Reports of Cases

OPINION OF ADVOCATE GENERAL
RANTOS
delivered on 20 September 2022 [1]

Case C-252/21

Meta Platforms Inc., formerly Facebook Inc.,
Meta Platforms Ireland Limited, formerly Facebook Ireland Ltd.,
Facebook Deutschland GmbH
v
Bundeskartellamt,
intervener:
Verbraucherzentrale Bundesverband e.V.

(Request for a preliminary ruling
from the Oberlandesgericht Düsseldorf (Higher Regional Court, Düsseldorf, Germany))

(Reference for a preliminary ruling – Regulation (EU) 2016/679 – Protection of natural persons with regard to the processing of personal data – Social networks – Article 4(11) – Notion of 'consent' of the data subject – Consent given to a dominant undertaking responsible for processing – Article 6(1)(b) to (f) – Lawfulness of processing – Processing necessary for the performance of a contract to which the data subject is party or for the purposes of the legitimate interests pursued by the controller or by a third party – Processing necessary for compliance with a legal obligation to which the controller is subject, the protection of the vital interests of the data subject or of another natural person or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller – Article 9(1) and (2)(e) – Special categories of personal data – Personal data which are manifestly made public by the data subject – Articles 51 to 66 – Powers of the national competition authority – Reconciliation with the powers of data protection supervisory authorities – Adoption of measures under competition law by an authority located in a Member State other than that of the lead authority for the supervision of data protection)

Introduction

1. This request for a preliminary ruling was made by the Oberlandesgericht Düsseldorf (Higher Regional Court, Düsseldorf, Germany) in proceedings between companies in the Meta Platforms group [2] and the Bundeskartellamt (Federal Cartel Office, Germany) concerning the decision by

[1] Original language: French.

[2] Namely Meta Platforms Inc. (formerly Facebook Inc.), Meta Platforms Ireland Limited (formerly Facebook Ireland Ltd.) and Facebook Deutschland GmbH ('Meta Platforms' or 'the applicant in the main proceedings').

which the Federal Cartel Office prohibited the applicant in the main proceedings from processing data as provided for in the terms of service of its Facebook social network and from implementing those terms of service, and imposed measures to stop it from doing so. [3]

2. The questions referred for a preliminary ruling essentially concern, on the one hand, the competence of a national competition authority such as the Federal Cartel Office to examine, as a principal issue or as an incidental question, the conduct of an undertaking in the light of certain provisions of Regulation (EU) 2016/679 [4] and, on the other hand, the interpretation of those provisions with regard to the processing of sensitive personal data, the relevant conditions for the lawfulness of personal data processing and the consent given freely to an undertaking in a dominant position.

Legal framework

European Union law

3. Article 4 of the GDPR provides:

'For the purposes of this Regulation:

…

(11) "consent" of the data subject means 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;

…'

4. Article 6(1) of the regulation, entitled 'Lawfulness of processing', reads as follows:

'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;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

[3] Decision B6-22/16 of 6 February 2019 ('the decision at issue').

[4] Regulation 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 (General Data Protection Regulation) (OJ 2016 L 119, p. 1, and corrigendum, OJ 2018 L 127, p. 2) ('GDPR').

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.'

5. Article 9(1) and (2) of the regulation, entitled 'Processing of special categories of personal data', provides:

'1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

…

(e) processing relates to personal data which are manifestly made public by the data subject;

…'

6. Article 51 of the regulation, entitled 'Supervisory authority', which forms part of Chapter VI, entitled 'Independent supervisory authorities', states:

'1. Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, 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 …

2. Each supervisory authority shall contribute to the consistent application of this Regulation throughout the Union. For that purpose, the supervisory authorities shall cooperate with each other and the Commission in accordance with Chapter VII.

…'

German law

7. Paragraph 19(1) of the Gesetz gegen Wettbewerbsbeschränkungen (Law against restrictions on competition; 'the GWB') provides:

'The abusive exploitation of a dominant position on the market by one or more undertakings is prohibited.' [5]

8. Paragraph 50f of the GWB provides:

'(1) The competition authorities, the regulatory authorities, the federal data protection and freedom of information officer, the regional data protection officers and the competent authorities within the meaning of Article 2 of the EU-Verbraucherschutzdurchführungsgesetz [Law on the implementation of EU consumer protection law] may, irrespective of the procedure chosen, exchange information, including personal data and trade and business secrets, to the extent necessary for the performance of their respective tasks and may use that information in the course of their proceedings. …'

The dispute in the main proceedings, the questions referred for a preliminary ruling and the procedure before the Court

9. Meta Platforms operates the online social network 'Facebook' in the European Union (www.facebook.com), as well as other online services, including Instagram and WhatsApp. The business model of the social networks operated by Meta Platforms essentially consists of offering social network services free of charge for private users and selling online advertising. The advertising is tailored to individual users and aims to show them products and services that might interest them on the basis of, inter alia, their consumer behaviour, interests, purchasing power and personal situation. The technical basis for this type of advertising is the automated production of detailed profiles of users of Facebook and the online services offered at group level. [6]

10. In order to collect and process user data, Meta Platforms relies on the contract for the use of the services entered into with its users when they click on the 'Sign up' button, thereby accepting Facebook's terms of service. Acceptance of those terms of service is an essential requirement for using the Facebook social network. [7] The central element of this case is the practice of *collecting* data from other group services, as well as from third-party websites and apps via integrated interfaces or via cookies placed on the user's computer or mobile device, *linking* those data with the user's Facebook account and then *using* them ('the practice at issue').

11. The Federal Cartel Office initiated proceedings against Meta Platforms as a result of which, by the decision at issue, it prohibited Meta Platforms from processing data as provided for in Facebook's terms of service and from implementing those terms, and imposed measures to stop

5 In the version in force until 18 January 2021.

6 To that end, in addition to data that users provide directly when signing up for the relevant online services, Meta Platforms collects other user- and device-related data on and off the social network and the online services provided by the group, and links the data to the various accounts of the users concerned. It is possible to draw detailed conclusions about users' preferences and interests from the aggregated data.

7 With regard to the processing of personal data in particular, the terms of service refer to the policies of Meta Platforms on the use of data and cookies. According to those policies, Meta Platforms collects user- and device-related data about user activities on and off the social network and links the data with users' Facebook accounts. User activities off the social network consist of visits to third-party websites and apps connected to Facebook by programming interfaces ('Facebook Business Tools') and the use of other online services belonging to the Meta Platforms group, including Instagram and WhatsApp.

it from doing so. The Federal Cartel Office based its decision, inter alia, on the fact that under Paragraph 19 of the GWB, the processing in question constituted an abuse of the company's dominant position in the social media market for private users in Germany. [8]

12. On 11 February 2019, Meta Platforms brought an action against the decision at issue before the Oberlandesgericht Düsseldorf (Higher Regional Court, Düsseldorf), [9] which is the referring court. In essence, the referring court has doubts as to the ability of national competition authorities to monitor the compliance of data processing with the requirements laid down in the GDPR and to determine and penalise breaches of the GDPR. It also has doubts as to the interpretation and application of certain provisions of that regulation.

13. In those circumstances, the Oberlandesgericht Düsseldorf (Higher Regional Court, Düsseldorf) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:

'(1) (a) Is it compatible with Article 51 et seq. of the GDPR if a national competition authority – such as the Federal Cartel Office – which is not a supervisory authority within the meaning of Article 51 et seq. of the GDPR, of a Member State in which an undertaking established outside the European Union has an establishment that provides the main establishment of that undertaking – which is located in another Member State and has sole responsibility for processing personal data for the entire territory of the European Union – with advertising, communication and public relations support, finds, for the purposes of monitoring abuses of competition law, that the main establishment's contractual terms relating to data processing and their implementation breach the GDPR and issues an order to end that breach?

(b) If so: is that compatible with Article 4(3) TEU if, at the same time, the lead supervisory authority in the Member State in which the main establishment, within the meaning of Article 56(1) of the GDPR, is located is investigating the undertaking's contractual terms relating to data processing?

If the answer to Question 1 is yes:

(2) (a) If an internet user merely visits websites or apps to which the criteria of Article 9(1) of the GDPR relate, such as flirting apps, gay dating sites, political party websites or health-related websites, or also enters information into them, for example when registering or when placing orders, and another undertaking, such as Facebook Ireland, uses interfaces integrated into those websites and apps, such as 'Facebook Business Tools', or cookies or similar storage technologies placed on the internet user's computer or mobile device, to collect data about those visits to the websites and apps and the information entered by the user, and links those data with the data from the user's [Facebook] account and uses them, does this collection and/or linking and/or use involve the processing of sensitive [personal] data for the purpose of that provision?

8 According to the Federal Cartel Office, that processing, which stems from market power, infringes the provisions of the GDPR and is not justified under Articles 6(1) and 9(2) of that regulation.

9 In addition, on 31 July 2019, Meta Platforms introduced new terms of service on the initiative of the European Commission and the national consumer protection organisations of the Member States. Those terms expressly state that the user agrees to be shown advertisements instead of paying to use Facebook products. Furthermore, since 28 January 2020, Meta Platforms has been offering, at a global level, 'Off-Facebook-Activity', which allows Facebook users to view a summary of the information about them, obtained in relation to their activities on other websites and apps, and to disconnect the data about past and future activities from their Facebook account if they so wish.

(b) If so: does visiting those websites or apps and/or entering information and/or clicking or tapping on the buttons integrated into them by a provider such as Facebook Ireland (social plugins such as 'Like', 'Share' or 'Facebook Login' or 'Account Kit') constitute manifestly making the data about the visits themselves and/or the information entered by the user public within the meaning of Article 9(2)(e) of the GDPR?

(3) Can an undertaking, such as Facebook Ireland, which operates a digital social network funded by advertising and offers personalised content and advertising, network security, product improvement and continuous, seamless use of all of its group products in its terms of service, justify collecting data for these purposes from other group services and third-party websites and apps via integrated interfaces such as Facebook Business Tools, or via cookies or similar storage technologies placed on the internet user's computer or mobile device, linking those data with the user's [Facebook] account and using them, on the ground of necessity for the performance of the contract under Article 6(1)(b) of the GDPR or on the ground of the pursuit of legitimate interests under Article 6(1)(f) of the GDPR?

(4) In those circumstances, can

– the fact of users being underage, vis-à-vis the personalisation of content and advertising, product improvement, network security and non-marketing communications with the user;

– the provision of measurements, analytics and other business services to enable advertisers, developers and other partners to evaluate and improve their services;

– the provision of marketing communications to the user to enable the undertaking to improve its products and engage in direct marketing;

– research and innovation [in the public interest], to further the state of the art or the academic understanding of important social issues and to affect society and the world in a positive way;

– the sharing of information with law enforcement agencies and responding to legal requests in order to prevent, detect and prosecute criminal offences, unlawful use, breaches of the terms of service and policies and other harmful behaviour;

also constitute legitimate interests within the meaning of Article 6(1)(f) of the GDPR if, for those purposes, the undertaking links data from other group services and from third-party websites and apps with the user's [Facebook] account via integrated interfaces such as Facebook Business Tools or via cookies or similar storage technologies placed on the internet user's computer or mobile device and uses those data?

(5) In those circumstances, can collecting data from other group services and from third-party websites and apps via integrated interfaces such as Facebook Business Tools, or via cookies or similar storage technologies placed on the internet user's computer or mobile device, linking those data with the user's [Facebook] account and using them, or using data already collected and linked by other lawful means, also be justified under Article 6(1)(c), (d) and (e) of the GDPR in individual cases, for example to respond to a legitimate request for certain data (point (c)), to combat harmful behaviour and promote security (point (d)), to [conduct] research [in the public interest] and to promote safety, integrity and security (point (e))?

(6) Can consent within the meaning of Article 6(1)(a) and Article 9(2)(a) of the GDPR be given effectively and, in accordance with Article 4(11) of the GDPR in particular, freely, to a dominant undertaking such as Facebook Ireland?

If the answer to Question 1 is no:

(7) (a) Can the national competition authority of a Member State, such as the Federal Cartel Office, which is not a supervisory authority within the meaning of Article 51 et seq. of the GDPR and which examines a breach by a dominant undertaking of the competition-law prohibition on abuse that is not a breach of the GDPR by that undertaking's data processing terms and their implementation, determine, when assessing the balance of interests, whether those data processing terms and their implementation comply with the GDPR?

(b) If so: in the light of Article 4(3) TEU, does that also apply if the competent lead supervisory authority in accordance with Article 56(1) of the GDPR is investigating the undertaking's data processing terms at the same time?

If the answer to Question 7 is yes, Questions 3 to 5 must be answered in relation to data from the use of the group's Instagram service.'

14. Written observations were received from Meta Platforms, the German, Czech, Italian and Austrian Governments, the Federal Cartel Office, the Verbraucherzentrale Bundesverband e V. (consumers' association, Germany) and the European Commission. Those parties also presented oral observations at the hearing held on 10 May 2022.

Analysis

15. The questions referred for a preliminary ruling that are the subject of this case, relating to the interpretation of several provisions of the GDPR, mainly concern: (i) the competence of a competition authority to determine and penalise a breach of the rules on the processing of personal data and its obligations to cooperate with the lead authority within the meaning of the GDPR (first and seventh questions); (ii) the prohibition on processing sensitive personal data and the conditions applicable to consenting to their use (second question); (iii) the lawfulness of the processing of personal data in the light of certain justification (third to fifth questions); (iv) the validity of consent to the processing of personal data given to an undertaking in a dominant position (sixth question).

16. In the points that follow, I will deal with the first and seventh questions first, before examining the other questions in the order in which they were raised, grouping together the third to fifth questions.

The first question

17. By its first question referred for a preliminary ruling, the referring court is asking, in essence, whether a competition authority, when prosecuting a breach of the competition rules, may rule primarily [10] on the infringement of GDPR data processing rules by an undertaking whose main establishment with sole responsibility for processing personal data for the entire territory of the European Union is in another Member State, and, furthermore, issue an order to end that breach (Question 1(a)), and if so, whether the competent lead supervisory authority under Article 56(1) of the GDPR may still investigate that undertaking's contractual terms relating to data processing (Question 1(b)).

18. Subject to verification by the referring court, it seems to me that the Federal Cartel Office, in the decision at issue, did not penalise a breach of the GDPR by Meta Platforms, but proceeded, for the sole purpose of applying competition rules, to review an alleged abuse of its dominant position while taking account, inter alia, of that undertaking's non-compliance with the provisions of the GDPR.

19. Accordingly, in my opinion, Question 1(a), in so far as it concerns a competition authority's ability to decide, as the main issue, on a breach of the GDPR and to issue an order to end that breach within the meaning of that regulation, is irrelevant. [11]

20. It follows that Question 1(b), which is contingent on an affirmative answer to Question 1(a), is also irrelevant. [12]

The seventh question

21. By its seventh question referred for a preliminary ruling, the referring court is asking, in essence, whether a competition authority is entitled, when prosecuting infringements of the competition rules, to establish, [13] as an incidental question, whether the data processing terms and their implementation comply with the GDPR (Question 7(a)) and, if so, whether the competition authority's analysis is also possible where those terms are, at the same time, under investigation by the competent lead supervisory authority (Question 7(b)).

22. First, with regard to Question 7(a), it seems to me that although a competition authority is not competent to establish a breach of the GDPR, [14] that regulation does not, in principle, preclude authorities other than the supervisory authorities, when exercising their own powers, from being able to take account, as an incidental question, of the compatibility of conduct with the provisions

10 It seems to me that the expression 'finds … that the main establishment's contractual terms relating to data processing and their implementation breach the GDPR and issues an order to end that breach' in the first question referred for a preliminary ruling must be interpreted in that sense.

11 At any rate, given that the GDPR provides for the full harmonisation of data protection laws, the central element of which is a harmonised enforcement mechanism based on the 'one-stop shop' principle set out in Articles 51 to 67 of that regulation, it seems obvious to me that an authority other than a supervisory authority within the meaning of that regulation (such as a competition authority) does not have the competence to make a ruling, primarily, on a breach of that regulation or to impose the penalties envisaged.

12 In any event, given that a competition authority is not competent to establish, primarily, a breach of that regulation or to impose the penalties envisaged, any such decision by a competition authority would not impinge on the powers of the supervisory authorities within the meaning of the GDPR.

13 It seems to me that that is how the terms 'determine, when assessing the balance of interests, whether those data processing terms and their implementation comply with the GDPR' in the seventh question should be interpreted.

14 See footnote 11 to this Opinion.

of the GDPR. This is especially true, in my opinion, where a competition authority exercises the powers conferred on it by Article 102 TFEU and by the first paragraph of Article 5 of Regulation (EC) No 1/2003, [15] or by any other equivalent national provision. [16]

23. In exercising its powers, a competition authority must assess, inter alia, whether the conduct in question entails resorting to methods other than those prevailing under merit-based competition, taking into account the legal and economic context in which that conduct takes place. [17] In that respect, the compliance or non-compliance of that conduct with the provisions of the GDPR, not taken in isolation but considering all the circumstances of the case, may be a vital clue as to whether that conduct entails resorting to methods prevailing under merit-based competition, it being stated that the lawful or unlawful nature of conduct under Article 102 TFEU is not apparent from its compliance or lack of compliance with the GDPR or other legal rules. [18]

24. Therefore, I consider that the examination of an abuse of a dominant position on the market may justify the interpretation, by a competition authority, of rules other than those relating to competition law, such as those of the GDPR, [19] while specifying that such an examination is carried out in an incidental manner [20] and is without prejudice to the application of that regulation by the competent supervisory authorities. [21]

15 Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in [Articles 101 and 102 TFEU] (OJ 2003 L 1, p. 1).

16 Such as Paragraph 19 of the GWB, on which the decision at issue is based.

17 See, by way of example, judgment of 6 September 2017, *Intel* v *Commission* (C-413/14 P, EU:C:2017:632, paragraph 136 and the case-law cited). Moreover, the Court has clarified that the scope of Article 102 TFEU is of general application and cannot be restricted by the existence of a regulatory framework adopted by the EU legislature – in this case, the regulatory framework for electronic communications (see, to that effect, judgment of 10 July 2014, *Telefónica and Telefónica de España* v *Commission*, C-295/12 P, EU:C:2014:2062, paragraph 128).

18 In the light of the different objectives of the two categories of provisions, it is clear that conduct relating to data processing may breach competition rules even if it complies with the GDPR; conversely, unlawful conduct under the GDPR does not automatically mean that it breaches competition rules. In that regard, the Court of Justice has clarified that the compliance of conduct with specific legislation does not preclude the applicability, to that conduct, of Articles 101 and 102 TFEU (see, in particular, judgment of 6 December 2012, *AstraZeneca* v *Commission* (C-457/10 P, EU:C:2012:770, paragraph 132), in which the Court of Justice also recalled that in the majority of cases, abuses of dominant positions consist of behaviour which is otherwise lawful under branches of law other than competition law). Indeed, if only practices which objectively restrict competition and are at the same time unlawful were regarded as abusive within the meaning of Article 102 TFEU, that would mean that conduct which is potentially harmful to competition could not, merely because it is lawful, be penalised under Article 102 TFEU, which would compromise the objective of that provision, namely to establish a system which ensures that competition in the internal market is not distorted (see, to that effect, my Opinion in *Servizio Elettrico Nazionale and Others*, C-377/20, EU:C:2021:998, point 37). According to the case-law of the Court of Justice, it is only if anticompetitive conduct is required of undertakings by national legislation, or if the latter creates a legal framework which itself eliminates any possibility of competitive activity on their part, that Articles 101 and 102 TFEU do not apply, whereas those articles may apply if it is found that the national legislation leaves open the possibility of competition which may be prevented, restricted or distorted by the autonomous conduct of undertakings (see, to that effect, judgment of 14 October 2010, *Deutsche Telekom* v *Commission*, C-280/08 P, EU:C:2010:603, paragraph 80 and the case-law cited).

19 An interpretation whereby competition authorities would be prohibited from interpreting the provisions of the GDPR when exercising their powers could call into question the effective application of EU competition law.

20 Moreover, the incidental nature of the competition authority's interpretation of the GDPR does not prevent that interpretation from being subject to judicial review before the national courts competent in competition matters. In the event of difficulties in interpretation, those courts could be required to submit a request for a preliminary ruling to the Court of Justice, as in the present case with regard to the second to sixth questions referred.

21 The competition authority's *interpretation* of the GDPR solely for the purpose of applying the rules (and possibly imposing penalties) provided for by competition law cannot deprive the supervisory authorities of their competences and powers under that regulation. Furthermore, the possibility of an incidental interpretation of that regulation by the competition authority raises no additional difficulties with regard to its *application*, which is reserved for the supervisory authorities, or the *imposition of corrective measures or penalties*, since any measures or penalties that may be imposed by a competition authority are based on different rules, objectives and legitimate interests than those protected by that regulation (for that reason, in such a situation, the penalties imposed by the competition authority and supervisory authority under the GDPR are not, in my view, covered by the principle *ne bis in idem* (see, by analogy, judgment of 22 March 2022, *bpost*, C-117/20, EU:C:2022:202, paragraphs 42 to 50)).

25. Second, with regard to Question 7(b), the referring court is asking what obligations, in the context of the application of the principle of sincere cooperation enshrined in Article 4(3) TEU, a competition authority has, when interpreting the provisions of the GDPR, in respect of the competent lead supervisory authority within the meaning of that regulation, particularly when the conduct under investigation by the competition authority is also being investigated by the competent lead supervisory authority.

26. In the present case, the investigation, albeit incidental, by a competition authority of an undertaking's conduct in the light of the GDPR carries the risk of differing interpretations of that regulation by the competition authority and the supervisory authorities, which could in principle undermine the uniform interpretation of the GDPR. [22]

27. EU law does not provide detailed rules on cooperation between a competition authority and supervisory authorities within the meaning of the GDPR in such a situation. More specifically, neither the mechanism for cooperation among competent authorities within the meaning of the GDPR when applying that regulation, [23] nor other specific rules on cooperation among administrative authorities, such as those on cooperation among competition authorities, and between competition authorities and the Commission when applying competition rules, [24] are applicable in the present case.

28. Nevertheless, a competition authority, when interpreting the GDPR, is bound by the duty to cooperate in good faith enshrined in Article 4(3) TEU, according to which the European Union and the Member States, including their administrative authorities, [25] must, in full mutual respect, assist each other in carrying out tasks which flow from the Treaties. In particular, the third paragraph of that article provides that the Member States must facilitate the achievement of the European Union's tasks and refrain from any measure which could jeopardise the attainment of the European Union's objectives. [26] In addition, like any administrative authority responsible for enforcing EU law, a competition authority is bound by the principle of sound administration as a general principle of EU law, which includes, inter alia, an extensive duty of diligence and care on the part of national authorities. [27]

29. Thus, in the absence of clear rules on cooperation mechanisms, which it may fall to the EU legislature to adopt, a competition authority, when interpreting the provisions of the GDPR, is subject, at the very least, to a duty to inform and cooperate with the competent authorities

22 In addition, the risk of differing interpretation is inherent in any area governed by rules that the competition authority must or may take into account in order to assess the legality of conduct under competition law.

23 Chapters VI and VII of the GDPR establish 'one-stop-shop' mechanisms for the exchange of information and for mutual assistance between supervisory authorities.

24 See Regulation No 1/2003 and Directive (EU) 2019/1 of the European Parliament and of the Council of 11 December 2018 to empower the competition authorities of the Member States to be more effective enforcers and to ensure the proper functioning of the internal market (OJ 2019 L 11, p. 3).

25 See in particular, to that effect, judgments of 14 November 1989, *Italy* v *Commission* (14/88, EU:C:1989:421, paragraph 20) and of 11 June 1991, *Athanasopoulos and Others* (C-251/89, EU:C:1991:242, paragraph 57).

26 Moreover, the cooperation mechanism established by the GDPR for supervisory authorities may itself be regarded as a *lex specialis* supplementing and clarifying the general principle of sincere cooperation set out in Article 4(3) TEU (see, in particular, Hijmans, H., 'Article 51 Supervisory authority', *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford, 2020, p. 869). The same applies to other cooperation instruments that pre-date the one provided for in the GDPR, such as the system of cooperation among competition authorities (see in particular Chapter IV of Regulation No 1/2003).

27 See, to that effect, the Opinion of Advocate General Trstenjak in *Gorostiaga Atxalandabaso* v *Parliament* (C-308/07 P, EU:C:2008:498, point 89).

within the meaning of that regulation, in accordance with the national provisions that govern its powers (principle of procedural autonomy of the Member States) and in compliance with the principles of equivalence and effectiveness. [28]

30. It follows, in my view, that where the competent lead supervisory authority has ruled on the application of certain provisions of the GDPR in respect of the same practice or similar practices, the competition authority cannot, in principle, deviate from the interpretation of that authority, which is the sole competent authority for the application of that regulation, [29] and must, as far as possible and with due regard, in particular, for the rights of the defence of the data subjects, comply with any decisions adopted by that authority concerning the same conduct, [30] and, in the event of doubts in the case at hand as to the interpretation given by the competent authority, consult it or, where that authority is in another Member State, the national supervisory authority. [31]

31. Even without a decision by the competent supervisory authority, it is still the competition authority's duty to inform [32] and cooperate with the competent supervisory authority where that authority has begun an investigation of the same practice or has indicated its intention to do so, and possibly to await the outcome of that authority's investigation before commencing its own assessment, in so far as that is appropriate and is without prejudice to the competition authority abiding by a reasonable investigation period and the rights of defence of the data subjects. [33]

32. In the present case, it seems to me that the fact that the Federal Cartel Office entered into cooperation with the supervisory authorities responsible at national level [34] and that the lead supervisory authority in Ireland has also been contacted informally – circumstances alluded to by the Federal Cartel Office and which it is for the referring court to verify – may be sufficient evidence that the authority has fulfilled its duties of diligence and sincere cooperation. [35]

33. In conclusion, I propose that the answer to the seventh question referred for a preliminary ruling should be that Articles 51 to 66 of the GDPR must be interpreted as meaning that a competition authority, within the framework of its powers under the competition rules, may examine, as an incidental question, the compliance of the practices under investigation with the

28 See, in particular, judgment of 2 June 2022, *Skeyes* (C-353/20, EU:C:2022:423, paragraph 52 and the case-law cited). In my opinion, guidance on the correct approach may, where appropriate, be derived from the cooperation system established by the GDPR, and from that established in the field of competition. However, in the absence of ad hoc provisions, the competition authority's duty of care does not extend as far as to subject it to detailed obligations such as those laid down in the cooperation procedure and consistency mechanism governed by Chapter VII of the GDPR (for example, the competition authority cannot be expected to send a draft decision to the competent supervisory authority within the meaning of that regulation in order to obtain its opinion).

29 See, in particular and by analogy, in relation to an area covered by EU rules on pharmaceutical matters, judgment of 23 January 2018, *F. Hoffmann-La Roche and Others* (C-179/16, EU:C:2018:25, paragraphs 58 to 64).

30 In other words, that decision forms part of the legal and factual framework which the competition authority is required to examine, while remaining free to draw its own conclusions from the point of view of the application of competition law (see footnote 18 to this Opinion).

31 Given the role and functions of national supervisory authorities in the system of cooperation established by the GDPR, I consider that interaction with the national supervisory authority alone may be sufficient to fulfil the competition authority's duties of diligence and sincere cooperation, particularly where the competition authority lacks the ability (given the applicable national law procedures) or the resources (linguistic or otherwise) to interact satisfactorily with the lead supervisory authority of another Member State.

32 Or where that authority is in another Member State the national supervisory authority (see footnote 31 to this Opinion).

33 Bearing in mind that a competition authority's interpretation of certain provisions of the GDPR when exercising its powers is without prejudice to the interpretation and application of those provisions by the competent supervisory authorities within the meaning of that regulation (see footnote 21 to this Opinion).

34 The Federal Cartel Office submits in that respect that it relied on German competition law, which allows it to interact with national supervisory authorities within the meaning of the GDPR.

35 This is particularly the case if, as the Federal Cartel Office contends, the German federal supervisory authority and the Irish lead supervisory authority have confirmed to it that the latter has not initiated any proceedings in respect of the same practices investigated by the Federal Cartel Office.

GDPR rules, while taking account of any decision or investigation of the competent supervisory authority on the basis of the GDPR, informing and, where appropriate, consulting the national supervisory authority.

The second question

34. By its second question referred for a preliminary ruling, the referring court is asking, in essence, whether Article 9(1) of the GDPR must be interpreted as meaning that the practice at issue, when it concerns visits to third-party websites and apps,[36] involves processing the types of sensitive personal data mentioned,[37] which is prohibited[38] (Question 2(a)), and if so, whether Article 9(2)(e) of that regulation must be interpreted as meaning that a user manifestly makes public within the meaning of that provision the data revealed by visiting those websites and apps, or entered into those websites or apps, or resulting from clicking on buttons integrated into those websites or apps[39] (Question 2(b)).

35. First, with regard to Question 2(a), I would point out that the processing of sensitive personal data is prohibited under Article 9(1) of the GDPR. The specific protection of such data is justified – as is apparent from recital 51 of that regulation – by the fact that they are, by their nature, particularly sensitive in relation to fundamental rights and freedoms and their processing could create significant risks to those fundamental rights and freedoms. Furthermore, despite the somewhat obscure wording of that provision,[40] it does not seem to me that, as the referring court assumes, it introduces a substantial difference between personal data that are sensitive because they 'reveal' a certain situation and data that are inherently sensitive.[41]

36 The referring court mentions visits by a user to websites or apps and enters data into those websites or apps (such as flirting apps, gay dating sites, political party websites or health-related websites), which reveal data protected by the provision in question.

37 Referred to hereinafter as 'sensitive personal data'. This involves processing personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

38 Incidentally, I note that the Federal Cartel Office has doubts as to the relevance of that question to the resolution of the dispute, since, in its decision, the Federal Cartel Office considered consent within the meaning of Article 6(1)(a) of the GDPR, and not consent under Article 9(2)(a) of the GDPR.

39 The referring court mentions social plugins such as 'Like' or 'Share' buttons, the 'Facebook Login' (in other words, the possibility of being identified using the login linked to the Facebook account) and the 'account kit' (in other words, the possibility of being identified on an app or a website, not necessarily linked to Facebook, by a telephone number or an email address, without the need for a password).

40 I also note a major inconsistency between the French version of the GDPR, which in the first sentence of that provision refers to the *processing* of personal data that *reveals* certain sensitive situations, and the German version (as well as the Greek and Italian versions), which refers to the processing of *personal data* that *reveal* those situations. Unless I am mistaken, the French version of that provision contradicts most of the other language versions. Moreover, in the context of that provision, it seems to me more logical to link the verb 'reveal' to the data, since in the rest of the provision it is the data that are the subject of the analysis and not the processing. This is also apparent from the French wording of recital 51 of the GDPR, which states that sensitive personal data 'should include *personal data* [*that reveal*] racial or ethnic origin' (emphasis added).

41 In my view, it is inconsistent with the spirit of Article 9(1) of the GDPR (and of the regulation as a whole) – namely to protect certain sensitive personal data – to distinguish, for example, between, on the one hand, racial or ethnic origin, which would include the prohibition on processing not only data that indicate that directly, but also data that reveal that situation, and on the other hand, genetic data, where the prohibition on processing would not extend to data revealing that situation, while adding that it would not always be easy to distinguish between data *revealing* certain situations (for example, racial or ethnic origin) and data *concerning* other situations (for example, health). In that respect, I note that while Article 9(1) of the GDPR refers to data *concerning* health, Article 4(15) of the GDPR defines 'data concerning health' as 'personal data *related* to the physical or mental health of a natural person, including the provision of health care services, *which reveal* information about his or her health status' (emphasis added). As the German Government suggests, it is possible that that inconsistency in the wording of the provision in question is merely a vain attempt to distinguish between pure data with a direct informational content and 'metadata' for which the corresponding informational content is only apparent in specific circumstances, for example when analysed or linked.

36. In the present case, it is clear, in my view, that the practice at issue entails the processing of personal data which is, in principle, liable to fall within the scope of that provision and to be prohibited where the data processed 'reveal' one of the sensitive situations referred to therein. It is necessary therefore to establish whether and to what extent visiting websites and apps or entering data into them may be 'indicative' of one of the sensitive situations listed in the provision in question.

37. In that respect, I doubt whether it is relevant (or always possible) to distinguish between the data subject merely being interested in certain information and the data subject belonging to one of the categories covered by the provision in question.[42] Although the parties to the main proceedings have opposing views in that regard,[43] I believe the answer to that question must be sought on a case-by-case basis and with regard to each of the activities comprising the practice at issue.

38. Although, as the German Government points out, simply collecting sensitive personal data about the visit to a website or an app is not, in itself, necessarily the same as processing sensitive personal data within the meaning of that provision,[44] linking the data to the relevant user's Facebook account or using the data could, on the other hand, both easily amount to such processing. The decisive factor for the purpose of applying Article 9(1) of the GDPR is, in my view, whether the data processed allow user profiling based on the categories that emerge from the types of sensitive personal data mentioned in that article.[45]

39. In that context, to be able to determine whether data processing falls within the scope of that provision, it might be worth distinguishing, where appropriate, between the processing of data which prima facie may be categorised as sensitive personal data, which alone allow profiling of the data subject, and the processing of data that are not inherently sensitive but require subsequent aggregation in order to draw plausible conclusions for profiling purposes.

42 In principle, as the applicant in the main proceedings contends, those are two different aspects. Indeed, the mere fact that a user has accessed or interacted with a website does not necessarily reveal information about his or her beliefs, health, political opinions and so forth, because having an interest in a website does not automatically entail endorsing the views expressed on that website or belonging to the categories it represents. That is especially the case with visits to the website of a political party or a website that espouses a particular political ideology: it does not necessarily mean that the user shares that ideology; he or she might simply be curious or even critical of that ideology.

43 According to Meta Platforms, the fact that a user has accessed or interacted with a website does not in itself reveal sensitive information, because even if an interest in a website were observed or used, it would not constitute processing of sensitive personal data. That would only be the case if users were *categorised* on the basis of those data. Consequently, the data concerned by the practice at issue would only be protected under Article 9(1) of the GDPR if they were in one of the categories covered by that article and were processed subjectively, in full knowledge of the facts and with the intention of deriving such information from them. Conversely, according to the interpretation of the Federal Cartel Office – which is too rigid in my view – the mere fact that the data subject visits a particular website or uses a specific app whose main focus is one of the categories listed in Article 9(1) of the GDPR already triggers the protection afforded by that provision. The protection of sensitive personal data does not depend on the controller's *intention* to use such data, because the rights of the data subject are already affected by the fact that those data are removed from his or her sphere of influence.

44 As the European Data Protection Board (EDPB) acknowledges, the mere fact that a social media provider processes large amounts of data which potentially could be used to infer special categories of data does not automatically mean that the processing falls under Article 9 of the GDPR (see EDPB Guidelines 8/2020 of 13 April 2021 on the targeting of social media users ('the EDPB Guidelines 8/2020'), paragraph 124).

45 Such an interpretation would, in my view, prevent a situation – criticised by the applicant in the main proceedings – in which the controller is essentially in breach of the GDPR by default since it could not avoid potentially receiving (including by automated means) information indirectly linked to categories of sensitive data, without prejudice to the controller's obligation to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk in accordance with Article 32 of the GDPR.

40. However, it should be clarified that the existence of categorisation within the meaning of that provision is independent of whether that categorisation is accurate or correct.[46] What counts is the possibility that such categorisation could create a significant risk to the fundamental rights and freedoms of the data subject, as stated in recital 51 of the GDPR, regardless of whether or not that possibility materialises.

41. Lastly, as to the referring court's question whether the purpose for which the data are used is relevant to the assessment in question,[47] I find – contrary to the argument put forward by the applicant in the main proceedings – that in principle, the controller is not required to process those data knowing and intending to derive particular categories of information directly from them. The aim of the provision in question is, in essence, objectively to prevent significant risks to the fundamental rights and freedoms of data subjects arising from the processing of sensitive personal data, irrespective of any subjective element such as the controller's intention.

42. Second, as regards Question 2(b), it should be recalled that, pursuant to Article 9(2)(e) of the GDPR, the prohibition on processing sensitive personal data does not apply if the processing relates to personal data which are *manifestly made public* by the data subject. Moreover, the inclusion in the wording of that provision of the adverb 'manifestly' and the fact that the provision constitutes an exemption to the prohibition on processing sensitive personal data[48] require a particularly stringent application of that exemption, on account of the significant risks to the fundamental rights and freedoms of data subjects.[49] In order for that exemption to apply, the user must, in my opinion, be *fully aware* that, by an *explicit act*,[50] he or she is making personal data public.[51]

43. In the present case, it seems to me that conduct consisting in visiting websites and apps, entering data into those websites and apps and clicking on buttons integrated into them cannot, in principle, be regarded in the same way as conduct that manifestly makes public the user's sensitive personal data within the meaning of Article 9(2)(e) of the GDPR.

44. In principle, the browsing data from *visits to websites and apps* is only visible to the administrator of the website or app in question and to the third parties to whom the administrator transmits such information, such as the applicant in the main proceedings.[52] Similarly, although by *entering data into websites and apps*, the data subject could disclose, directly and voluntarily, information about certain sensitive personal data, that information is

46 See, to that effect, EDPB Guidelines 8/2020, paragraph 125.

47 The referring court mentions, in that respect, the personalisation of the social network and advertising, network security, service improvements, provision of measurement and analytics services for advertisers, research for public interest purposes, responses to legal requests, compliance with legal obligations, protection of the vital interests of users and third parties, and tasks carried out in the public interest.

48 See, by analogy, judgment of 21 December 2016, *Tele2 Sverige and Watson and Others* (C-203/15 and C-698/15, EU:C:2016:970, paragraph 89 and the case-law cited), on the interpretation of Article 15(1) of 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) (OJ 2002 L 201, p. 37), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (OJ 2009 L 337, p. 11).

49 See also pages 10 and 11 of Opinion 6/2014 of the Article 29 Data Protection Working Party, an independent advisory body set up under Article 29 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31), replaced, since the adoption of the GDPR, by the EDPB.

50 In my view, that condition is very similar to that of the data subject's consent.

51 Under Article 5(2) of the GDPR, the burden of proof is on the controller to demonstrate that personal data are processed in accordance with the GDPR.

52 Although an observant user is probably aware that the login information is visible to the administrator of the website or app in question, it is not a given, in my view, that he or she is also aware that that information is also visible to the administrator of his or her Facebook account.

only visible to the administrator of the website or app in question and to third parties to whom the administrator transmits that information. I would say therefore that those actions cannot constitute evidence of the user's wish to make the data publicly available.[53] Furthermore, while it is clear that, by *clicking on buttons integrated into websites or apps*,[54] the data subject is clearly expressing a wish to share certain information with the public outside the website or app in question, I am of the opinion that, as the Federal Cartel Office points out, by doing so, the person in question is conscious that he or she is sharing information with a *specific group of people*, often defined by the user himself or herself,[55] and not with the general public.[56]

45. Lastly, with regard to the relevance of any consent given by the user within the meaning of Article 5(3) of Directive 2002/58 so that personal data may be collected by cookies or similar technologies, as described by the referring court, I do not consider such consent, in view of its specific purpose, to be sufficient to justify the processing of sensitive personal data collected by such methods.[57] Indeed, such consent, which is necessary to install the technical means to capture certain user activities,[58] does not involve the processing of sensitive personal data and cannot be regarded as a wish to make such data manifestly public within the meaning of Article 9(2)(e) of the GDPR.[59]

46. In conclusion, I propose that the answer to the second question referred for a preliminary ruling should be that Article 9(1) of the GDPR must be interpreted as meaning that the prohibition on processing sensitive personal data may include the processing of data carried out by an operator of an online social network consisting in the collection of a user's data when he or she visits other websites or apps or enters such data into them, the linking of such data to the user account on the social network and the use of such data, provided that the information processed, considered in isolation or aggregated, make it possible to profile users on the basis of the categories that emerge from the listing in that provision of types of sensitive personal data. In addition, Article 9(2)(e) of the GDPR must be interpreted as meaning that a user does not manifestly make public data revealed by visiting websites and apps or entered into those websites or apps or resulting from clicking on buttons integrated into those websites or apps.

53 At most, the user is aware of his or her 'relationship' with the site or app administrator and the third parties to whom the administrator transmits that information. However, the user might not even be aware of that relationship, because – depending on the circumstances – he or she might be under the impression that he or she is sharing information, potentially anonymously, with a mere device.

54 Those are buttons such as 'Like' and 'Share' (see footnote 39 to this Opinion).

55 For example, Facebook allows users to customise their preferences, with several options for sharing the information available in their Facebook account.

56 Admittedly, it is possible that by doing so, the user actually wants to share his or her information with an indefinite number of people in some cases. For example, it is possible that the user has configured the sharing options of his or her Facebook account so that the content present on his or her profile is visible to all users of the social network, and that he or she is aware of that. However, even in those circumstances, it is not self-evident that the user, in acting thus, unquestionably intended to make the personal data in question *manifestly public*, given the strict nature of the exemption in question (see point 42 of this Opinion).

57 See, to that effect, judgment of 29 July 2019, *Fashion ID* (C-40/17, EU:C:2019:629, paragraphs 87 to 89).

58 Including 'cookies' (see recital 25 of Directive 2002/58).

59 Moreover, that consent cannot be regarded as explicit consent to the processing of personal data within the meaning of Article 9(2)(a) of the GDPR. Consent to profiling within the meaning of Article 22(1)(c) of the GDPR, which is evidently limited to profiling operations, is also irrelevant.

The third to fifth questions

47. By its third to fifth questions referred for a preliminary ruling, the referring court is asking, in essence, whether Article 6(1)(b), (c), (d), (e) and (f) of the GDPR must be interpreted as meaning that the practice at issue [60] falls within the scope of one of the grounds provided for in those provisions, and in particular:

– the necessity for the performance of the contract [61] or the taking account of legitimate interests, [62] given that Meta Platforms operates a social network funded by advertising and offering, in its terms of service, personalised content and advertising, network security, product improvement and continuous, seamless use of all group products (third question referred for a preliminary ruling);

– the taking account of those legitimate interests [63] in the context of certain situations [64] (fourth question referred for a preliminary ruling);

– the need to respond to a legitimate request for certain data, [65] to combat harmful behaviour and promote security, [66] or to conduct research in the public interest and to promote safety, integrity and security [67] (fifth question referred for a preliminary ruling).

48. As a preliminary point, notwithstanding several questions as to the admissibility of the fourth and fifth questions, [68] I propose to answer the third to fifth questions together, in so far as the information I will provide below, mainly with regard to the third question, may also be useful to the referring court when applying the provisions that are the subject of the fourth and fifth questions.

49. Principally, I note that, in accordance with Article 8 of the Charter of Fundamental Rights of the European Union ('the Charter'), personal data must be processed fairly for specified purposes and on the basis of a legitimate basis laid down by law. In that respect, Article 6(1) of the GDPR specifies that the processing of such data is lawful only if one of the six conditions set out in that article is met. [69]

50. In the present case, I believe that the third to fifth questions call for a detailed case-by-case analysis of the various clauses of the Facebook terms of service in the context of the practice at issue, since it is impossible to establish whether, in respect of that practice, 'an undertaking, such

60 In relation to the fifth question, the referring court has included in the practice at issue – in addition to collecting the data, linking them to the user's Facebook account and using data from other group services, as well as from third-party websites and apps (see point 10 of this Opinion) – 'using data already collected and linked by other lawful means' to the user's Facebook account.

61 Article 6(1)(b) of the GDPR.

62 Article 6(1)(f) of the GDPR.

63 Article 6(1)(f) of the GDPR.

64 Those include the fact of users being underage, the provision of measurement, analytics and other business services, the provision of marketing communications to users, research and innovation in the public interest, the sharing of information with law enforcement agencies and responses to legal requests.

65 Article 6(1)(c) of the GDPR.

66 Article 6(1)(d) of the GDPR.

67 Article 6(1)(e) of the GDPR.

68 The fourth question appears to ask the Court of Justice to rule on the *application*, rather than on the *interpretation*, of Article 6(1)(f) of the GDPR. The fifth question does not mention the reasons why the referring court has doubts as to the interpretation of Article 6(1)(c), (d) and (e) of that regulation.

69 See EDPB Guidelines 2/2019 of 8 October 2019 on the processing of personal data under Article 6(1)(b) of the GDPR in the context of the provision of online services to data subjects ('EDPB Guidelines 2/2019'), paragraph 1.

as [Meta Platforms]' can comprehensively rely on all (or some) of the grounds set out in Article 6(1) of the GDPR, even though it is possible that said practice, or some of its component activities, may, in certain cases, fall within the scope of that article. [70]

51. Furthermore, the processing envisaged by the provisions cited is carried out, in the present case, on the basis of the general conditions of contract imposed by the controller, in the absence of the consent of the data subject, [71] or even against his or her will, which, in my opinion, calls for a strict interpretation of the grounds in question, particularly in order to avoid any circumvention of the requirement for consent. [72]

52. Lastly, I would point out that, under Article 5(2) of the GDPR, the controller is responsible for demonstrating that the personal data are processed in accordance with the regulation. Moreover, under Article 13(1)(c) of that regulation, it is for the controller to specify the purposes of the processing for which the personal data are intended, as well as the legal basis for the processing.

The third question

53. First, according to Article 6(1)(b) of the GDPR, the processing of personal data is lawful to the extent that it is necessary for the performance of a contract to which the data subject is party. [73]

54. In that regard, I note that the concept of 'necessity' is not defined in EU legislation, but according to the case-law, is still an autonomous concept of EU law. [74] For the processing to be necessary for the performance of the contract, it is not sufficient for it to be carried out at the time of performance of the contract, to be mentioned in the contract, [75] or even merely to be useful for the performance of the contract. [76] According to the case-law of the Court of Justice, the processing must be objectively necessary for the performance of the contract in the sense

70 Although the parties to the main proceedings essentially agree on the premiss that a case-by-case analysis is required for the application of the grounds in question, their positions differ as to the practical implications of that premiss. The Federal Cartel Office points out that it is for the controller to establish in detail which data will actually be processed in each use scenario. It further contends that the applicant in the main proceedings merely stated that *all processing* of data from sources other than Facebook would be necessary for *each of the purposes* of processing mentioned in the terms of service. By contrast, Meta Platforms Ireland takes the view that, without examining the specific aspects of each processing operation, the Federal Cartel Office cannot rule out the fact that the practice at issue might be based on the grounds in question and so cannot conclude that the practice is incompatible with the GDPR.

71 The user's consent is provided for in Article 6(1)(a) of the GDPR.

72 Paragraph 16 of the EDPB Guidelines 2/2019 states, inter alia, that both purpose limitation (Article 5(1)(b) of the GDPR) and data minimisation (Article 5(1)(c) of the GDPR) principles are particularly relevant in contracts for online services, which typically are not negotiated on an individual basis, in view of the acute risk that data controllers may seek to include general processing terms in contracts in order to maximise the possible collection and uses of data, without adequately specifying those purposes or considering data minimisation obligations.

73 According to paragraph 2 of the EDPB Guidelines 2/2019, that provision supports the freedom to conduct a business, which is guaranteed by Article 16 of the Charter, and reflects the fact that sometimes the contractual obligations towards the data subject cannot be performed without the data subject providing certain personal data. I note that the second situation envisaged in that provision, pursuant to which processing is necessary in order to take steps at the request of the data subject prior to entering into a contract, is not relevant in the present case. The same can be said for the question of the existence of a contract which is valid under both the applicable contract law and other legal requirements, including those relating to consumer contracts (see in particular Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (OJ 1993 L 95, p. 29)), which is not the subject of the reference for a preliminary ruling.

74 See, with regard to the provision corresponding to Article 6(1)(b) of the GDPR, contained in Article 7(e) of Directive 95/46, judgment of 16 December 2008, *Huber* (C-524/06, EU:C:2008:724, paragraph 52).

75 Moreover, although merely referencing or mentioning data processing in a contract is not enough to bring the processing in question within the scope of Article 6(1)(b) of the GDPR, processing may be objectively necessary even if not specifically mentioned in the contract, without prejudice to the controller's transparency obligations (see EDPB Guidelines 2/2019, paragraph 27).

76 See EDPB Guidelines 2/2019, paragraph 25.

that there must be no realistic, less intrusive alternatives,[77] taking into account the reasonable expectations of the data subject.[78] It also concerns the fact that, where the contract consists of several separate services or elements of a service that can be performed independently of one another, the applicability of Article 6(1)(b) of the GDPR should be assessed in the context of each of those services separately.[79]

55. As part of that justification, the referring court mentions the personalised content and continuous, seamless use of the group's products (or rather services).

56. As far as the personalised content is concerned, it seems to me that, although that activity may, to some extent, be in the user's interest, since it makes it possible to display content, particularly in the 'newsfeed', which, on the basis of an automated evaluation, matches the user's interests, it is not apparent that it is also necessary in order to provide the service of the social network at issue, such that the processing of personal data to that end does not require the user's consent.[80] For the purpose of that examination, consideration should also be given to the fact that the practice at issue concerns the processing not of data relating to the user's activities on the Facebook site or app, but data originating from external and therefore potentially unlimited sources. Therefore, I am curious as to what extent the processing might correspond to the expectations of an average user and, more generally, what 'degree of personalisation' the user can expect from the service he or she signs up for.[81]

57. With regard to the continuous, seamless use of the group's services, I note that a link between the various services offered by the applicant in the main proceedings – for example, between Facebook and Instagram – could be useful or even preferable on occasion for the user. However, I doubt that the processing of personal data from other group services (including Instagram) is necessary to provide Facebook services.[82]

77 See, to that effect, judgment of 9 November 2010, *Volker und Markus Schecke* and *Eifert* (C-92/09 and C-93/09, EU:C:2010:662, paragraph 86), and EDPB Guidelines 2/2019, paragraph 25. Paragraphs 27 to 32 of those guidelines refer to the fact that the processing is objectively necessary for a purpose that is integral to the delivery of that contractual service to the data subject, the controller having to be able to demonstrate how the main subject matter of the specific contract with the data subject cannot, as a matter of fact, be performed if the specific processing of the personal data in question does not occur. In Paragraph 33, those guidelines contain guidance questions for that purpose.

78 See EDPB Guidelines 2/2019, paragraph 32.

79 See EDPB Guidelines 2/2019, paragraph 37.

80 The Austrian Government makes the pertinent observation that in the past, the applicant in the main proceedings allowed Facebook users to choose between a chronological presentation and a personalised presentation of newsfeed content, which proves that an alternative method is possible.

81 Subject to the referring court's assessment, I do not believe that the collection and use of personal data outside Facebook are necessary for the provision of the services offered as part of the Facebook profile, such that the consent initially given for access to the social network (in other words, setting up a Facebook profile) may legitimately cover the processing of the user's personal data outside Facebook. Indeed, in that case, the use of the services in question would be subject to consent which is not necessary for the performance of the contract. Under Article 7(4) of the GDPR, the referring court will have to take the utmost account of that circumstance (which, according to recital 43 of the GDPR, constitutes a presumption of invalidity of the consent which the controller must rebut pursuant to Article 7(1) of the GDPR). Furthermore, such consent would not, in my view, comply with the rule whereby separate consent is required for different personal data processing operations (see the third part of point 74 of this Opinion), since there is nothing to link the user's initial consent to the opening of the Facebook account with any consent to the processing of personal data outside Facebook. Moreover, even in the event of any subsequent consent, given specifically for the data to be used outside Facebook, it is important to consider whether the controller offers the choice of an equivalent service that does not involve consenting to data use for additional purposes (see EDPB Guidelines 5/2020 of 4 May 2020 on consent under Regulation (EU) 2016/679 ('EDPB Guidelines 5/2020', paragraph 37, which also specify, in paragraph 38, that the controller cannot refer to an equivalent service offered by another operator).

82 As the Austrian Government points out, it seems decisive in that respect that the group's various products can be used independently of each other and that the use of each service is based on a separate user agreement. Moreover, as the Federal Cartel Office observes, the continuous, seamless use of the group's services, rather than being regarded as necessary for those services to function, should be regarded as being of interest to the user, such that, in principle, it would seem more appropriate that it should be at the user's discretion.

58. Second, according to Article 6(1)(f) of the GDPR, the processing of personal data is lawful only if it is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

59. According to the case-law of the Court of Justice, the provision in question lays down three cumulative conditions so that the processing of personal data is lawful, namely, first, the pursuit of a legitimate interest by the data controller or by the third party or parties to whom the data are disclosed; second, the need to process personal data for the purposes of the legitimate interests pursued; and third, that the fundamental rights and freedoms of the person concerned by the data protection do not take precedence. [83]

60. First, with regard to the pursuit of a legitimate interest, the GDPR and the case-law recognise a wide range of interests considered legitimate, [84] while specifying that, according to Article 13(1)(d) of the GDPR, it is the responsibility of the controller to indicate the legitimate interests pursued under Article 6(1)(f) of the GDPR. [85]

61. As to the condition relating to the necessity of processing personal data for the purposes of the legitimate interests pursued, according to the case-law of the Court of Justice, derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary. [86] It is necessary therefore for a close link to exist between the processing and the interest pursued, in the absence of alternatives that are more data-protection friendly, since it is not enough for the processing merely to be of use to the controller.

62. Lastly, as regards the balancing of the interests of the controller and the interests or fundamental rights and freedoms of the data subject, according to the case-law of the Court of Justice, it is for the referring court to weigh the interests at stake. [87] To that end, as stated in recital 47 of the GDPR, it is essential to take into consideration the reasonable expectations of data subjects based on their relationship with the controller and to determine whether the data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place.

83 See, by analogy, judgment of 4 May 2017, *Rīgas satiksme* (C-13/16, EU:C:2017:336, paragraph 28), on the equivalent provision to Article 6(1)(f) of the GDPR contained in Article 7(f) of Directive 95/46.

84 As noted in the Opinion of Advocate General Bobek in *Fashion ID* (C-40/17, EU:C:2018:1039, point 122), the notion of 'legitimate interest' under Directive 95/46 appeared to be rather elastic and open-ended. Indeed, as argued by the applicant in the main proceedings, the Court of Justice recognised several interests as being legitimate (see in particular judgments of 13 May 2014, *Google Spain and Google* (C-131/12, EU:C:2014:317, paragraph 81); of 19 October 2016, *Breyer* (C-582/14, EU:C:2016:779, paragraph 55); of 4 May 2017, *Rīgas satiksme* (C-13/16, EU:C:2017:336, paragraph 29); of 24 September 2019, *GC and Others (De-referencing of sensitive data)* (C-136/17, EU:C:2019:773, paragraph 53); of 11 December 2019, *Asociația de Proprietari bloc M5A-ScaraA* (C-708/18, EU:C:2019:1064, paragraph 59); and of 17 June 2021, *M.I.C.M.* (C-597/19, EU:C:2021:492, paragraphs 108 and 109). The same conclusion may be drawn, in my view, from recital 47 of the GDPR, which mentions, by way of illustration, situations in which the data subject is a client or in the service of the controller, and the processing of personal data for the purposes of preventing fraud or for direct marketing purposes, and from recital 49, which refers to network and information security and the security of the services offered.

85 That includes, in my view, the requirement to specify which processing operation is based on which legitimate interest.

86 See judgments of 4 May 2017, *Rīgas satiksme* (C-13/16, EU:C:2017:336, paragraph 30), and of 17 June 2021, *M.I.C.M.* (C-597/19, EU:C:2021:492, paragraph 110).

87 See, to that effect, judgments of 4 May 2017, *Rīgas satiksme* (C-13/16, EU:C:2017:336, paragraph 31), and of 17 June 2021, *M.I.C.M.* (C-597/19, EU:C:2021:492, paragraph 111). The Court of Justice recalled, in that regard, that Article 7(f) of Directive 95/46 (which corresponds to Article 6(1)(f) of the GDPR) precluded Member States from excluding, categorically and in general, the possibility of processing certain categories of personal data without allowing the opposing rights and interests at issue to be balanced against each other in a particular case, specifying that Member States could not definitively prescribe, for those categories, the result of the balancing of the opposing rights and interests, without allowing a different result by virtue of the particular circumstances of an individual case (judgment of 19 October 2016, *Breyer*, C-582/14, EU:C:2016:779, paragraph 62 and the case-law cited).

63. As part of that justification, the referring court mentions the personalisation of advertising, network security and product improvement.

64. First, with regard to the personalisation of advertising, it is clear from recital 47 of the GDPR that the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest of the controller. However, when it comes to the necessity of the processing, it is worth noting that the data in question originate from sources outside Facebook. The question therefore arises as to the 'degree of personalisation' of the advertising objectively necessary in that respect. As for balancing the interests at stake, consideration should be given to the nature of the legitimate interest in question (in this case, a purely economic interest), as well as the impact of the processing on the user, including his or her reasonable expectations, and to any safeguards put in place by the controller. [88]

65. Similar points can be made in relation to network security. While such a justification may constitute a legitimate interest of the controller, [89] it is less obvious to conclude that the processing is necessary in the present case, given that the data in question originate from sources outside Facebook. [90] At any rate, it is the responsibility of the controller to specify the security purposes on which any processing is based.

66. Lastly, with regard to product improvement, although security-related improvements – which fall under the specific justification examined above – are excluded, it seems to me that such a justification should be in the interest of the user rather than the data controller. From that perspective, it is unclear to what extent it could constitute a legitimate interest of the controller, thus avoiding the need for the user's consent. With regard to the condition of necessity and the balancing of the rights and interests at stake, I refer to the points made previously.

The fourth and fifth questions

67. By its fourth question referred for a preliminary ruling, which is essentially an extension of the second part of the third question referred, the referring court seeks to ascertain whether the recurrence of some of the situations mentioned implies the existence of a legitimate interest within the meaning of Article 6(1)(f) of the GDPR. Conversely, by its fifth question referred for a preliminary ruling, the referring court seeks to ascertain whether the need to respond to a

88 Opinion 6/2014 of the Article 29 Working Party makes some interesting points in that regard in paragraph III.3.4.

89 According to recital 49 of the GDPR, the processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security constitutes a legitimate interest of the data controller concerned. That could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution. I also note that, according to Article 32 of that regulation, the data controller must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, while Article 5(1)(f) of that regulation states that personal data must be processed in such a way as to ensure appropriate security of the personal data.

90 It is necessary therefore to check to what extent the processing of personal data external to the Facebook site or app is necessary for Facebook's security. While the referring court notes, in that respect, the possibility of using WhatsApp data in anti-spam mode (using information from WhatsApp accounts that send spam to take measures against the corresponding Facebook accounts) and Instagram data to identify dubious or unlawful behaviour, I doubt that the applicant in the main proceedings can claim the right to process personal data for 'policing' purposes in the broader sense, given that, according to the case-law of the Court of Justice, in the (different but related) field of data relating to electronic communications, even *legislative* measures providing, as a preventive measure, for the general and indiscriminate retention of traffic and location data are not compatible with Directive 2002/58 (see judgment of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraph 168). Besides, in the event that the need to ensure network security is a legal requirement, the controller can rely on the specific justification provided for in Article 6(1)(c) of the GDPR.

legitimate request to provide certain data, the need to combat harmful behaviour and promote security or to conduct research in the public interest and to promote safety, integrity and security justify the practice at issue. [91]

68. Regardless of whether those questions are admissible, [92] in general, it cannot be excluded, in relation to the fourth question, that certain clauses characterising the practice at issue may be justified by legitimate interests in the circumstances described by the referring court, [93] and in relation to the fifth question, that in certain situations, the practice at issue may be justified on the basis of the provisions cited.

69. Nevertheless, it is unclear from the order for reference whether, and to what extent, Meta Platforms Ireland has explained – for each purpose of processing and type of data processed – the actual legitimate interests pursued or other justification that may be relevant in the present case. [94] It is for the referring court, in the light of the foregoing, to examine to what extent, in the circumstances described by that court, the practice at issue is justified by the existence of legitimate interests of Meta Platforms Ireland in the processing of data within the meaning of Article 6(1)(f) of the GDPR or by any other condition laid down in Article 6(1)(c), (d) and (e) of that regulation.

The answer to the third to fifth questions

70. In conclusion, I propose that the answer to the third to fifth questions referred for a preliminary ruling should be that Article 6(1)(b), (c), (d), (e) and (f) of the GDPR must be interpreted as meaning that the practice at issue, or some of the activities that comprise it, may be covered by the exemptions laid down in those provisions, as long as each data processing method examined fulfils the conditions provided for by the justification specifically put forward by the controller, and that therefore:

– the processing is objectively necessary for the provision of the services relating to the Facebook account;

– the processing is necessary for the purposes of the legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed and does not have a disproportionate effect on the fundamental rights and freedoms of the data subject;

– the processing is necessary to respond to a legitimate request for certain data, to combat harmful behaviour and promote security, to conduct research in the public interest and to promote safety, integrity and security.

91 In accordance with Article 6(1)(c), (d) and (e) of the GDPR.

92 See point 48 of this Opinion.

93 In view of the wide range of legitimate interests recognised by the case-law (see point 60 of this Opinion). For example, in principle it seems obvious to me that the protection of minors may justify the adoption of appropriate protection measures, to prevent them from accessing inappropriate or dangerous content.

94 In accordance with Article 13(1)(c) and (d) of the GDPR, it is for the controller to state, for each purpose of processing, the legitimate interests pursued by it or by a third party.

The sixth question

71. By its sixth question referred for a preliminary ruling, the referring court is asking, in essence, whether Article 6(1)(a) and Article 9(2)(a) of the GDPR are to be interpreted as meaning that consent within the meaning of Article 4(11) of that regulation may be given effectively and freely to an undertaking having a dominant position in the national market for online social networks for private users.

72. I would first like to point out that Article 6(1)(a) and Article 9(2)(a) of the GDPR respectively require the consent of the data subject to the processing of personal data in general and to the processing of sensitive personal data. Furthermore, according to Article 4(11) of the GDPR, for the purposes of the regulation, 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which that person, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. [95]

73. With regard, in particular, to the requirement for 'freedom' of consent, which is the only requirement challenged in this case, I note that, according to recital 42 of the GDPR, consent should not be regarded as freely given if the data subject has no genuine or free choice [96] or is unable to refuse or withdraw consent without detriment. [97] Furthermore, as provided for in Article 7(1) of the GDPR (and reiterated in recital 42 thereof), where processing is based on consent of the data subject, the controller must be able to demonstrate that that person consented to the processing of his or her personal data.

74. As to relevance in the present case, as stated in the first sentence of recital 43 of the GDPR, consent should not serve as a valid legal ground for the processing of personal data where there is a 'clear imbalance' between the data subject and the controller. [98] Furthermore, under Article 7(4) of the GDPR, when assessing whether consent is freely given, utmost account must 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

95 In its judgment of 11 November 2020, *Orange Romania* (C-61/19, EU:C:2020:901, paragraphs 35 and 36 and the case-law cited), the Court of Justice clarified that the wording of Article 4(11) of the GDPR, which defines the 'consent of the data subject', appears even more stringent than Article 2(h) of Directive 95/46, in that it requires a 'freely given, specific, informed and unambiguous' indication of the data subject's wishes in the form of a statement or by 'a clear affirmative action' signifying agreement to the processing of personal data relating to him or her.

96 As the EDPB points out, the adjective 'free' implies real choice and control for data subjects (see EDPB Guidelines 5/2020, paragraph 13). The same paragraph specifies, inter alia, that consent has not been freely given if, on the one hand, the data subject feels compelled to consent or will endure *significant negative consequences* if they do not consent, and, on the other hand, consent is presented as a *non-negotiable part of terms and conditions*. Accordingly, consent will not be considered to be free if the data subject is unable to refuse or withdraw his or her consent without detriment. In that case, as the applicant in the main proceedings points out, the only disadvantage which the data subject must accept is that the service may, where appropriate, not have the same functionality or quality, to the extent that the processing of the data for which consent has not been given is technically necessary for that purpose.

97 In that respect, the EDPB Guidelines 5/2020 refer to deception, intimidation, coercion or significant negative consequences if the data subject does not consent, and confirms that the controller should be able to prove that the data subject had a free or genuine choice about whether to consent and that it was possible to withdraw consent (paragraph 47).

98 Apart from relations with public authorities and employment relations referred to in recital 43, which are not relevant in this case, paragraph 24 of the EDPB Guidelines 5/2020 refers to situations where the data subject is unable to exercise a real choice, or where there is a risk of deception, intimidation, coercion or significant negative consequences (for example, substantial extra costs) if he or she does not consent.

performance of that contract.[99] Lastly, according to the second sentence of recital 43 of the GDPR, consent is also 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.[100]

75. In the present case, I am of the opinion that any dominant position on the market held by a personal data controller operating a social network is a factor when assessing whether users of that network have given their consent freely. Indeed, the market power of the controller could lead to a clear imbalance in the sense described in point 74 of this Opinion.[101] However, it should be clarified that for such a market power to be relevant from the point of view of enforcing the GDPR, it need not necessarily be regarded as a dominant position within the meaning of Article 102 TFEU.[102] Besides, that circumstance alone cannot, in principle, render the consent invalid.[103]

76. Therefore, the validity of consent should be examined on a case-by-case basis, in the light of the other factors mentioned in points 73 and 74 of this Opinion, taking into account all the circumstances of the case and the controller's responsibility to demonstrate that the data subject has given his or her consent to the processing of personal data relating to him or her.

77. In conclusion, I propose that the answer to the sixth question referred for a preliminary ruling should be that Article 6(1)(a) and Article 9(2)(a) of the GDPR must be interpreted as meaning that the mere fact that an undertaking that operates a social network enjoys a dominant position in the domestic market for online social networks for private users cannot, on its own, render invalid the consent of the user of that network to the processing of his or her personal data under Article 4(11) of that regulation. However, that fact does play a role in the assessment of the freedom of consent within the meaning of that provision, which it is for the controller to demonstrate, taking into account, where appropriate, the existence of a clear imbalance of power between the data subject and the controller, any requirement for consent to the processing of personal data other than those strictly necessary for the provision of the services in question, the need for consent to be specific for each purpose of processing and the need to prevent the withdrawal of consent from being detrimental to users who withdraw it.

99 That question overlaps, in part, with the one that is the subject of the first part of the third question referred for a preliminary ruling (see points 53 to 57 of this Opinion). The second sentence of recital 43 of the GDPR specifies that, in such a situation, consent is presumed not to be freely given (paragraph 26 of the EDPB Guidelines 5/2020 states that in doing so, the GDPR ensures that the processing of personal data for which consent is sought cannot become directly or indirectly the counter-performance of a contract), since the use of the word 'presumed' clearly indicates that the cases in which consent is valid will be highly exceptional (see paragraph 35 of the guidelines). Moreover, Article 7(4) of the GDPR has been drafted in a non-exhaustive fashion by the words 'inter alia', meaning that there may be a range of other situations which are caught by that provision, including any inappropriate pressure or influence upon the data subject which prevents him or her from exercising his or her free will (EDPB Guidelines 5/2020, paragraph 14).

100 Recital 32 of the GDPR states, inter alia, that consent should cover all processing activities carried out for the same purpose or purposes and that when the processing has multiple purposes, consent should be given for all of them. In that respect, the EDPB Guidelines 5/2020 refer to the 'granularity' of consent as an obstacle to its freedom (paragraph 44).

101 Such a situation favours conditions that are not necessary for the performance of the contract (see points 53 to 57 of this Opinion).

102 As the Commission observes, the degree of relative market power of the undertaking that is critical for consent to be valid under the GDPR cannot necessarily be equated with the threshold for market dominance within the meaning of Article 102 TFEU.

103 Although the existence of a dominant position alone does not preclude the possibility of consent to the processing of personal data being freely given, the absence of such a position is not, on its own, a sufficient guarantee that such consent is valid in all circumstances.

Conclusion

78. In the light of the foregoing, I propose that the Court of Justice reply to the questions referred for a preliminary ruling by the Oberlandesgericht Düsseldorf (Higher Regional Court, Düsseldorf, Germany) as follows:

(1) Articles 51 to 66 of Regulation (EU) 2016/679 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 (General Data Protection Regulation)

must be interpreted as meaning that a competition authority, within the framework of its powers under the competition rules, may examine, as an incidental question, the compliance of the practices investigated with the rules of that regulation, while taking into account any decision or investigation of the competent supervisory authority on the basis of said regulation, informing and, where appropriate, consulting that authority.

(2) Article 9(1) of Regulation 2016/679

must be interpreted as meaning that the prohibition on processing sensitive personal data may include the processing of data carried out by an operator of an online social network consisting in the collection of the user's data when that user visits other websites or apps or enters such data into those websites or apps, linking the data to the user account on the social network and then using the data, provided that the information processed, considered in isolation or aggregated, allows user profiling based on the categories that emerge from the types of sensitive personal data mentioned in that article.

Article 9(2)(e) of that regulation

must be interpreted as meaning that a user does not manifestly make public the data revealed by visiting websites and apps or entered into those websites or apps or resulting from having clicked on buttons integrated into those websites or apps.

(3) Article 6(1)(b), (c), (d), (e) and (f) of Regulation 2016/679

must be interpreted as meaning that the practice consisting in (i) the *collection* of data from other group services, as well as from third-party websites and apps, by interfaces integrated into the latter or by cookies placed on the user's computer or mobile terminal, (ii) the *linking* of such data with the user's Facebook account and (iii) the *use* of said data or some of the activities comprising that practice may be covered by the exemptions laid down in those provisions, as long as each data processing method examined fulfils the conditions provided for by the justification specifically put forward by the controller, and that therefore:

– the processing is objectively necessary for the provision of the services relating to the Facebook account;

– the processing is necessary for the purposes of the legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed and does not have a disproportionate effect on the fundamental rights and freedoms of the data subject;

– the processing is necessary to respond to a legitimate request for certain data, to combat harmful behaviour and promote security, to conduct research in the public interest and to promote safety, integrity and security.

(4) Articles 6(1)(a) and 9(2)(a) of Regulation 2016/679

must be interpreted as meaning that the mere fact that an undertaking providing a social network enjoys a dominant position in the domestic market for online social networks for private users cannot, on its own, render invalid the consent of the user of that network to the processing of his or her personal data under Article 4(11) of that regulation. However, that fact does play a role in the assessment of the freedom of consent within the meaning of that provision, which it is for the controller to demonstrate, taking into account, where appropriate, the existence of a clear imbalance of power between the data subject and the controller, any requirement for consent to the processing of personal data other than those strictly necessary for the provision of the services in question, the need for consent to be specific for each purpose of processing and the need to prevent the withdrawal of consent from being detrimental to users who withdraw it.