46 – 48. See also paragraph 24.

⁸⁹ EDPB Guidelines on consent, paragraph 46.

84. If a data subject refuses to give their consent to the data processing for behavioural advertising purposes, and there are no other free of charge alternatives allowing them to access the same service, the data subject would face a financial consequence, as they would have to pay a fee in order to be able to use the service. This would especially be the case where there are lock-in effects present and the user has been able to use the service for a prolonged amount of time without a fee being present.
85. In order to avoid detriment within the meaning of Recital 42 GDPR and ensure that data subjects have the possibility to make a genuine choice, the manner in which the service is offered⁹⁰ as well as the fee (if any) should not be such to effectively inhibit data subjects from making a free choice, for example by nudging the data subject towards consenting. Therefore, the fee in question should not be inappropriately high, which is further addressed in Section 4.2.1.4.2.
86. If the data subject refuses to consent or withdraws consent, and does not pay the requested fee, they would not be able to use the service, which may constitute a detriment for the data subject. In these cases, various factors may lead to the data subjects facing detriments.
87. Data subjects may suffer detriment if it becomes impossible for them to use a service that is part of their daily lives and has a prominent role. This could be the case, for instance, of a platform that is commonly and systematically used to disseminate information that may not be readily available from other sources, or of a platform whose use is necessary to have access to certain services relevant for the individual's daily life. This may be information or exchanges which the users are reliant upon in their daily lives, which makes it harder for them not to participate on the platform. These types of situations may range from important information during public emergencies to parents receiving information regarding social activities for their children. Additionally, the platform may be a key forum for public debate on political, social, cultural and economic issues.
88. In the same vein, the use of certain social media services might be decisive for the data subjects' participation in social life. With rapid technological innovations and the fact that most people have an online presence, the role that social media play in data subjects' day-to-day lives and interactions ought not to be underestimated. Many data subjects rely on these platforms as an important means to stay in contact with people that they do not physically interact with in their daily routines, such as friends and/or family. Considering that social media provide a particularly valuable and convenient alternative to in-person interactions, not having access to them can have important consequences on some users' emotional and psychological well-being. In the above cases, the data subjects might be shut out from the social interactions taking place on the platform and feel socially isolated, especially when there is no alternative service that offers a similar experience and is also used by the data subject's social contacts. The same goes for taking part in online discussion forums. Data subjects might be shut out of taking part in those online discussion forums, even though these now constitute an important part of online debates.
89. Data subjects can also suffer detriment if, due to not paying a fee and not consenting, they are denied access to professional or employment-oriented platforms. More specifically their possibilities to find job opportunities or build and/or maintain professional networks can be negatively affected, they may feel disadvantaged compared to users that have access to the service or unable to follow important developments in their respective fields of work.

⁹⁰ Whilst consenting can often be done by a single action, refusing consent could potentially require the data subject to go through a longer and more cumbersome payment process, possibly connected with further data processing activities.

90. Further, a detriment may be more likely to occur, and possibly of a more significant nature, in case of a large online platform in which **lock-in or network effects** may be present. The detrimental consequences of denying access to a service **can be even more important for the users of online platforms which have not been implementing ‘consent or pay’ models from the outset but have subsequently decided to introduce them.**
91. **Network effects** may make it harder for data subjects to decide not to access the service without suffering any negative consequence. This is particularly relevant for platforms which rely on user-generated content or user-to-user interaction, such as video/image-sharing platforms and platforms for communication, such as social media sites, dating platforms, discussion forums, or booking platforms with a large amount of users. If a platform has a large user base, new and existing users may consider that interacting on that particular service is necessary to join a digital community where their friends, family, colleagues are, or to participate in political discussions or conversations. Others may feel that they have to use a service in a professional context, or that they, as parents, have to use a particular site to receive information regarding their children, such as parents groups for planning social activities for children. Not interacting on the platform or choosing another service may be unrealistic, as it is difficult for an individual to, as an example, convince their social, professional or political circles to move from one service to another which does not track their users.
92. Any **lock-in effects** may also lead to detriment for data subjects. Users who have used the platform for a while may have already established their online presence on the platform invested in it, for example as regards connections and interactions with other users, creating content, gaining followers and ‘likes’, etc. This effect is further amplified when a user has spent a large amount of time on the platform, e.g. when the platform has been offered for a longer time period already. Where such users are asked to pay a fee or consent to the processing of their personal data for behavioural advertising purposes in order to continue using the service, but they refuse to do so and lose access to the service, they risk not being able to bring their interactions, followers and connections to a new platform, and/or losing content and information that they have compiled or generated while previously using the service. This could encompass a wide range of material, such as personal communication, contact lists, search history, saved preferences, images, dashboards, different kinds of personalised databases etc. For a content-creator on a media sharing-site, this may entail a very substantial and potentially irreparable loss for the user, in the sense of a possible financial loss, the loss of a portfolio a creator might have built over the years on a platform and a loss of following.
93. In this context, it is important to recall the importance of data subject’s rights and the fact that these rights should always be respected by the controller. Even in the case where a data subject would no longer have access to the service, they would still be entitled to exercise their rights as a data subject under the GDPR, for example the right to access their personal data and the right to data portability. It is the responsibility of the controller to inform the data subjects of this when providing the data subjects with the choice to either give their consent or not and ensuring that the ability to exercise these rights will be maintained.
94. If any of the (non-exhaustive) negative consequences described in the paragraphs above are present, offering the sole choice between a paid service and a service entailing behavioural advertising based on the data subject’s consent would impact the possibility for data subjects to make a genuine choice and withhold consent without detriment.
95. In light of the above, detriment is likely to occur when large online platforms use a ‘consent or pay’ model to obtain consent for the processing. As mentioned above in Section 4.2.1.1, whether the controller offers the Free Alternative Without Behavioural Advertising as a further alternative would

play a relevant role to remove, reduce or mitigate the detriment that may arise for non-consenting users from either having to pay a fee to access the service or not being able to access it.

4.2.1.3 Imbalance of power

96. In the first part of Recital 43 GDPR it is stated that the power dynamic between the data subject and the controller is relevant in the assessment of whether the data subject's consent was freely given:
- “In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. (...)”*
97. Because ‘freely given’ means that the data subject must exercise autonomy, it is necessary to consider the position of the controller, and the power they have in relation to the data subjects. If there is a clear imbalance between the controller and the data subject in a given situation, the data subject may feel compelled to make a decision they otherwise would not have made, which impinges on their freedom of choice. As previously mentioned, Recital 43 GDPR makes it clear that consent cannot, as a rule, be used as a legal basis in a situation of clear imbalance.
98. As previously indicated by the EDPB, where a clear imbalance exists, consent can only be used in ‘exceptional circumstances’ and where the controller, in line with the accountability principle, can prove that there are no ‘adverse consequences at all’ for the data subject if they do not consent, notably if data subjects are offered an alternative that does not have any negative impact⁹¹. In the context of this Opinion, such an alternative could be the offering of the Free Alternative without Behavioural Advertising (see Section 4.2.1.1).
99. All controllers who use consent as a legal basis must assess whether they are in a situation of clear imbalance of power. When the controller is a ‘large online platform’ as defined for the purposes of this Opinion, certain elements can be taken into account to verify whether there is a situation of clear imbalance of power. Several of these non-exhaustive and non-cumulative factors are listed below. Some of these will be more relevant for certain controllers, and less so for others. A case by case evaluation of these factors should always be necessary.
100. A first factor that can be relevant is the **position of the company in the market**. In this regard, it can be recalled that a clear imbalance might be more evident where there is a formal relationship between the controller and the data subject, such as when the controller is a public authority or an employer⁹². However, as the EDPB has previously pointed out, imbalances of power are not limited to public authorities and employers and may also occur in other situations⁹³. The real and specific factors of the individual case should always be assessed.
101. The GDPR does not provide any explicit guidance on how a controller's position in the market factors in to the assessment of whether there exists a situation of clear imbalance. The CJEU stated in the

⁹¹ EDPB Guidelines on consent, paragraph 22 and Example 5.

⁹² See also the EDPB Guidelines on consent, section 3.1.1.

⁹³ EDPB Guidelines on consent, paragraph 24.

Bundeskartellamt judgement that the existence of a dominant position ‘may create a clear imbalance’⁹⁴. The Court also stated that this is ‘an important factor’ in the assessment⁹⁵.

102. The term ‘dominant position’ is well established in EU competition law. Controllers of large online platforms may find the considerations used to determine a company’s dominant position useful when assessing whether there is a clear imbalance of power. These considerations include defining the relevant market (such as the product market and the geographic market), and identifying the market share as well as the barriers to entry or expansion⁹⁶.
103. Furthermore, the Advocate General stated in his opinion in the case that a controller does not need to have a ‘dominant position’ within the meaning of Article 102 TFEU for their market power to be considered relevant for enforcing the GDPR⁹⁷. The EDPB shares the view of the Advocate General on this point.
104. It must be recalled, however, that the CJEU stated that the validity of a data subject’s consent must be determined in light of Articles 4(11) and 7 GDPR and its recitals. Furthermore, the purpose of the rules on valid consent is to ensure that data subjects enjoy autonomy and freedom of choice. In the view of the EDPB, controllers should assess on a case-by-case basis whether the data subjects’ freedom of choice is limited. Whether or not a controller has a ‘dominant position’, while relevant when assessing the imbalance of power, does not determine the validity of consent *per se*.
105. In light of the above, it can be concluded that, depending on the circumstances of the concrete case, there might be situations where supervisory authorities might conclude on the existence of clear imbalance within the meaning of the GDPR, without a dominant position being established. The crucial question is whether the controller’s position in the market, by itself or in combination with other factors, leads the data subjects to experience that there are no other realistic alternative services available to them, such as video sharing-platforms, job application portals, or platforms for buying and selling certain goods and services.
106. More generally, as recalled above in Section 4.1, in line with the principle of fairness, power balance should be a key consideration of the controller-data subject relationship: power imbalances should be avoided or, where this is not possible, they should be recognised and accounted for with suitable countermeasures⁹⁸. This is with a view to ensuring that the data subject can engage in a genuinely free choice when consenting to the processing of personal data.
107. When assessing whether a clear imbalance exists, the considerations made in Section 4.2.1.2 above are also relevant. Indeed, in the context of large online platforms implementing ‘consent or pay’ models, the criterion of ‘imbalance of power’ and ‘detriment’ for the assessment of whether consent is freely given are strongly connected.
108. In particular, the existence of network or lock-in effects, as described above, may make it harder or unrealistic for a user to choose another service. In instances where the platform has a much larger user

⁹⁴ CJEU *Bundeskartellamt* judgment, paragraph 149.

⁹⁵ CJEU *Bundeskartellamt* judgment, paragraph 154.

⁹⁶ A general methodology for defining the relevant market can be found in Commission Notice C/2024/1645. See also the EU Commission Communication — Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings (2009/C 45/02), OJ C 45, 24.2.2009, p. 7-20, as amended in 2023 (C/2023/1923, OJ C 116, 31.3.2023, p. 1–5).

⁹⁷ Case C-252/21, Opinion of Advocate General Rantos, delivered on 20 September 2022, ECLI:EU:C:2022:704, paragraph 75.

⁹⁸ EDPB Guidelines on Data Protection by Design and by Default, paragraph 70.

base compared to any relevant alternatives, or the user has significantly invested in the platform, the user may feel compelled to rely on the platform; in these cases and choosing another service may be unrealistic or convincing their social, professional or political circles to move from one service to another may be difficult. Furthermore, and as explained above, lock-in effects may entail that popular or relevant content is centered around a particular platform, which may also influence the power balance in relation to new users looking to access such content.

109. Particular caution is warranted for services which have built a large user base while offering their services without a fee for all users. Such services may have attracted a large number of users that do not have willingness or ability to pay a fee, and who availed of the service trusting that it would not have a financial impact on them. The users may over time have increased their reliance on the service due to *inter alia* network effects and lock-in effects. If such a service subsequently starts providing users with a choice between processing of personal data and paying a fee, this could be seen as an example of leveraging a clear imbalance against users, as users are not likely to be able to exercise free choice in this situation.
110. Another important factor in assessing imbalance is the extent to which the data subject **relies on the service** provided. The data subject's experience of having a genuinely free choice is limited if the service is considered essential, e.g. to search for jobs, to get access to essential information for the data subjects' daily life or to participate in the public debate⁹⁹.
111. Additionally, the **target or predominant audience** of the platform is an element to be considered. For example, if the platform is primarily directed at children, through the design or marketing of the service, or it is used predominantly by children or other vulnerable persons, this may also lead to a clear imbalance between the controller and the data subjects¹⁰⁰.
112. The above are examples of elements that, when present, might create a situation of imbalance of power in the relationship between the data subject and the controller.
113. A controller may argue however, that the data subjects are not forced to consent or pay. They may opt not to use the service at all, or use another service which does not process personal data in the same manner as the controller. Firstly, the elements described above may result in a situation where there is no real practical option for the users to refuse to use the service. Secondly, as mentioned in Section 4.2.1.4.1 below, the EDPB stated in its Guidelines on consent that consent cannot be considered freely given simply because there is another similar service provided by a different controller which does not entail consenting to the processing of personal data for additional purposes¹⁰¹.

⁹⁹ In these cases the data subject may feel compelled to accept tracking. The EDPB has previously stated that consent can only be valid if there are no elements of compulsion or pressure, see EDPB Guidelines on consent, paragraph 24.

¹⁰⁰ In this regard, the EDPB recalls that operators of online platforms under the DSA should not present advertisements on their interface based on profiling, as defined in GDPR Article 4(4), using personal data of the recipient of the service when they are aware with reasonable certainty that the recipient of the service is a minor, see Article 28(2) DSA.

¹⁰¹ EDPB Guidelines on consent, paragraph 38.

4.2.1.4 Conditionality

114. Pursuant to Article 7(4) GDPR, when assessing whether consent is freely given, utmost account shall be taken of whether data subjects are asked to consent to processing activities not objectively necessary for the contract¹⁰² in order to gain access to the service¹⁰³.
115. The EDPB has stated in its Guidelines on consent that a controller could argue to be offering data subjects a genuine choice if they are able to choose between a version of the service that includes consenting to the use of personal data for additional purposes on the one hand, and an equivalent version of the service offered by the same controller that does not involve consenting to data use for additional purposes on the other hand, and that if it is possible to have the service delivered without consenting to the other data use in question, there is no conditional service¹⁰⁴.
116. Recently, the CJEU stated in the *Bundeskartellamt* judgment that, where data processing operations are not strictly necessary for the performance of the contract, users must be free to refuse to consent to such processing operations without being obliged to refrain entirely from using the service¹⁰⁵. In this regard, the CJEU judgment mentions the obligation to offer ‘an equivalent alternative not accompanied by such data processing operations’ (‘if necessary for an appropriate fee’)¹⁰⁶.
117. This statement by the CJEU indicates that ‘consent or pay’ models are not prohibited in principle. At the same time, the Court did not provide any more details on the meaning of the expressions ‘equivalent alternative’, ‘if necessary for an appropriate fee’. The EDPB wishes therefore to clarify that its interpretation of this part of the judgment is that data subjects opting not to consent must be offered an ‘equivalent alternative’: this can avoid the situation where data subjects would be faced with a situation of conditionality leading to invalid consent. In this regard, please see paragraph 73.
118. However, this statement of the CJEU mainly addresses the aspect of conditionality. Controllers should ensure that all the conditions for consent to be freely given, and generally to be valid, are met. Therefore, it will always be necessary to carry out a case-by-case assessment as to whether consent is valid.

4.2.1.4.1 Providing an ‘equivalent alternative’

119. The EDPB wishes to provide criteria that can help assessing whether an alternative version of the service is to be regarded as equivalent to the version of the service provided under the condition of consent to the processing of personal data for behavioural advertising purposes (referred to in this

¹⁰² EDPB 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, adopted on 8 October 2019 (hereinafter, ‘EDPB Guidelines on Article 6(1)(b) GDPR’, paragraphs 30–33).

¹⁰³ See also in this regard Recital 43 GDPR and EDPB Guidelines on consent, paragraphs 25-41.

¹⁰⁴ EDPB Guidelines on consent, paragraph 37.

¹⁰⁵ CJEU *Bundeskartellamt* judgment, paragraph 150. In paragraph 102, within the section dealing with the question of the applicability of Article 6(1)(b) as a lawful basis for processing, the CJEU also states that the provision of personalised content is ‘useful to the user’ but ‘does not appear to be necessary in order to offer that user the services of the online social network’, therefore those services ‘may, where appropriate, be provided to the user in the form of an equivalent alternative which does not involve such a personalisation, such that the latter is not objectively indispensable for a purpose that is integral to those services’.

¹⁰⁶ CJEU *Bundeskartellamt* judgment, paragraph 150.

section as '**Version With Behavioural Advertising**'). The EDPB has highlighted, in this regard, that 'both services need to be genuinely equivalent'¹⁰⁷.

120. The EDPB has stated that consent cannot be considered freely given if a controller argues that a choice exists between its service (including consenting to the use of personal data for additional purposes) and an equivalent service offered by a different controller, since freedom of choice would be made dependent on what other market players do and whether a data subject would find the other controller's services genuinely equivalent¹⁰⁸. In this context, therefore this Opinion refers to an **alternative version of the service at hand offered by the same controller** that does not involve consenting to the processing of personal data for behavioural advertising purposes (referred to in this section as '**Alternative Version**').
121. If the Alternative Version differs from the Version With Behavioural Advertising only to the extent necessary as a consequence of the controller not being able to process personal data for behavioural advertising purposes, it can be in principle regarded as equivalent.
122. In other cases, the assessment can depend, taking the Version With Behavioural Advertising as point of departure, on whether the Alternative Version in essence contains the same elements and functions. While equivalence exists if the Alternative Version includes in principle the same features and functions (functional equivalence), the Alternative Version and the Version with Behavioural Advertising do not have to be absolutely identical.
123. If, compared to the Version With Behavioural Advertising, the Alternative Version is not of a different or degraded quality, and no functions are suppressed (unless any changes are a direct consequence of the controller not being able to process personal data for the purposes for which it sought consent)¹⁰⁹, then the Alternative Version can likely be considered to be genuinely equivalent to the Version With Behavioural Advertising.
124. The more the Alternative Version differs from the Version With Behavioural Advertising, the less likely it is for the Alternative Version to be considered as genuinely equivalent, although this remains a case-by-case assessment.
125. Equivalence - meaning 'having the same value' - points in two directions. On one hand, as indicated above, if the Alternative Version was of a lower quality or is less rich in functionalities than the Version With Behavioural Advertising, users would not be presented with a real choice.
126. On the other hand, the possibility of including additional functionalities in the Alternative Version should be evaluated with caution: this is because a genuine equivalence between the versions of the service, as described above, has to be maintained, and users need to be able to make a genuine choice.
127. Importantly, the CJEU refers to the provision of an equivalent alternative '**not accompanied by such data processing operations**'¹¹⁰, i.e. by the data processing operations that are not necessary for the

¹⁰⁷ EDPB Guidelines on consent, paragraph 37.

¹⁰⁸ EDPB Guidelines on consent, paragraph 38.

¹⁰⁹ See also DMA Recitals 36, 37: the DMA gives guidance for conditions of equivalence of a service, stating the 'less personalised alternative should not be different or of degraded quality compared to the service provided to the end users who provide consent'. While the DMA is neutral on the nature of what a 'less personalised' alternative could be, the principles laid out there are helpful in the given context. See also Section 4.2.1.2 ('Detriment').

¹¹⁰ CJEU *Bundeskartellamt* judgment, paragraph 150.

provision of the service and rely on consent. Hence, since processing for behavioural advertising purposes is not necessary for the provision of the service and relies on consent, this processing has to be omitted in the Alternative Version. The EDPB wishes to recall that this is not limited to serving data subjects with ads personalised on the basis of their profile, as indicated in the definition of behavioural advertising in Section 2.1.2. Rather, it also relates to the different processing activities that controllers carry out for behavioural advertising purposes, starting from the initial tracking of users for such a purpose. Therefore, the Alternative Version should in principle also omit the processing operations that would be carried out as a precondition of processing for behavioural advertising purposes¹¹¹.

128. However, the EDPB highlights that in case controllers carry out, within the Alternative Version, tracking for purposes other than behavioural advertising purposes, e.g., for security purposes, such processing operations do not necessarily have to be omitted, provided that they fully comply with the requirements set by the GDPR, including the need to rely on an appropriate lawful basis under Article 6 GDPR and Article 5(3) of the ePrivacy Directive.
129. Additionally, as highlighted in Section 4.2.2 on ‘Informed consent’, compliance with the principles of transparency and fairness¹¹² and with transparency obligations is of crucial importance also for the purpose of ensuring that the user has a genuine choice. Therefore, the user must be in a position to fully compare all the alternative options provided by the controller. The user should understand the implications of consenting to the processing for behavioural advertising purposes, leading to the Version With Behavioural Advertising, and of choosing the Alternative Version. The user should also be able to and understand the consequences of their choice in terms of which processing operations are carried out in each case and as to the details of the alternative options provided.

4.2.1.4.2 *‘if necessary for an appropriate fee’*

130. The EDPB wishes to recall first and foremost that **personal data cannot be considered as a tradeable commodity**¹¹³. The right to data protection is enshrined inter alia in Article 8 of the Charter for Fundamental Rights and is a right that applies to all, regardless of payment or financial status.
131. While the English version of the Court’s judgment states that an appropriate fee may be imposed on non-consenting users ‘if necessary’, the other language versions use different terminology for this element of the assessment. For example, the French version uses the term ‘le cas échéant’, whereas the German version uses ‘gegebenfalls’. The EDPB considers **that certain circumstances should be present for a fee to be imposed**, taking into account both possible alternatives to behavioural advertising that entail the processing of less personal data and the data subjects’ position. This is suggested by **the words ‘necessary’ and ‘appropriate’**, which should, however, not be read as requiring the imposition of a fee to be ‘necessary’ in the meaning of Article 52(1) of the Charter and EU data protection law. Such wording should be understood in a way that is compatible with the different language versions of the judgment.
132. In other words, **controllers should assess, on a case-by-case basis, both whether a fee is appropriate at all and what amount is appropriate in the given circumstances, bearing in mind the requirements of valid consent under the GDPR as well as the need of preventing the fundamental right to data**

¹¹¹ These stages might include the observation of the user’s behaviour and collection of the personal data necessary for the behavioural advertisement.

¹¹² See Article 5 (1)(a) GDPR.

¹¹³ EDPB Guidelines on Article 6(1)(b) GDPR, paragraph 54; Directive 2019/770, Recital 24.

protection from being transformed into a feature that data subjects have to pay to enjoy, or a premium feature reserved for the wealthy or the well-off.

133. While the *Bundeskartellamt* judgment does not specify the elements upon which an assessment of appropriateness should rely, the EDPB recalls that the issue of what constitutes valid consent is an assessment of data protection law. This entails that **the assessment of valid consent should be rooted in the data protection principles and the objectives that the GDPR seeks to fulfil.**
134. When controllers offer a paid service as the alternative to a service entailing behavioural advertising based on the processing of personal data for which consent is needed, they should among others **ensure that the fee does not hinder data subjects to withhold consent, nor make them feel compelled to consent.** Controllers should assess whether they offer a **genuine choice for data subjects and are not nudging data subjects towards consenting.** The imposition of a fee should respect data subjects' **autonomy**, and data subjects should have a real choice between consenting or not. Controllers should assess whether the fee for their paid version of the service allows data subjects to validly give consent to the processing of their personal data for a version of the service entailing behavioural advertising.
135. When determining whether the fee may hinder the data subject's ability to consent, controllers should pay special attention to the principles of data protection in Article 5 GDPR. **Fairness** should be a guiding principle¹¹⁴ for the determination of what an appropriate fee is in the given case. Presenting data subjects with additional options, as discussed in Section 4.2.1.1, makes it easier to justify as fair the fee imposed for the access to the service to non-consenting users because of the enhanced freedom of choice for users.
136. The **accountability principle** in Article 5(2) GDPR is key in this regard. Businesses are free to set their own prices and choose how their revenue models are structured, but this right should be balanced with the fundamental right for individuals to protection of their personal data. The accountability principle entails that controllers have the responsibility to ensure and to document that consent is freely given if they charge a fee for access to the version of the service that does not entail behavioural advertising. Controllers should document their choices and assessment of whether a given fee is appropriate in the specific case to demonstrate that imposing the fee does not effectively undermine the possibility of freely given consent in the situation at hand.
137. As recalled above in paragraph 32, **supervisory authorities are tasked with enforcing the application of the GDPR, including the requirements of valid consent.** This may also relate to the impact of any fee on the data subjects' freedom of choice. While it is for controllers to set the amount of a fee in itself, if supervisory authorities find that consent is not freely given or that the accountability principle has not been complied with, they can intervene and impose corrective measures. In this respect, they are competent to review or evaluate the assessment of appropriateness carried out by controllers. It is for supervisory authorities to ascertain to which extent it is appropriate to investigate this matter¹¹⁵.
138. The EDPB highlights that enforcing the GDPR is a task of supervisory authorities. Assessing whether consent is valid and freely given is not a task that can be outsourced. However, there are many circumstances in which supervisory authorities may benefit from consulting authorities in other fields of law, including in particular consumer protection and competition authorities, in line with the

¹¹⁴ In this regard, see EDPB Guidelines on Article 25 Data Protection by Design and by Default, Version 2.0, paragraph 70.

¹¹⁵ See Article 57(1)(f) GDPR, which is also relevant for *ex officio* investigations.

principle of sincere cooperation under Article 4(3) TEU, as recently underlined by the CJEU¹¹⁶. If appropriate, supervisory authorities may choose to consult with such authorities in the exercise of their tasks. Consultation with such authorities may be legally mandatory where supervisory authorities apply or interpret fields of EU law that are subject to other authorities' supervision.

4.2.1.5 Granularity

139. Another condition with regard to consent being freely given relates to granularity. Granularity is a key element when assessing whether the purposes are sufficiently separated. When presented with a 'consent or pay' model, the data subject should be free to choose the individual purpose(s) they accept, rather than having to consent to a bundle of processing purposes. Reference to granularity in the GDPR can be found in Recital 43 GDPR, in which it is clarified that consent is presumed not to be freely given if the request for consent does not allow data subjects to give separate consent for different purposes of processing¹¹⁷. Granularity is closely related to the requirement for consent to be specific, as further discussed in Section 4.2.3¹¹⁸. As previously stated by the EDPB, 'When data processing is done in pursuit of several purposes, the solution to comply with the conditions for valid consent lies in granularity, i.e. the separation of these purposes and obtaining consent for each purpose'¹¹⁹.
140. Granularity of consent in relation to behavioural advertising by large online platforms merits special attention, as the complex dynamics at play present significant challenges. In this context, it should be noted that online platforms that are involved in behavioural advertising use technically advanced infrastructure, which are often part of a digital ecosystem in which multiple data points originating from different sources are most likely combined, analysed and may be subject to real time auctioning. Given these different dynamics, controllers cannot present data subjects with blanket consent for a number of different purposes, e.g. personalisation of content, personalisation of advertisements, service development, service improvement, audience measurement. In this vein, the EDPB recalls that the data subjects should be free to choose which purpose they accept, rather than being confronted with one consent request bundling several purposes. The emphasis in this regard should be placed on differentiating the purposes related to the functionality of the service from behavioural advertising purposes, and processing operations accompanied by this¹²⁰. The considerations made in this regard in Sections 4.2.2 and 4.2.3 on informed and specific consent are also relevant in this case.

¹¹⁶ CJEU *Bundeskartellamt* judgment, paragraph 53: 'Under that principle, in accordance with settled case-law, in areas covered by EU law, Member States, including their administrative authorities, must assist each other, in full mutual respect, in carrying out tasks which flow from the Treaties, take any appropriate measure to ensure fulfilment of the obligations arising from, inter alia, the acts of the institutions of the European Union and refrain from any measure which could jeopardise the attainment of the European Union's objectives.'

¹¹⁷ Recital 32 GDPR states 'Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them'.

¹¹⁸ See EDPB Guidelines on consent, paragraphs 42 and 55.

¹¹⁹ EDPB Guidelines on consent, paragraph 44.

¹²⁰ Such purpose may also concern technical processing operations intrinsically linked to the advertising purpose, such as frequency capping or measuring the effectiveness of ad campaigns. See EDPB reply to the Commission's Initiative for a voluntary business pledge to simplify the management by consumers of cookies and personalised advertising choices, p. 7 of the Annex.

4.2.2 Informed consent

141. Explicit mention of informed consent can be found in Recital 42 GDPR: ‘for consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended’.
142. Providing information to data subjects **prior to obtaining their consent** is essential to enable them to make informed decisions and understand what they are agreeing to. If the controller does not provide accessible information, the user’s control becomes illusory and the consent will be invalid.
143. Therefore, it is necessary to inform the data subject of certain elements that are crucial to make a genuine choice. Depending on the context, more information may be needed to allow the data subject to **genuinely understand the processing operations** at hand¹²¹.
144. As the condition of informed consent is also related to the overarching principles such as transparency, fairness and accountability, regard shall be had to these principles when assessing ‘consent or pay’ models (see Section 4.1 above). Further, as the conditions of informed and specific consent concern the level and quality of the information to be provided to the data subject, Section 4.2.2 and Section 4.2.3 of the present Opinion should be understood as complementing each other.

4.2.2.1 Content requirements for consent to be informed

145. In the context of the ‘consent or pay’ models, large online platforms should determine what information should be provided to data subjects about the processing of their personal data for behavioural advertising purposes. In general, controllers have the responsibility, under the principle of accountability, to build up and document an information process enabling data subjects to have a full and clear comprehension of the value, the scope and the consequences of their possible choices.
146. By using the terms ‘at least’, Recital 42 GDPR does not provide an exhaustive list of information to be transmitted to the data subject to ensure informed consent. The identity of the controller and the description of the purposes of the processing activities are minimum requirements. Such requirements shall be adapted on a case-by-case basis, depending on the processing activities planned by the controller¹²².
147. The wording ‘the data subject should be aware’ establishes a responsibility upon controllers to make sure users understand what data processing will be performed by the controller when they start using the service. This includes a duty to inform users of processing activities that run in the background and of which they may not be aware. If the appropriate information is not provided, an information asymmetry may occur and data subjects may not be able to foresee the manner in which their personal data will be processed¹²³. Large online platforms should ensure that data subjects have a clear

¹²¹ The EDPB notes that the CJEU issued a judgment in which it is specified that information ‘must enable the data subject to be able to determine easily the consequences of any consent’ and ‘ensure that the consent given is well informed’. Judgment of the Court of Justice of the European Union of 11 November 2020, *Orange Romania v Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)*, C-61/19, ECLI:EU:C:2020:901,, paragraph 40.

¹²² On the minimum content requirements for consent to be ‘informed’, see Section 3.3.1. in EDPB Guidelines on consent.

¹²³ In this respect, the EDPB notes that Articles 7(1) and (2) of the Unfair Commercial Practice Directive (Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial

understanding of the processing activities and of any changes affecting them, for example when such a platform switches to a 'consent or pay' model.

148. In the context of behavioural advertising, it is important to provide information that is sufficiently granular, so that data subjects can understand which aspects of the service they consent to, while retaining the possibility not to consent to others. Granular information enabling data subjects to differentiate between different purposes of processing is a requirement for valid consent. In this regard, large online platforms should not require data subjects to consent to processing activities the purpose of which is not appropriately defined or ambiguous. For example, it should be clear to the data subject for which purposes their data is being collected, what data is being collected for each purpose and why¹²⁴. Large online platforms should not define the purpose of the processing activity in terms that are too broad for the data subject to understand the consequences of their choice (e.g. 'commercial purposes' or 'personalisation'). The considerations provided in Section 4.2.3 on the requirements for specific consent are also relevant in this respect.
149. Large online platforms should describe in a fair and complete manner the purpose for which the consent is collected. For example, large online platforms may not limit the description of the purpose of the processing to the advantages it provides to the data subjects (e.g. a more personalised experience) if such processing also entails other consequences for them (e.g. profiling, intrusive tracking,...).
150. In the context of 'consent or pay' models, the choices presented to data subjects need to align with the information they are provided with. It has to be clear to the data subject what exactly they would be paying a fee for and how that would affect the data processing involved. When information about the controller's business models in each of the options is provided, such information should not substitute information on the processing of personal data.
151. Furthermore, behavioural advertising necessarily pertains to profiling of the data subject's online activities, and often entails the use of personal data obtained indirectly from the data subject. The process of profiling consists of often opaque interactions and data exchanges between the controller and third parties. This opacity may, for example, occur in the cross-use of on and off-platform data. Large online platforms may process personal data collected both on and off their platform for profiling purposes. It is the responsibility of controllers to make sure data subjects understand the techniques involved in the profiling processes¹²⁵. In this context, Recital 60 GDPR states that giving information about profiling is part of the controller's transparency obligations under Article 5(1)(a) GDPR.
152. Controllers should provide appropriate information on each version of the service they offer, including where one or more of them do not require consent for behavioural advertising purposes. This also applies to the Free Alternative Without Behavioural Advertising (see Section 4.2.1.1). The controller should be transparent about the legal basis relied on for the processing of data subjects' personal data in each of the options.

practices in the internal market, OJ C 526, 29 December 2021, p.1-129) establish an obligation for companies to provide all the information which the average consumer needs to make an informed decision.

¹²⁴ See 'Minimum content requirements for consent to be 'informed'' in EDPB Guidelines on consent, paragraphs 64 and 65.

¹²⁵ Article 29 Working Party, WP251 rev.1, 3 October 2017, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, as last revised and adopted on 6 February 2018, endorsed by the EDPB on 25 May 2018 (hereinafter, 'WP29 Guidelines on Automated Individual Decision-Making'), p. 9.

153. Large online platforms should consider in particular the following points when providing information to data subjects:
- where applicable, the recipients or categories of recipients of the personal data;
 - where applicable, the fact that the controller intends to transfer personal data to a third country and the period for which the personal data will be stored;
 - the collection and processing of data maintained by the controller irrespective of the data subject choosing to consent to the behavioural advertising;
 - the right of data subject to withdraw their consent at any time and its consequences; and
 - the combination or cross-use of data, meaning if and to what extent the data is merged with data collected by other services (of the same controller) and data collected by other controllers.

4.2.2.2 *How to provide information*

4.2.2.2.1 *Time and display of communication*

154. Large online platforms should provide complete information prior to the start of the data processing for behavioural advertising purposes. They may, for instance, present a short summary of the differences between each option offered in the ‘consent or pay’ model and then give the complete and detailed information option-by-option through distinct and separate buttons for each option.
155. The recommendations included in the EDPB Guidelines on deceptive design patterns in social media platform interfaces are relevant to define the manner in which the information should be communicated to data subjects¹²⁶. In addition, data subjects should be afforded sufficient time to assimilate the information they receive¹²⁷.

4.2.2.2.2 *Transparency requirements*

156. The Guidelines on transparency under the GDPR should be taken into account by large online platforms implementing a ‘consent or pay’ model¹²⁸.
157. Concerning the language used to provide the information, the ‘concise’ and ‘clear and plain language’ elements require from the controller to adapt the language to the data subjects¹²⁹. This means that the information should be provided in a clear and intelligible manner for the target audience.
158. In order to comply with these transparency requirements, a controller should assess what kind of audience it serves. After identifying their audience, controllers should determine what language and communication approach is appropriate. With that, they should ensure that their audience understands the service and how the use of the service affects their personal data.
159. The wording used shall clearly identify the consequences of the data subject’s choice on the processing of their personal data¹³⁰. For example, the controller shall not only explain to the data subject that

¹²⁶ EDPB Guidelines on deceptive design patterns.

¹²⁷ In this regard, see also EDPB Guidelines on deceptive design patterns, paragraphs 43-48.

¹²⁸ Article 29 Working Party, WP260 rev.01, Guidelines on transparency under Regulation 2016/679, adopted on 29 November 2017, as last revised and adopted on 11 April 2018, endorsed by the EDPB on 25 May 2018 (hereinafter, ‘WP29 Guidelines on Transparency’).

¹²⁹ WP29 Guidelines on Transparency, paragraph 13 mentioning that ‘A translation in one or more other languages should be provided where the controller targets data subjects speaking those languages’.

¹³⁰ EDPB Guidelines on consent, paragraph 70.

their choice will determine the presence or absence of advertising, but also that their choice will determine if, and to what extent, the controller will process personal data for behavioural advertising.

160. Controllers may use different channels of information depending on the type of the online platform provided. For example, information may be provided to the data subjects by means of videos explaining the differences between the alternatives, or interactive pages with examples of how the service will look like under the different options. Controllers may consider running user tests to identify the most appropriate channel of information.

4.2.3 Specific consent

161. Article 6(1)(a) GDPR states that consent must be given for 'one or more specific' purposes. The requirement that consent must be 'specific' is closely linked to the requirements that the consent must also be 'informed' and 'granular'. In order for the consent to be specific, large online platforms should define a specific, explicit and legitimate purpose for the processing activities for which consent is collected, and provide sufficient information to the data subjects on such processing activities¹³¹. A creeping expansion or blurring of the purposes (so called 'function creep') is to be avoided as this would undermine and contradict the principle of purpose limitation¹³².
162. Considering the complex system of data processing activities behind behavioural advertising, large online platforms should precisely define and delimit the purposes of their processing activities. The behavioural advertising purposes have to be presented by the controller so as to allow the user to understand which processing activities take place for each purpose and decide whether to provide their consent¹³³.
163. Large online platforms should assess and document on a case-by-case basis whether providing behavioural advertising entails for them to process personal data for different purposes, and to require separate consents for these purposes¹³⁴. Conversely, technical processes that may be inextricably linked to a single purpose may not require separate consents¹³⁵. The considerations made in section 138 (on granularity) and section 4.2.2 (on informed consent) should also be taken into account.

4.2.4 Unambiguous indication of wishes

164. For consent to be valid under Article 4 (11) GDPR, it must be, *inter alia*, an unambiguous 'indication of the data subject's wishes in the form of a statement or by "a clear affirmative action' signifying

¹³¹ See also Recital 28, which says that purposes 'must be determined at the time of collection of the data'. EDPB Guidelines on consent, paragraph 56.

¹³² EDPB Guidelines on consent, paragraph 56.

¹³³ See WP 29 Opinion 3/2013 on purpose limitation (WP 203), p. 16: 'For these reasons, a purpose that is vague or general, such as for instance 'improving users' experience', 'marketing purposes', 'IT-security purposes' or 'future research' will - without more detail - usually not meet the criteria of being 'specific'.'

¹³⁴ See for example CJEU *Bundeskartellamt* judgment, paragraph 151: 'it is appropriate (...) to have the possibility of giving separate consent for the processing of the latter data, on the one hand, and the off-Facebook data, on the other.'

¹³⁵ EDPB reply to the Commission's Initiative for a voluntary business pledge to simplify the management by consumers of cookies and personalised advertising choices, p. 7 (where it is specified: 'If a user consents to access or storage of information in their terminal equipment for a well described advertising purpose, such purpose may concern technical processing operations intrinsically linked to the advertising purpose, such as the use of cookies for frequency capping or measuring the effectiveness of ad campaigns. Such technical processing operations may involve access or storage of information in terminal equipment').

agreement to the processing of personal data relating to him or her'¹³⁶. This means that it must be obvious that the data subject has given their consent to specific data processing¹³⁷.

165. Controllers should attentively design the way in which data subjects are asked to provide their consent, in particular where they intend to collect consent for purposes other than behavioural advertising purposes (e.g. service improvement or personalisation of content). It generally cannot be considered that data subjects are unambiguously consenting to all purposes with a single action where it would be appropriate for data subjects to be able to express more detailed preferences.
166. In the context of 'consent or pay' models, users are requested to provide consent to certain processing activities in order to access the service without paying a fee. When a user provides consent to the processing activities that are allowing to access the service for free, it should be considered that user is providing consent to those processing activities only, bearing in mind the requirements for consent to be 'specific'. In order for consent to be regarded as clearly given for other purposes, these purposes should be actively selected by the user.
167. Another aspect that is important for the existence of an unambiguous indication of wishes is that the user is not exposed to deceptive design patterns and that the different options are equally presented. In this regard the EDPB also recalls its Guidelines on Deceptive design patterns in social media platform interfaces¹³⁸.
168. With 'consent or pay' models, it is for example important to remember that users can be misled into giving their consent if controllers are providing ambiguous information. This is the case if the consent is collected via wording such as 'simply continue' or 'continue without payment'¹³⁹. In these cases, non-payment is emphasised in such a way that it is unclear choosing the free option implies to consent.¹⁴⁰ To ensure that there is an unambiguous indication of wishes, the questions asked should therefore be framed in an accurate and transparent way, and consent to processing of personal data should not be presented as merely a possibility to avoid paying a fee.

4.3 Additional elements

4.3.1 Withdrawal of consent

169. Article 7(3) GDPR states that the data subject shall have the right to withdraw their consent at any time. In addition, according to Article 7(3) GDPR it 'shall be as easy to withdraw as to give consent'¹⁴¹. The requirement of an easy withdrawal is a necessary aspect of valid consent in the GDPR¹⁴². There is no set specific solution for implementation of these requirements. It is therefore generally necessary to review on a case-by-case basis whether an easily accessible withdrawal option is provided that

¹³⁶C-61/19, *Orange Romania*, ECLI:EU:C:2020:901 paragraph 36.

¹³⁷EDPB Guidelines on consent, paragraph 75.

¹³⁸ EDPB Guidelines on deceptive design patterns.

¹³⁹ EDPB Guidelines on consent, paragraph 84.

¹⁴⁰ See EDPB Guidelines on deceptive design patterns, Annex I checklist 4.6.2.

¹⁴¹ This does not have to happen always through the same action, but when consent is obtained via electronic means through only one mouse-click, swipe, or keystroke, data subjects must, in practice, be able to withdraw that consent equally as easily. EDPB Guidelines on consent, paragraphs 113-114.

¹⁴² EDPB Guidelines on consent, paragraph 116.

fulfills the legal requirements¹⁴³. This also depends on whether the option to withdraw consent is clearly and distinctly recognizable and not presented in a deceiving or manipulating design¹⁴⁴.

170. It is mandatory that the controller informs the data subject of the right to withdraw consent before consent is actually given¹⁴⁵. The controller must also inform data subjects of how this right can be exercised¹⁴⁶.
171. Data subjects should be able to withdraw their consent without detriment¹⁴⁷. It is important to note that, when a data subject does experience detriment when withdrawing consent, it can be concluded that consent was never validly obtained and it is the responsibility of the controller to delete all personal data about the user that has been collected on the basis of such invalid consent¹⁴⁸.
172. In the context of 'consent or pay' models to be considered here, a distinction must first be made between the exercise of the right of withdrawal as such and the user's wish to continue the use of the service after withdrawal of consent. It is important that transparent and clearly recognizable information is provided on how the right of withdrawal can be exercised, in order to avoid giving the impression that the withdrawal would automatically lead to entering into a paid subscription. In such cases, exercising the right of withdrawal will result in the user being once again faced with the choice of whether to give consent to the processing for behavioural advertising purposes or take out a paid subscription (or opt for the Free Alternative Without Behavioural Advertising where this is offered). This consequence should be answered in the same way as the general question of whether a free choice can be made in the case of 'consent or pay' models. The standard for determining whether there is a detriment is therefore referred to the explanations under Section 4.2.1.2 ('Detriment'). If it is assessed in an individual case that a free choice can be made, this should also apply to withdrawal, as this would otherwise always lead to invalidity of the consent.
173. Irrespective of this, it should be clear that a user's decision to subscribe to the paid version of service when they had first initially provided their consent to the processing for behavioural advertising purposes constitutes a withdrawal of their consent. Conversely, the termination of the paid subscription is not equivalent to giving consent.
174. In order to assess whether the right of withdrawal fulfills the requirements of the GDPR, the consequences of exercising the right of withdrawal should also be considered. The EDPB Guidelines on consent explain that, as a general rule, if consent is withdrawn, all processing operations that were based on consent and took place before the withdrawal of consent and in accordance with the GDPR remain lawful, but the controller must stop the related processing operations¹⁴⁹. If there is no other lawful basis justifying the processing, including the further storage, of the data, they should be deleted by the controller¹⁵⁰.

¹⁴³ Please see the Report of the work undertaken by the EDPB Cookie Banner Taskforce, paragraph 35.

¹⁴⁴ See also Recital 37 of the DMA: 'Lastly, it should be as easy to withdraw consent as to give it. Gatekeepers should not design, organise or operate their online interfaces in a way that deceives, manipulates or otherwise materially distorts or impairs the ability of end users to freely give consent.'

¹⁴⁵ Article 7(3) GDPR.

¹⁴⁶ EDPB Guidelines on consent, paragraph 116.

¹⁴⁷ Recital 42 of the GDPR, EDPB Guidelines on consent, paragraphs 46, 114.

¹⁴⁸ EDPB Guidelines on consent, paragraph 49.

¹⁴⁹ EDPB Guidelines on consent, paragraph 117

¹⁵⁰ EDPB Guidelines on consent, paragraph 117.

175. The withdrawal of consent to processing for behavioural advertising purposes should therefore lead to the termination of all processing activities allowed by the data subject's consent. This does not only affect the storage of and/or the access to the data on the terminal equipment for behavioural advertising purposes but also the subsequent processing of the data collected for such purposes (e.g., where this data is further shared with third parties). This is especially relevant in circumstances where the controller uses a large advertising network to target individuals and track them across several websites.
176. The conclusions of the CJEU in the *Proximus* judgment¹⁵¹ also apply in the context of behavioural advertising, especially under the use of online marketing methods like real time bidding. It would also be contradictory to the principle of making withdrawal as simple as consenting if the user himself had to exercise his or her right of withdrawal against each controller involved, where consent can be given to all of them with one click. In addition, particularly when creating and enriching user profiles that are used for behavioural advertising, profiles should be deleted after consent is withdrawn and they should not be processed, including for another purpose based on a different legal basis, except when personal data are processed for another purpose with a valid legal basis from the outset.

4.3.2 Refreshing consent

177. The GDPR does not set a specific time limit as to how often consent should be refreshed, or for how long consent can be considered as expressing the data subject's wishes. Controllers should conduct this assessment on a case-by case basis.

The EDPB provided in its guidelines criteria which could guide controllers in identifying how long consent should be considered to last, including the context, the scope of the original consent and the expectations of the data subject¹⁵². Provisions included in other EU legislation might have to be considered in such assessment, depending on the specific circumstances of each case, such as the one provided under Article 5(2) DMA.

178. In the context of behavioural advertising, considering the intrusiveness of the processing, a limited period of time during which consent remains valid, such as one year, seems appropriate¹⁵³.

¹⁵¹ CJEU, judgment in Case C-129/21, *Proximus NV v Gegevensbeschermingsautoriteit*, ECLI:EU:C:2022:833. In the *Proximus* judgement, the CJEU stated that where various controllers rely on the single consent of the data subject, it is sufficient, in order for that data subject to withdraw such consent, that he or she contacts any one of such controllers (paragraph 84). The CJEU further states: '(...) in order to ensure the effectiveness of the right of the data subject to withdraw his or her consent (...) and to ensure that the data subject's consent is strictly linked to the purpose for which it was given, the controller to which the data subject has notified the withdrawal of his or her consent to the processing of his or her personal data is in fact required to communicate that withdrawal to any person who has forwarded those data to it and to the person to whom it has, in turn, forwarded those data. The controllers thus informed are then, in turn, obliged to forward that information to the other controllers to which they have communicated such data' (paragraph 85).

¹⁵² EDPB Guidelines on consent, paragraph 110.

¹⁵³ Please see also WP29 Opinion on online behavioural advertising, p. 16.

5 CONCLUSIONS

179. In the context of ‘consent or pay’ models operated by large online platforms, the EDPB highlights the need for controllers to comply with all the requirements of the GDPR, in particular the requirements for valid consent, as described in this opinion, while assessing the specificities of each case.

It has to be concluded that, in most cases, it will not be possible for large online platforms to comply with the requirements for valid consent if they confront users only with a binary choice between consenting to processing of personal data for behavioural advertising purposes and paying a fee.

180. The EDPB recalls that personal data cannot be considered as a tradeable commodity, and large online platforms should bear in mind the need of preventing the fundamental right to data protection from being transformed into a feature that data subjects have to pay to enjoy. Therefore, the offering of (only) a paid alternative to the service which includes processing for behavioural advertising purposes should not be the default way forward for controllers. On the contrary, when developing the alternative to the version of the service with behavioural advertising, large online platforms should consider providing data subjects with an ‘equivalent alternative’ that does not entail the payment of a fee (e.g. including a different form of advertising that is not behavioural advertising).

181. Should they decide to provide data subjects with an ‘equivalent alternative’ which involves the payment of a fee, in order to ensure genuine choice and avoid presenting users with a binary choice between paying a fee and consenting to processing for behavioural advertising purposes, controllers should consider also offering a further alternative, free of charge, without behavioural advertising, e.g. with a form of advertising involving the processing of less (or no) personal data. This is a particularly important factor in the assessment of certain criteria for valid consent under the GDPR.

In most cases, whether a further alternative without behavioural advertising is offered by the controller, free of charge, will have a substantial impact on the assessment of the validity of consent, in particular with regard to the detriment aspect. The offering of a free alternative without behavioural advertising should therefore be given significant consideration by large online platforms.

182. On the basis of the request for an opinion from the Dutch, Norwegian and German (Hamburg) supervisory authorities and on the basis of the analysis above, the EDPB concludes that the **consent collected by large online platforms** (as defined for the purposes of this Opinion) **in the context of ‘pay-or-consent’ models relating to behavioural advertising may only be considered as valid to the extent that such platforms can demonstrate, in line with the principle of accountability, that all the requirements for valid consent are met**, i.e. that:

- The consent is **freely given**. In this respect, large online platforms should consider, *inter alia*, the following elements:
 - Whether the data subject suffers **detriment** as a consequence of not consenting or withdrawing consent. In this regard, large online platforms using ‘consent or pay’ models should ensure that any fee is not such as to effectively inhibit data subjects from making a free choice, for example by nudging them towards consenting. Furthermore, detriment may arise where data subjects do not pay a fee to withhold consent and thus face exclusion from the service if they do not consent, especially in cases where the service has a prominent role, or is decisive for participation in social life or access to professional networks, even more so in the presence of lock-in or network effects. As a result,

detriment is likely to occur when large online platforms use a 'consent or pay' model to obtain consent for the processing.

- Whether there is an **imbalance of power** between the data subject and them. In this respect, certain non-exhaustive and non-cumulative factors may help large online platforms in this case-by-case assessment, including the position of the company in the market, the existence of lock-in or network effects, the extent to which the data subject relies on the service, and the target or predominant audience of the service; where a clear imbalance exists, consent can only be used in 'exceptional circumstances' and where the controller, in line with the accountability principle, can prove that there are no 'adverse consequences at all' for the data subject if they do not consent, notably if data subjects are offered an alternative that does not have any negative impact.
- Whether the consent is required to access goods or services, even though the processing based on consent is not necessary for the performance of the contract applicable to the offer of such goods or services. The EDPB notes that the Court of Justice of the European Union (CJEU) stated in the *Bundeskartellamt* judgment that users refusing to give consent to particular processing operations are to be offered, 'if necessary for an appropriate fee, an equivalent alternative not accompanied by such processing operation'. In doing so, controllers will avoid an issue of conditionality. In any case, the other criteria for 'freely given' consent still needs to be fulfilled as well. The EDPB considers that the need for data subjects to be offered an '**equivalent alternative**' mentioned by the CJEU refers to an alternative version of the service at hand offered by the same controller that does not involve consenting to the processing of personal data for behavioural advertising purposes. The EDPB provides elements that can help ensuring the alternative is genuinely equivalent. If the alternative version is different only to the extent necessary as a consequence of the controller not being able to process personal data for behavioural advertising purposes, it can be in principle regarded as equivalent. Further, in the 'equivalent alternative', processing operations that are not necessary for the provision of the service and rely on consent are to be omitted. Since processing operations carried out for behavioural advertising purposes are not necessary for the provision of the service and rely on consent, such operations are to be omitted from the equivalent alternative, unless such processing operations also serve another lawful purpose.
- Whether any **fee** imposed is such as to inhibit data subjects from making a genuine choice or nudge them towards providing their consent. In respect of the imposition of any fee to access the 'equivalent alternative' version of the service, controllers should assess, on a case-by-case basis, both whether a fee is appropriate at all and what amount is appropriate in the given circumstances, bearing in mind the need of preventing the fundamental right to data protection from being transformed into a premium feature reserved for the wealthy. This evaluation should be carried out in light of the requirements of valid consent and of the principles under Article 5 GDPR, in particular the fairness principle, and taking into account both possible alternatives to behavioural advertising that entail the processing of less personal data and the data subjects' position.

Supervisory authorities are tasked with enforcing the application of the GDPR, which may also relate to the impact of any fee on the data subjects' freedom of choice. In many circumstances, supervisory authorities may benefit from consulting authorities in other fields of law, including in particular consumer protection and competition authorities.

- Whether data subjects are free to choose which purpose of processing they accept, rather than being confronted with one consent request bundling several purposes (**granularity**).
 - The consent is **informed**. Controllers have the responsibility, under the principle of accountability, of building up and documenting an information process enabling data subjects to have a full and clear comprehension of the value, the scope and the consequences of their possible choices. This means that prior to making any choice, the data subjects should be provided with clear information about the processing activities linked to each of the options offered to them. Large online platforms should take into account the complexity of the data processing activities required to provide behavioral advertising and ensure that the information is provided in a clear and intelligible manner for the target audience.
 - The consent is an **unambiguous indication of wishes**. Large online platforms should attentively design the way in which data subjects are asked to provide their consent, to ensure that data subjects are not subject to deceptive design patterns. When a user provides consent to the processing activities that allow to access the service for free, it should be considered that the user is providing consent to those processing activities only, bearing in mind the requirements for consent to be specific. In order for consent to be regarded as clearly given for other purposes, these purposes should be actively selected by the user.
 - The consent is **specific**. This means that large online platforms should precisely define and delimit the purposes of the processing activities for which consent is required. For example, the consent obtained for behavioural advertising purposes should not be bundled with other purposes. Large online platforms should assess and document on a case-by-case basis whether providing behavioural advertising entails for them to process personal data for different purposes, and to require separate consents for these purposes.
183. The EDPB recalls that **obtaining consent does not absolve large online platforms from complying with the other rules and principles provided by the GDPR**, including the principles outlined in Article 5 GDPR. The following principles are of particular importance for large online platforms implementing ‘pay-or-consent’ models, not only when assessing whether consent is valid:
- **Purpose limitation and data minimisation** - Large online platforms have the responsibility to clearly define the purpose of their processing activities, and to ensure that only personal data that is necessary to achieve this purpose is processed.
 - **Fairness** - To ensure their processing activities are fair, large online platforms should consider the impact of their processing activities on the individuals’ rights and dignity and grant the highest degree of autonomy possible to data subjects.
 - **Data Protection by Design** - Large online platforms are required to implement appropriate technical and organizational measures and to integrate the necessary safeguards into their processing activities in order to meet the requirements of the GDPR and protect the rights and freedoms of data subjects.
 - **Data Protection by Default** - Large online platforms are accountable for implementing default processing settings and options in a way that only processing that is strictly necessary to achieve the set, lawful purpose is carried out by default.
 - **Accountability** - Large online platforms are responsible for and must be able to demonstrate compliance with the GDPR, including with the principles listed above.

For the European Data Protection Board

The Chair

(Anu Talus)