Reports of Cases

JUDGMENT OF THE COURT (Grand Chamber)

4 July 2023 *

Table of contents

* Language of the case: German.

(Reference for a preliminary ruling – Protection of natural persons with regard to the processing of personal data – Regulation (EU) 2016/679 – Social networks – Abuse of a dominant position by the operator of such a network – Abuse which entails the processing of the personal data of the users of that network as provided for in its general terms of use – Powers of a competition authority of a Member State to find that processing is not consistent with that regulation – Reconciliation with the powers of the national data protection supervisory authorities – Article 4(3) TEU – Principle of sincere cooperation – Points (a) to (f) of the first subparagraph of Article 6(1) of Regulation 2016/679 – Whether the processing is lawful – Article 9(1) and (2) – Processing of special categories of personal data – Article 4(11) – Concept of 'consent')

In Case C-252/21,

REQUEST for a preliminary ruling under Article 267 TFEU from the Oberlandesgericht Düsseldorf (Higher Regional Court, Düsseldorf, Germany), made by decision of 24 March 2021, received at the Court on 22 April 2021, in the proceedings

Meta Platforms Inc., formerly Facebook Inc.,

Meta Platforms Ireland Ltd, formerly Facebook Ireland Ltd,

Facebook Deutschland GmbH

v

Bundeskartellamt,

intervener:

Verbraucherzentrale Bundesverband eV,

THE COURT (Grand Chamber),

composed of K. Lenaerts, President, L. Bay Larsen, Vice-President, A. Prechal, K. Jürimäe, C. Lycourgos, M. Safjan, L.S. Rossi (Rapporteur), D. Gratsias and M.L. Arastey Sahún, Presidents of Chambers, J.-C. Bonichot, S. Rodin, F. Biltgen, M. Gavalec, Z. Csehi and O. Spineanu-Matei, Judges,

Advocate General: A. Rantos,

Registrar: D. Dittert, Head of Unit,

having regard to the written procedure and further to the hearing on 10 May 2022,

after considering the observations submitted on behalf of:

– Meta Platforms Inc., formerly Facebook Inc., Meta Platforms Ireland Ltd, formerly Facebook Ireland Ltd, and Facebook Deutschland GmbH, by M. Braun, M. Esser, L. Hesse, J. Höft and H.-G. Kamann, Rechtsanwälte,

– the Bundeskartellamt, by J. Nothdurft, K. Ost, I. Sewczyk and J. Topel, acting as Agents,

– Verbraucherzentrale Bundesverband eV, by S. Louven, Rechtsanwalt,

– the German Government, by J. Möller and P.-L. Krüger, acting as Agents,

– the Czech Government, by M. Smolek and J. Vláčil, acting as Agents,

– the Italian Government, by G. Palmieri, acting as Agent, and E. De Bonis and P. Gentili, avvocati dello Stato,

– the Austrian Government, by A. Posch, J. Schmoll and G. Kunnert, acting as Agents,

– the European Commission, by F. Erlbacher, H. Kranenborg and G. Meessen, acting as Agents,

after hearing the Opinion of the Advocate General at the sitting on 20 September 2022,

gives the following

Judgment

1 This request for a preliminary ruling concerns the interpretation of Article 4(3) TEU and of Article 6(1), Article 9(1) and (2), Article 51(1) and Article 56(1) 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) (OJ 2016 L 119, p. 1, and corrigendum OJ 2018 L 127, p. 2; 'the GDPR').

2 The request has been made in proceedings between Meta Platforms Inc., formerly Facebook Inc., Meta Platforms Ireland Ltd, formerly Facebook Ireland Ltd, and Facebook Deutschland GmbH, on the one hand, and the Bundeskartellamt (Federal Cartel Office, Germany), on the other, concerning the decision by which the latter prohibited those companies from processing certain personal data as provided for in the general terms of use of the social network Facebook ('the general terms').

Legal context

European Union law

Regulation (EC) No 1/2003

3 Article 5 of 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), entitled 'Powers of the competition authorities of the Member States', provides:

'The competition authorities of the Member States shall have the power to apply Articles [101 and 102 TFEU] in individual cases. For this purpose, acting on their own initiative or on a complaint, they may take the following decisions:

– requiring that an infringement be brought to an end,

– ordering interim measures,

– accepting commitments,

– imposing fines, periodic penalty payments or any other penalty provided for in their national law.

Where on the basis of the information in their possession the conditions for prohibition are not met they may likewise decide that there are no grounds for action on their part.'

The GDPR

4 Recitals 1, 4, 38, 42, 43, 46, 47, 49 and 51 of the GDPR state:

'(1) The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the "Charter") and Article 16(1) [TFEU] provide that everyone has the right to the protection of personal data concerning him or her.

…

(4) The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity.

…

(38) Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child.

…

(42) Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. … For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.

(43) In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.

…

(46) The processing of personal data should also be regarded to be lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis. Some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters.

(47) The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. … At any rate the existence of a legitimate interest would need careful assessment including whether a 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. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in

circumstances where data subjects do not reasonably expect further processing. … The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.

…

(49) The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems … constitutes a legitimate interest of the data controller concerned. …

…

(51) Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Those personal data should include personal data revealing racial or ethnic origin, whereby the use of the term "racial origin" in this Regulation does not imply an acceptance by the [European] Union of theories which attempt to determine the existence of separate human races. The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person. Such personal data should not be processed, unless processing is allowed in specific cases set out in this Regulation, taking into account that Member States law may lay down specific provisions on data protection in order to adapt the application of the rules of this Regulation for compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. In addition to the specific requirements for such processing, the general principles and other rules of this Regulation should apply, in particular as regards the conditions for lawful processing. Derogations from the general prohibition for processing such special categories of personal data should be explicitly provided, inter alia, where the data subject gives his or her explicit consent or in respect of specific needs in particular where the processing is carried out in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms.'

5 Article 4 of that regulation provides:

'For the purposes of this Regulation:

(1) "personal data" means any information relating to an identified or identifiable natural person ("data subject"); …

(2) "processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

…

(7) "controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

…

(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;

…

(23) "cross-border processing" means either:
(a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or
(b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

…'

6 Article 5 of that regulation, headed 'Principles relating to processing of personal data', provides:

'1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency");

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; …

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimisation");

…

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ("accountability").'

7 Article 6 of the regulation, entitled 'Lawfulness of processing', reads as follows:

'1. 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;

(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.

…

3. The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:

(a) Union law; or

(b) Member State law to which the controller is subject.

…

… The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.'

8 Article 7 of the GDPR, entitled 'Conditions for consent', states:

'1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

…

4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.'

9 Article 9 of that 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 [provides] 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;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

…'

10 Article 13 of that regulation, 'Information to be provided where personal data are collected from the data subject', provides, in its paragraph 1, as follows:

'Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

…

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

…'

11 Chapter VI of the GDPR, 'Independent supervisory authorities', comprises Articles 51 to 59 of the regulation.

12 Under Article 51(1) and (2) of the GDPR, that article being entitled 'Supervisory authority':

'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 [European] Commission in accordance with Chapter VII.'

13 As set out in Article 55 of the GDPR, headed 'Competence':

'1. Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State.

2. Where processing is carried out by public authorities or private bodies acting on the basis of point (c) or (e) of Article 6(1), the supervisory authority of the Member State concerned shall be competent. In such cases Article 56 does not apply.'

14 Article 56(1) of that regulation, that article being entitled 'Competence of the lead supervisory authority', states:

'Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60.'

15 Article 57(1) of that regulation, that article being entitled 'Tasks', provides:

'Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory:

(a) monitor and enforce the application of this Regulation;

…

(g) cooperate with, including sharing information[,] and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Regulation;

…'

16 Article 58 of the regulation lists, in paragraph 1, the investigative powers available to each supervisory authority and states, in paragraph 5, that 'each Member State shall provide by law that its supervisory authority shall have the power to bring infringements of this Regulation to the attention of the judicial authorities and where appropriate, to commence or engage otherwise in legal proceedings, in order to enforce the provisions of this Regulation'.

17 Section 1, entitled ‘Cooperation’, of Chapter VII of the GDPR comprises Articles 60 to 62 of that regulation. Article 60, ‘Cooperation between the lead supervisory authority and the other supervisory authorities concerned’, provides in paragraph 1:

‘The lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with this Article in an endeavour to reach consensus. The lead supervisory authority and the supervisory authorities concerned shall exchange all relevant information with each other.’

18 Article 61(1) of the GDPR, that article being headed ‘Mutual assistance’, states:

‘Supervisory authorities shall provide each other with relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner, and shall put in place measures for effective cooperation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and investigations.’

19 Article 62 of that regulation, headed ‘Joint operations of supervisory authorities’, provides in paragraphs 1 and 2:

‘1. The supervisory authorities shall, where appropriate, conduct joint operations including joint investigations and joint enforcement measures in which members or staff of the supervisory authorities of other Member States are involved.

2. Where the controller or processor has establishments in several Member States or where a significant number of data subjects in more than one Member State are likely to be substantially affected by processing operations, a supervisory authority of each of those Member States shall have the right to participate in joint operations. …’

20 Section 2, entitled ‘Consistency’, of Chapter VII of the GDPR comprises Articles 63 to 67 of that regulation. Article 63, headed ‘Consistency mechanism’, is worded as follows:

‘In order to contribute to the consistent application of this Regulation throughout the Union, the supervisory authorities shall cooperate with each other and, where relevant, with the Commission, through the consistency mechanism as set out in this Section.’

21 Article 64(2) of that regulation is worded as follows:

‘Any supervisory authority, the Chair of the [European Data Protection] Board or the Commission may request that any matter of general application or producing effects in more than one Member State be examined by the [European Data Protection] Board with a view to obtaining an opinion, in particular where a competent supervisory authority does not comply with the obligations for mutual assistance in accordance with Article 61 or for joint operations in accordance with Article 62.’

22 Article 65(1) of that regulation, that article being headed 'Dispute resolution by the Board', provides:

'In order to ensure the correct and consistent application of this Regulation in individual cases, the [European Data Protection] Board shall adopt a binding decision in the following cases:

(a) where, in a case referred to in Article 60(4), a supervisory authority concerned has raised a relevant and reasoned objection to a draft decision of the lead supervisory authority and the lead supervisory authority has not followed the objection or has rejected such an objection as being not relevant or reasoned. The binding decision shall concern all the matters which are the subject of the relevant and reasoned objection, in particular whether there is an infringement of this Regulation;

(b) where there are conflicting views on which of the supervisory authorities concerned is competent for the main establishment;

…'

German law

23 Paragraph 19(1) of the Gesetz gegen Wettbewerbsbeschränkungen (Law against restrictions on competition), in its version published on 26 June 2013 (BGBl. 2013 I, p. 1750, 3245), last amended by Paragraph 2 of the Law of 16 July 2021 (BGBl. 2021 I, p. 2959) ('the GWB'), provides:

'The abuse of a dominant position by one or more undertakings is prohibited.'

24 In accordance with Paragraph 32(1) of the GWB:

'The competition authority may require undertakings or associations of undertakings to bring to an end an infringement of a provision of this Part or of Articles 101 or 102 [TFEU].'

25 Paragraph 50f(1) of the GWB provides:

'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 Paragraph 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 and the questions referred for a preliminary ruling

26 Meta Platforms Ireland operates the online social network Facebook within the European Union and promotes, inter alia via www.facebook.com, services that are free of charge for private users. Other undertakings of the Meta group offer, within the European Union, other online services, including Instagram, WhatsApp, Oculus and – until 13 March 2020 – Masquerade.

27 The business model of the online social network Facebook is based on financing through online advertising, which is tailored to the individual users of the social network according, inter alia, to their consumer behaviour, interests, purchasing power and personal situation. Such advertising is made possible in technical terms by the automated production of detailed profiles in respect of the network users and the users of the online services offered at the level of the Meta group. To that end, in addition to the data provided by the users directly when they sign up for the online services concerned, other user- and device-related data are also collected on and off that social network and the online services provided by the Meta group, and linked to their various user accounts. The aggregate view of the data allows detailed conclusions to be drawn about those users' preferences and interests.

28 For the processing of those data, Meta Platforms Ireland relies on the user agreement to which the users of the social network Facebook adhere when they click on the 'Sign up' button, thereby accepting the general terms drawn up by that company. Acceptance of those terms is necessary in order to be able to use the social network Facebook. With regard to the processing of personal data, the general terms refer to that company's data and cookies policies. According to those policies, Meta Platforms Ireland collects user- and device-related data about user activities on and off the social network and links the data with the Facebook accounts of the users concerned. The latter data, relating to activities outside the social network ('the off-Facebook data'), are data concerning visits to third-party webpages and apps, which are linked to Facebook through programming interfaces – 'Facebook Business Tools' – as well as data concerning the use of other online services belonging to the Meta group, including Instagram, WhatsApp, Oculus and – until 13 March 2020 – Masquerade.

29 The Federal Cartel Office brought proceedings against Meta Platforms, Meta Platforms Ireland and Facebook Deutschland, as a result of which, by decision of 6 February 2019, based on Paragraph 19(1) and Paragraph 32 of the GWB, it essentially prohibited those companies from making, in the general terms, the use of the social network Facebook by private users resident in Germany subject to the processing of their off-Facebook data and from processing the data without their consent on the basis of the general terms in force at the time. In addition, it required them to adapt those general terms in such a way that it is made clear that those data will neither be collected, nor linked with Facebook user accounts nor used without the consent of the user concerned, and it clarified the fact that such a consent is not valid if it is a condition for using the social network.

30 The Federal Cartel Office based its decision on the fact that the processing of the data of the users concerned, as provided for in the general terms and implemented by Meta Platforms Ireland, constituted an abuse of that company's dominant position on the market for online social networks for private users in Germany, within the meaning of Paragraph 19(1) of the GWB. In particular, according to the Federal Cartel Office, those general terms, as a result of that dominant position, constitute an abuse since the processing of the off-Facebook data that they provide for is not consistent with the underlying values of the GDPR and, in particular, it cannot be justified in the light of Article 6(1) and Article 9(2) of that regulation.

31 On 11 February 2019, Meta Platforms, Meta Platforms Ireland and Facebook Deutschland brought an action against the decision of the Federal Cartel Office before the Oberlandesgericht Düsseldorf (Higher Regional Court, Düsseldorf, Germany).

32 On 31 July 2019, Meta Platforms Ireland introduced new general terms expressly stating that the user, instead of paying to use Facebook products, agrees to being shown advertisements.

33 Furthermore, since 28 January 2020, Meta Platforms has been offering, at a global level, '*Off-Facebook Activity*', which allows the users of the social network Facebook to view a summary of the information about them that Meta group companies obtain in relation to their activities on other websites and apps, and to disconnect the data about past and future activities from their Facebook.com account if they so wish.

34 The Oberlandesgericht Düsseldorf (Higher Regional Court, Düsseldorf) has doubts (i) as to whether national competition authorities may review, in the exercise of their powers, whether the processing of personal data complies with the requirements set out in the GDPR; (ii) as to whether the operator of an online social network may process the data subject's sensitive personal data within the meaning of Article 9(1) and (2) of that regulation; (iii) as to the lawfulness of the processing by such an operator of the personal data of the user concerned, under Article 6(1) of that regulation; and (iv) as to the validity, in the light of point (a) of the first subparagraph of Article 6(1) and Article 9(2)(a) of that regulation, of the consent given to an undertaking with a dominant position on the national market for online social networks for the purposes of such processing.

35 In those circumstances, taking the view that the resolution of the case in the main proceedings depends on the answer to those questions, 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 [an] undertaking, such as [Meta Platforms 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.com account and uses them, does this collection and/or linking and/or use involve the processing of sensitive data for the purpose of that provision?

(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 [Meta Platforms 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 [Meta Platforms Ireland], which operates a digital social network funded by advertising and offers personalised content and advertising, network security, product improvement and consistent, 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.com 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 intended for 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 intended for the user to enable the undertaking to improve its products and engage in direct marketing;

– research and innovation for social good, 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 [collects 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, links those data with the user's Facebook.com account and uses them]?

(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.com 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 research for social good 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 [Meta Platforms 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, make findings, when assessing the balance of interests, as to 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.'

The questions referred

Questions 1 and 7

36 By Questions 1 and 7, which it is appropriate to examine together, the referring court asks, in essence, whether Article 51 et seq. of the GDPR must be interpreted as meaning that a competition authority of a Member State can find, in the context of the examination of an abuse of a dominant position by an undertaking within the meaning of Article 102 TFEU, that that undertaking's general terms of use relating to the processing of personal data and the implementation thereof are not consistent with the GDPR, and if so, whether Article 4(3) TEU must be interpreted as meaning that such a finding, of an incidental nature, by the competition authority is also possible where those terms are being investigated, simultaneously, by the competent lead supervisory authority in accordance with Article 56(1) of the GDPR.

37 In order to answer that question, it is important to recall at the outset that Article 55(1) of the GDPR states the general rule that each supervisory authority is to be competent for the performance of the tasks assigned to it and the exercise of the powers conferred on it, in accordance with that regulation, on the territory of its own Member State (judgment of 15 June 2021, *Facebook Ireland and Others*, C-645/19, EU:C:2021:483, paragraph 47 and the case-law cited).

38 The tasks assigned to those supervisory authorities include monitoring and enforcing the application of the GDPR, as provided for in Article 51(1) and Article 57(1)(a) of that regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to the processing of their personal data and to facilitate the free flow of such data within the European Union. In addition, in accordance with Article 51(2) and Article 57(1)(g) of that regulation, the supervisory authorities must cooperate with each other, including sharing information, and provide mutual assistance with a view to ensuring the consistency of application and enforcement of the regulation.

39 In order to carry out those tasks, Article 58 of the GDPR confers on those supervisory authorities, in paragraph 1, investigative powers, in paragraph 2, corrective powers, and in paragraph 5, the power to bring infringements of that regulation to the attention of the judicial authorities and, where appropriate, to commence legal proceedings in order to enforce the provisions of that regulation.

40 Without prejudice to the rule on competence set out in Article 55(1) of the GDPR, Article 56(1) of that regulation lays down, with respect to 'cross-border processing', within the meaning of Article 4(23) of that regulation, the 'one-stop-shop mechanism', based on an allocation of competences between one 'lead supervisory authority' and the other supervisory authorities concerned as well as on cooperation between all of those authorities in accordance with the cooperation procedure laid down in Article 60 of that regulation.

41 Furthermore, Article 61(1) of the GDPR obliges the supervisory authorities, inter alia, to provide each other with relevant information and mutual assistance in order to implement and apply that regulation in a consistent manner throughout the European Union. Article 63 of the GDPR states that it was for that purpose that provision was made for the consistency mechanism set out in Articles 64 and 65 of that regulation (judgment of 15 June 2021, *Facebook Ireland and Others*, C-645/19, EU:C:2021:483, paragraph 52 and the case-law cited).

42 That said, it should be noted that the rules on cooperation laid down in the GDPR are not addressed to the national competition authorities but govern cooperation between the national supervisory authorities concerned and the lead supervisory authority as well as, where appropriate, cooperation between those authorities and the European Data Protection Board and the Commission.

43 Neither the GDPR nor any other instrument of EU law provides for specific rules on cooperation between a national competition authority and the relevant national supervisory authorities concerned or the lead supervisory authority. Furthermore, there is no provision in that regulation that prevents the national competition authorities from finding, in the performance of their duties, that a data processing operation carried out by an undertaking in a dominant position and liable to constitute an abuse of that position does not comply with that regulation.

44 In that regard, it should be made clear, in the first place, that the supervisory authorities, on the one hand, and the national competition authorities, on the other, perform different functions and pursue their own objectives and tasks.

45 On the one hand, as has been stated in paragraph 38 above, under Article 51(1) and (2) and Article 57(1)(a) and (g) of the GDPR, the primary task of the supervisory authority is to monitor and enforce the application of that regulation, while contributing to its consistent application within the European Union, in order to protect the fundamental rights and freedoms of natural persons in relation to the processing of their personal data and to facilitate the free flow of such data within the European Union. To that end, as recalled in paragraph 39 above, the supervisory authority has at its disposal the various powers conferred on it under Article 58 of the GDPR.

46 On the other hand, in accordance with Article 5 of Regulation No 1/2003, the national competition authorities have the power to take, inter alia, decisions finding an abuse of a dominant position by an undertaking, within the meaning of Article 102 TFEU, whose objective is to establish a system which ensures that competition in the internal market is not distorted, having regard also to the consequences of such an abuse for consumers in that market.

47 As the Advocate General observed, in essence, in point 23 of his Opinion, when taking such a decision, a competition authority must assess, on the basis of all the specific circumstances of the case, whether, by resorting to methods different from those governing normal competition in products or services, the conduct of the dominant undertaking has the effect of hindering the maintenance of the degree of competition existing in the market or the growth of that competition (see, to that effect, judgment of 25 March 2021, *Deutsche Telekom* v *Commission*, C-152/19 P, EU:C:2021:238, paragraphs 41 and 42). In that respect, the compliance or non-compliance of that conduct with the provisions of the GDPR may, depending on the circumstances, be a vital clue among the relevant circumstances of the case in order to establish whether that conduct entails resorting to methods governing normal competition and to assess the consequences of a certain practice in the market or for consumers.

48 It follows that, in the context of the examination of an abuse of a dominant position by an undertaking on a particular market, it may be necessary for the competition authority of the Member State concerned also to examine whether that undertaking's conduct complies with rules other than those relating to competition law, such as the rules on the protection of personal data laid down by the GDPR.

49 In view of the different objectives pursued by the rules established in competition matters, in particular Article 102 TFEU, on the one hand, and those laid down in relation to the protection of personal data under the GDPR, on the other, it must be held that, where a national competition authority identifies an infringement of that regulation in the context of the finding of an abuse of a dominant position, it does not replace the supervisory authorities. In particular, that national competition authority neither monitors nor enforces the application of that regulation for the purpose referred to in Article 51(1) of the GDPR, namely in order to protect the fundamental rights and freedoms of natural persons in relation to processing or to facilitate the free flow of personal data within the European Union. Furthermore, by merely noting the non-compliance of a data processing operation with the GDPR for the sole purpose of establishing an abuse of a dominant position and by imposing measures to put an end to that abuse on a legal basis derived from competition law, that authority does not carry out any of the tasks set out in Article 57 of that regulation, nor does it make use of the powers reserved to the supervisory authority under Article 58 of that regulation.

50 Moreover, it is important to state that access to and use of personal data are of great importance in the context of the digital economy. That importance is illustrated, in the context of the dispute in the main proceedings, by the business model on which the social network Facebook relies, which, as recalled in paragraph 27 above, provides for financing through the marketing of personalised advertising messages according to user profiles established on the basis of personal data collected by Meta Platforms Ireland.

51 As pointed out by the Commission, inter alia, access to personal data and the fact that it is possible to process such data have become a significant parameter of competition between undertakings in the digital economy. Therefore, excluding the rules on the protection of personal data from the legal framework to be taken into consideration by the competition authorities when examining an abuse of a dominant position would disregard the reality of this economic development and would be liable to undermine the effectiveness of competition law within the European Union.

52 However, in the second place, it should be noted that, where a national competition authority considers it necessary to rule, in the context of a decision on an abuse of a dominant position, on the compliance or non-compliance with the GDPR of the processing of personal data by the

undertaking in question, that authority and the supervisory authority concerned or, where appropriate, the competent lead supervisory authority within the meaning of that regulation must cooperate with each other in order to ensure the consistency of application of that regulation.

53 Although, as has been noted in paragraphs 42 and 43 above, neither the GDPR nor any other instrument of EU law provides for specific rules in that regard, the fact remains that, as the Advocate General observed, in essence, in point 28 of his Opinion, when they apply the GDPR, the various national authorities involved are all bound by the duty of sincere cooperation enshrined in Article 4(3) TEU. Under that principle, in accordance with settled case-law, in areas covered by EU law, Member States, including their administrative authorities, must assist each other, in full mutual respect, in carrying out tasks which flow from the Treaties, take any appropriate measure to ensure fulfilment of the obligations arising from, inter alia, the acts of the institutions of the European Union and refrain from any measure which could jeopardise the attainment of the European Union's objectives (see, to that effect, judgments of 7 November 2013, *UPC Nederland*, C-518/11, EU:C:2013:709, paragraph 59, and of 1 August 2022, *Sea Watch*, C-14/21 and C-15/21, EU:C:2022:604, paragraph 156).

54 Thus, in the light of this principle, when national competition authorities are called upon, in the exercise of their powers, to examine whether an undertaking's conduct is consistent with the provisions of the GDPR, they are required to consult and cooperate sincerely with the national supervisory authorities concerned or with the lead supervisory authority, all of which are then bound, in that context, to observe their respective powers and competences, in such a way as to ensure that the obligations arising from the GDPR and the objectives of that regulation are complied with while their effectiveness is safeguarded.

55 The examination by a competition authority of an undertaking's conduct in the light of the provisions of the GDPR may entail the risk of divergences between that authority and the supervisory authorities in the interpretation of that regulation.

56 It follows that, where, in the context of the examination seeking to establish whether there is an abuse of a dominant position within the meaning of Article 102 TFEU by an undertaking, a national competition authority takes the view that it is necessary to examine whether that undertaking's conduct is consistent with the provisions of the GDPR, that authority must ascertain whether that conduct or similar conduct has already been the subject of a decision by the competent national supervisory authority or the lead supervisory authority or the Court. If that is the case, the national competition authority cannot depart from it, although it remains free to draw its own conclusions from the point of view of the application of competition law.

57 Where it has doubts as to the scope of the assessment carried out by the competent national supervisory authority or the lead supervisory authority, where the conduct in question or similar conduct is, simultaneously, under examination by those authorities, or where, in the absence of investigation by those authorities, it takes the view that an undertaking's conduct is not consistent with the provisions of the GDPR, the national competition authority must consult and seek their cooperation in order to dispel its doubts or to determine whether it must wait for the supervisory authority concerned to take a decision before starting its own assessment.

58 For its part, where the supervisory authority is called upon by a national competition authority, it must respond to such a request for information or cooperation within a reasonable period of time, providing the latter with the information in its possession capable of dispelling that authority's

doubts as to the scope of the assessment carried out by the supervisory authority or, where appropriate, by informing the national competition authority if it intends to initiate the cooperation procedure with the other supervisory authorities concerned or with the lead supervisory authority, in accordance with Article 60 et seq. of the GDPR, in order to reach a decision seeking to establish whether or not the conduct in question is consistent with that regulation.

59 In the absence of a reply, within a reasonable time, from the supervisory authority thus called upon, the national competition authority may continue its own investigation. The same applies where the competent national supervisory authority and the lead supervisory authority have no objection to such an investigation being continued without having to wait for a decision on their part.

60 In the present case, it is apparent from the file before the Court that in October and November 2018, that is to say, before the adoption of the decision of 6 February 2019, the Federal Cartel Office contacted the Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) (Federal Commissioner for Data Protection and Freedom of Information, Germany), the Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (Commissioner for Data Protection and Freedom of Information, Hamburg, Germany), which is the competent authority for Facebook Deutschland, and the Data Protection Commission (DPC) (Ireland), to notify those authorities of the action it had taken. In addition, it is apparent that the Federal Cartel Office obtained confirmation that no investigation was being conducted at the time by those authorities in relation to facts similar to those at issue in the main proceedings, and they raised no objection to its actions. Finally, in paragraphs 555 and 556 of its decision of 6 February 2019, the Federal Cartel Office expressly referred to that cooperation.

61 In those circumstances, and subject to verification by the referring court, the Federal Cartel Office appears to have fulfilled its obligations of sincere cooperation with the national supervisory authorities concerned and the lead supervisory authority.

62 In the light of the foregoing, the answer to Questions 1 and 7 is that Article 51 et seq. of the GDPR and Article 4(3) TEU must be interpreted as meaning that, subject to compliance with its duty of sincere cooperation with the supervisory authorities, a competition authority of a Member State can find, in the context of the examination of an abuse of a dominant position by an undertaking within the meaning of Article 102 TFEU, that that undertaking's general terms of use relating to the processing of personal data and the implementation thereof are not consistent with that regulation, where that finding is necessary to establish the existence of such an abuse.

63 In view of this duty of sincere cooperation, the national competition authority cannot depart from a decision by the competent national supervisory authority or the competent lead supervisory authority concerning those general terms or similar general terms. Where it has doubts as to the scope of such a decision, where those terms or similar terms are, simultaneously, under examination by those authorities, or where, in the absence of an investigation or decision by those authorities, the competition authority takes the view that the terms in question are not consistent with the GDPR, it must consult and seek the cooperation of those supervisory authorities in order to dispel its doubts or to determine whether it must wait for them to take a decision before starting its own assessment. In the absence of any objection on their part or of any reply within a reasonable time, the national competition authority may continue its own investigation.

Question 2

64 By Question 2(a), the referring court asks, in essence, whether Article 9(1) of the GDPR must be interpreted as meaning that, where the user of an online social network visits websites or apps to which one or more of the categories referred to in that provision relate and, as the case may be, enters information into them when registering or when placing online orders, the processing of personal data by the operator of that online social network, which entails the collection – by means of integrated interfaces, cookies or similar storage technologies – of data from visits to those sites and apps and of the information entered by the user, the linking of all those data with the user's social network account and the use of those data by that operator, must be regarded as 'processing of special categories of personal data' within the meaning of that provision, which is in principle prohibited, subject to the derogations provided for in Article 9(2).

65 If so, the referring court asks, in essence, by Question 2(b), whether Article 9(2)(e) of the GDPR must be interpreted as meaning that, where the user of an online social network visits websites or apps to which the categories set out in Article 9(1) of the GDPR relate, enters information into those sites or apps or clicks or taps on the buttons integrated into them, such as the 'Like' or 'Share' buttons or the buttons enabling the user to identify himself or herself on those sites or apps using the login credentials linked to his or her online social network user account, his or her telephone number or email address, the user is deemed to have manifestly made public, within the meaning of the first of those provisions, the data collected on that occasion by the operator of that online social network via cookies or similar storage technologies.

Question 2(a)

66 Recital 51 of the GDPR states that personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. That recital further states that such personal data should not be processed unless processing is allowed in the specific cases set out in that regulation.

67 In that context, Article 9(1) of the GDPR lays down the principle that the processing of special categories of personal data listed therein is prohibited. This includes data revealing racial or ethnic origin, political opinions, religious beliefs and data concerning health or a natural person's sex life or sexual orientation.

68 For the purposes of applying Article 9(1) of the GDPR, it is important to determine, where personal data is processed by the operator of an online social network, if those data allow information falling within one of the categories referred to in that provision to be revealed, irrespective of whether that information concerns a user of that network or any other natural person. If so, then such processing of personal data is prohibited, subject to the derogations provided for in Article 9(2) of the GDPR.

69 As the Advocate General observed, in essence, in points 40 and 41 of his Opinion, that fundamental prohibition, laid down in Article 9(1) of the GDPR, is independent of whether or not the information revealed by the processing operation in question is correct and of whether the controller is acting with the aim of obtaining information that falls within one of the special categories referred to in that provision.

70 In view of the significant risks to the fundamental freedoms and fundamental rights of data subjects arising from any processing of personal data falling within the categories referred to in Article 9(1) of the GDPR, the objective thereof is to prohibit such processing, irrespective of its stated purpose.

71 In the present case, the processing operation at issue in the main proceedings carried out by Meta Platforms Ireland entails, first of all, the collection of personal data of the users of the social network Facebook when they visit websites or apps – including those that may reveal information falling within one or more of the categories referred to in Article 9(1) of the GDPR – and, as the case may be, they enter information into them when they register or place online orders, then the linking of those data with those users' social network accounts and, lastly, the use of those data.

72 In that regard, it will be for the referring court to determine whether the data thus collected, on their own or by linking them with the Facebook accounts of the users concerned, actually allow such information to be revealed, irrespective of whether that information concerns a user of that network or any other natural person. However, given the referring court's questions, it should be made clear that it appears, subject to verification by that court, that the processing of data relating to visits to the websites or apps in question may, in certain cases, reveal such information without it being necessary for those users to enter information into them when they register or place online orders.

73 In the light of the foregoing, the answer to Question 2(a) is that Article 9(1) of the GDPR must be interpreted as meaning that, where the user of an online social network visits websites or apps to which one or more of the categories referred to in that provision relate and, as the case may be, enters information into them when registering or when placing online orders, the processing of personal data by the operator of that online social network, which entails the collection – by means of integrated interfaces, cookies or similar storage technologies – of data from visits to those sites and apps and of the information entered by the user, the linking of all those data with the user's social network account and the use of those data by that operator, must be regarded as 'processing of special categories of personal data' within the meaning of that provision, which is in principle prohibited, subject to the derogations provided for in Article 9(2), where that data processing allows information falling within one of those categories to be revealed, irrespective of whether that information concerns a user of that network or any other natural person.

Question 2(b)

74 As regards Question 2(b), as reformulated in paragraph 65 above and which relates to the derogation laid down in Article 9(2)(e) of the GDPR, it must be recalled that, under that provision, the fundamental prohibition of any processing of special categories of personal data, established in Article 9(1) of the GDPR, does not apply in the circumstance where the processing relates to personal data which are 'manifestly made public by the data subject'.

75 As a preliminary point, it should be noted that, first, the derogation applies only to data which are manifestly made public 'by the data subject'. Accordingly, it is not applicable to data concerning persons other than the person who made those data public.

76 Second, in so far as it provides for an exception to the principle that the processing of special categories of personal data is prohibited, Article 9(2) of the GDPR must be interpreted strictly (see, to that effect, judgments of 17 September 2014, *Baltic Agro*, C-3/13, EU:C:2014:2227, paragraph 24 and the case-law cited, and of 6 June 2019, *Weil*, C-361/18, EU:C:2019:473, paragraph 43 and the case-law cited).

77 It follows that, for the purposes of the application of the exception laid down in Article 9(2)(e) of the GDPR, it is important to ascertain whether the data subject had intended, explicitly and by a clear affirmative action, to make the personal data in question accessible to the general public.

78 In that regard, as regards, first, visits to websites or apps to which one or more of the categories referred to in Article 9(1) of the GDPR relate, it should be noted that the user concerned does not in any way thereby intend to make public the fact that he or she has visited those sites or apps and the data from those visits which can be linked to his or her person. The latter can at most expect the operator of the site or app to have access to those data and to share them, as the case may be and subject to that user's explicit consent, with certain third parties and not with the general public.

79 Thus, it cannot be inferred from the mere visit to such websites or apps by a user that the personal data in question were manifestly made public by that user within the meaning of Article 9(2)(e) of the GDPR.

80 Second, as regards the entering of information into those websites or apps and the clicking or tapping on buttons integrated into them, such as the 'Like' or 'Share' buttons or buttons enabling the user to identify himself or herself on a website or app using the login credentials linked to his or her Facebook user account, his or her telephone number or email address, it should be noted that these actions mean that the user interacts with the website or app in question, and, as the case may be, the website of the online social network, whereby the extent to which that interaction is public may vary in that it may be determined by the individual settings chosen by that user.

81 In those circumstances, it is for the referring court to ascertain whether it is possible for the users concerned to decide, on the basis of settings selected with full knowledge of the facts, whether to make the information entered into the websites or apps in question and the data from clicking or tapping on buttons integrated into them accessible to the general public or, rather, to a more or less limited number of selected persons.

82 When the users concerned actually have that choice, they can be regarded, when they voluntarily enter information into a website or app or when they click or tap on buttons integrated into them, as manifestly making public, within the meaning of Article 9(2)(e) of the GDPR, data relating to them only in the circumstance where, on the basis of individual settings selected with full knowledge of the facts, those users have clearly made the choice to have the data made accessible to an unlimited number of persons, which it is for the referring court to ascertain.

83 By contrast, if no such individual settings are available, it must be held, in the light of what has been stated in paragraph 77 above, that, where users voluntarily enter information into a website or app or click or tap on buttons integrated into them, they must, in order to be deemed to have manifestly made those data public, have explicitly consented, on the basis of express information provided by that site or app prior to any such entering or clicking or tapping, to the data being viewed by any person having access to that site or app.

84 In the light of the foregoing, the answer to Question 2(b) is that Article 9(2)(e) of the GDPR must be interpreted as meaning that, where the user of an online social network visits websites or apps to which one or more of the categories set out in Article 9(1) of the GDPR relate, the user does not manifestly make public, within the meaning of the first of those provisions, the data relating to those visits collected by the operator of that online social network via cookies or similar storage technologies.

85 Where he or she enters information into such websites or apps or where he or she clicks or taps on buttons integrated into those sites and apps, such as the 'Like' or 'Share' buttons or buttons enabling the user to identify himself or herself on those sites or apps using login credentials linked to his or her social network user account, his or her telephone number or email address, that user manifestly makes public, within the meaning of Article 9(2)(e), the data thus entered or resulting from the clicking or tapping on those buttons only in the circumstance where he or she has explicitly made the choice beforehand, as the case may be on the basis of individual settings selected with full knowledge of the facts, to make the data relating to him or her publicly accessible to an unlimited number of persons.

Questions 3 to 5

86 By Questions 3 and 4, which it is appropriate to examine together, the referring court asks, in essence, whether and under what conditions points (b) and (f) of the first subparagraph of Article 6(1) of the GDPR must be interpreted as meaning that the processing of personal data by the operator of an online social network, which entails the collection of data of the users of such a network from other services of the group to which that operator belongs or from visits by those users to third-party websites or apps, the linking of those data with the social network account of those users and the use of such data, may be considered to be necessary for the performance of a contract to which the data subjects are party, within the meaning of point (b), or for the purposes of the legitimate interests pursued by the controller or by a third party, within the meaning of point (f). That court asks, in particular, whether, to that end, certain interests which it explicitly lists constitute 'legitimate interests' within the meaning of the latter provision.

87 By Question 5, the referring court asks, in essence, whether points (c) to (e) of the first subparagraph of Article 6(1) of the GDPR must be interpreted as meaning that such processing of personal data can be regarded as necessary for compliance with a legal obligation to which the controller is subject, within the meaning of point (c), in order to protect the vital interests of the data subject or of another natural person, within the meaning of point (d), or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, within the meaning of point (e), where such processing is carried out, respectively, in order to respond to a legitimate request for certain data, to combat harmful behaviour and promote security, and to research for social good and promote safety, integrity and security.

Preliminary observations

88 As a preliminary point, it must be observed, first, that Questions 3 to 5 are raised on account of the fact that, according to the findings of the Federal Cartel Office in its decision of 6 February 2019, the users of the social network Facebook cannot be regarded as having given their consent to the processing of their data at issue in the main proceedings, within the meaning of point (a) of the first subparagraph of Article 6(1) and Article 9(2)(a) of the GDPR. It is therefore in that context that the referring court, while asking the Court by Question 6 in relation to that premiss,

considers that it must ascertain whether that processing corresponds to one of the other conditions of lawfulness referred to in points (b) to (f) of the first subparagraph of Article 6(1)of that regulation.

89 In that context, it should be noted that the operations entailing the collection, the linking and the use of the data, referred to in Questions 3 to 5, may include both sensitive data within the meaning of Article 9(1) of the GDPR and non-sensitive data. It must be made clear that, where a set of data containing both sensitive data and non-sensitive data is subject to such operations and is, in particular, collected *en bloc* without it being possible to separate the data items from each other at the time of collection, the processing of that set of data must be regarded as being prohibited, within the meaning of Article 9(1) of the GDPR, if it contains at least one sensitive data item and none of the derogations in Article 9(2) of that regulation applies.

90 Second, in order to answer Questions 3 to 5, it should be recalled that the first subparagraph of Article 6(1) of the GDPR sets out an exhaustive and restrictive list of the cases in which processing of personal data can be regarded as lawful. Thus, in order to be capable of being regarded as such, processing must fall within one of the cases provided for in that provision (judgment of 22 June 2021, *Latvijas Republikas Saeima (Penalty points)*, C-439/19, EU:C:2021:504, paragraph 99 and the case-law cited).

91 Under point (a) of the first subparagraph of Article 6(1) of that regulation, the processing of personal data is lawful if and to the extent that the data subject has given consent for one or more specific purposes.

92 In the absence of such consent, or where that consent is not freely given, specific, informed and unambiguous, within the meaning of Article 4(11) of the GDPR, such processing is nevertheless justified where it meets one of the requirements of necessity mentioned in points (b) to (f) of the first subparagraph of Article 6(1) of that regulation.

93 In that context, the justifications provided for in that latter provision, in so far as they allow the processing of personal data carried out in the absence of the data subject's consent to be made lawful, must be interpreted restrictively (see, to that effect, judgment of 24 February 2022, *Valsts ieņēmumu dienests (Processing of personal data for tax purposes)*, C-175/20, EU:C:2022:124, paragraph 73 and the case-law cited).

94 Furthermore, as the Court has held, where it can be found that the processing of personal data is necessary in respect of one of the justifications provided for in points (b) to (f) of the first subparagraph of Article 6(1) of the GDPR, it is not necessary to determine whether that processing also falls within the scope of another of those justifications (see, to that effect, judgment of 1 August 2022, *Vyriausioji tarnybinės etikos komisija*, C-184/20, EU:C:2022:601, paragraph 71).

95 It should finally be noted that, in accordance with Article 5 of the GDPR, the controller bears the burden of proving that those data are collected, inter alia, for specified, explicit and legitimate purposes and that they are processed lawfully, fairly and in a transparent manner in relation to the data subject. In addition, according to Article 13(1)(c) of that regulation, where personal data are collected from the data subject, the controller must inform the data subject of the purposes of the processing for which those data are intended as well as the legal basis for the processing.

96 Although it is for the referring court to determine whether the various elements of the processing at issue in the main proceedings are justified by one or other of the necessity requirements referred to in points (b) to (f) of the first subparagraph of Article 6(1) of the GDPR, the Court can nevertheless provide it with useful guidance to enable it to resolve the dispute before it.

Questions 3 and 4

97 As regards, in the first place, point (b) of the first subparagraph of Article 6(1) of the GDPR, that provision provides that processing of personal data is lawful if it 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'.

98 In that regard, in order for the processing of personal data to be regarded as necessary for the performance of a contract, within the meaning of that provision, it must be objectively indispensable for a purpose that is integral to the contractual obligation intended for the data subject. The controller must therefore be able to demonstrate how the main subject matter of the contract cannot be achieved if the processing in question does not occur.

99 The fact that such processing may be referred to in the contract or may be merely useful for the performance of the contract is, in itself, irrelevant in that regard. The decisive factor for the purposes of applying the justification set out in point (b) of the first subparagraph of Article 6(1) of the GDPR is rather that the processing of personal data by the controller must be essential for the proper performance of the contract concluded between the controller and the data subject and, therefore, that there are no workable, less intrusive alternatives.

100 In that regard, as the Advocate General observed in point 54 of his Opinion, where the contract consists of several separate services or elements of a service that can be performed independently of one another, the applicability of point (b) of the first subparagraph of Article 6(1) of the GDPR should be assessed in the context of each of those services separately.

101 In the present case, in the context of the justifications that are capable of falling within the scope of that provision, the referring court mentions, as elements intended to ensure the proper performance of the contract concluded between Meta Platforms Ireland and its users, personalised content and the consistent and seamless use of the Meta group's own services.

102 As regards, first, the justification based on personalised content, it is important to note that, although such a personalisation is useful to the user, in so far as it enables the user, inter alia, to view content corresponding to a large extent to his or her interests, the fact remains that, subject to verification by the referring court, personalised content does not appear to be necessary in order to offer that user the services of the online social network. Those services may, where appropriate, be provided to the user in the form of an equivalent alternative which does not involve such a personalisation, such that the latter is not objectively indispensable for a purpose that is integral to those services.

103 As regards, second, the justification based on the consistent and seamless use of the Meta group's own services, it is apparent from the file before the Court that there is no obligation to subscribe to the various services offered by the Meta group in order to create a user account in the social network Facebook. The various products and services offered by that group can be used independently of each other and the use of each product or service is based on the conclusion of a separate user agreement.

104 Therefore, and subject to verification by the referring court, the processing of personal data from services offered by the Meta group, other than the online social network service, does not appear to be necessary for the latter service to be provided.

105 As regards, in the second place, point (f) of the first subparagraph of Article 6(1) of the GDPR, that provision provides that 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'.

106 As the Court has already held, that provision lays down three cumulative conditions so that the processing of personal data covered by that provision is lawful, namely, first, the pursuit of a legitimate interest by the data controller or by a third party; second, the need to process personal data for the purposes of the legitimate interests pursued; and third, that the interests or fundamental freedoms and rights of the person concerned by the data protection do not take precedence over the legitimate interest of the controller or of a third party (judgment of 17 June 2021, *M.I.C.M.*, C-597/19, EU:C:2021:492, paragraph 106 and the case-law cited).

107 First, with regard to the condition relating to the pursuit of a legitimate interest, it must be stated that, according to Article 13(1)(d) of the GDPR, it is the responsibility of the controller, at the time when personal data relating to a data subject are collected from that person, to inform him or her of the legitimate interests pursued where that processing is based on point (f) of the first subparagraph of Article 6(1) of that regulation.

108 Second, with regard to the condition that the processing of personal data be necessary for the purposes of the legitimate interests pursued, that condition requires the referring court to ascertain that the legitimate data processing interests pursued cannot reasonably be achieved just as effectively by other means less restrictive of the fundamental rights and freedoms of data subjects, in particular the rights to respect for private life and to the protection of personal data guaranteed by Articles 7 and 8 of the Charter (see, to that effect, judgment of 22 June 2021, *Latvijas Republikas Saeima (Penalty points)*, C-439/19, EU:C:2021:504, paragraph 110 and the case-law cited).

109 In this context, it should also be recalled that the condition relating to the need for processing must be examined in conjunction with the 'data minimisation' principle enshrined in Article 5(1)(c) of the GDPR, in accordance with which personal data must be 'adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed' (see, to that effect, judgment of 11 December 2019, *Asociația de Proprietari bloc M5A-ScaraA*, C-708/18, EU:C:2019:1064, paragraph 48).

110 Third, with regard to the condition that the interests or fundamental rights and freedoms of the person concerned by the data protection do not take precedence over the legitimate interests of the controller or of a third party, the Court has already held that that condition entails a balancing of the opposing rights and interests at issue which depends in principle on the specific circumstances of the particular case and that, consequently, it is for the referring court to carry out that balancing exercise, taking account of those specific circumstances (judgment of 17 June 2021, *M.I.C.M.*, C-597/19, EU:C:2021:492, paragraph 111 and the case-law cited).

111 In this respect, it is apparent from the very wording of point (f) of the first subparagraph of Article 6(1) of the GDPR that it is necessary, in such a balancing exercise, to pay particular attention to the situation where the data subject is a child. According to recital 38 of that regulation, children merit specific protection with regard to the processing of their personal data because they may be less aware of the risks, consequences and safeguards concerned and of their rights related to such processing of personal data. Thus, such specific protection should, in particular, apply to the processing of personal data of children for the purposes of marketing or creating personality or user profiles or offering services aimed directly at children.

112 Furthermore, as can be seen from recital 47 of the GDPR, the interests and fundamental rights of the data subject may in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect such processing.

113 In the present case, in the context of the justifications that are capable of falling within the scope of point (f) of the first subparagraph of Article 6(1) of the GDPR, the referring court mentions personalised advertising, network security, product improvement, the sharing of informing with law-enforcement agencies, the fact that the user is a minor, research and innovation for social good and the offer of services for commercial communication intended for the user and of analytics tools intended for advertisers and other business partners, enabling them to evaluate their performance.

114 In that regard, it should be noted at the outset that the request for a preliminary ruling does not contain any explanation as to how research and innovation for social good or the fact that the user is a minor could justify, as legitimate interests within the meaning of point (f) of the first subparagraph of Article 6(1) of the GDPR, the collection and use of the data in question. Consequently, the Court is not in a position to rule on this matter.

115 First, with regard to personalised advertising, it must be borne in mind that, according to recital 47 of the GDPR, the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest of the controller.

116 However, such processing must also be necessary in order to achieve that interest and the interests or fundamental freedoms and rights of the data subject must not override that interest. In the context of that balancing of the opposing rights at issue, namely, those of the controller, on the one hand, and those of the data subject, on the other, account must be taken, as has been noted in paragraph 112 above, in particular of the reasonable expectations of the data subject as well as the scale of the processing at issue and its impact on that person.

117 In this regard, it is important to note that, despite the fact that the services of an online social network such as Facebook are free of charge, the user of that network cannot reasonably expect that the operator of the social network will process that user's personal data, without his or her consent, for the purposes of personalised advertising. In those circumstances, it must be held that the interests and fundamental rights of such a user override the interest of that operator in such personalised advertising by which it finances its activity, with the result that the processing by that operator for such purposes cannot fall within the scope of point (f) of the first subparagraph of Article 6(1) of the GDPR.

118 Furthermore, the processing at issue in the main proceedings is particularly extensive since it relates to potentially unlimited data and has a significant impact on the user, a large part – if not almost all – of whose online activities are monitored by Meta Platforms Ireland, which may give rise to the feeling that his or her private life is being continuously monitored.

119 Second, as regards the objective of ensuring network security, that objective, as stated in recital 49 of the GDPR, constitutes a legitimate interest of Meta Platforms Ireland, capable of justifying the processing operation at issue in the main proceedings.

120 However, as regards the need for that processing for the purposes of that legitimate interest, the referring court will have to ascertain whether and to what extent the processing of personal data collected from sources outside the social network Facebook is actually necessary to ensure that the internal security of that network is not compromised.

121 In that context, as noted in paragraphs 108 and 109 above, it will also have to ascertain whether the legitimate data processing interest pursued cannot reasonably be achieved just as effectively by other means less restrictive of the fundamental freedoms and rights of the data subjects, in particular the rights to respect for private life and to the protection of personal data guaranteed by Articles 7 and 8 of the Charter and whether the 'data minimisation' principle enshrined in Article 5(1)(c) of the GDPR has been observed.

122 Third, as regards the 'product improvement' objective, it cannot be ruled out from the outset that the controller's interest in improving the product or service with a view to making it more efficient and thus more attractive can constitute a legitimate interest capable of justifying the processing of personal data and that such processing may be necessary in order to pursue that interest.

123 However, subject to final assessment by the referring court in that respect, it appears doubtful whether, as regards the data processing at issue in the main proceedings, the 'product improvement' objective, given the scale of that processing and its significant impact on the user, as well as the fact that the user cannot reasonably expect those data to be processed by Meta Platforms Ireland, may override the interests and fundamental rights of such a user, particularly in the case where that user is a child.

124 Fourth, as regards the objective referred to by the referring court, relating to the sharing of information with law-enforcement agencies in order to prevent, detect and prosecute criminal offences, it must be held that that objective is not capable, in principle, of constituting a legitimate interest pursued by the controller, within the meaning of point (f) of the first subparagraph of Article 6(1) of the GDPR. A private operator such as Meta Platforms Ireland cannot rely on such a legitimate interest, which is unrelated to its economic and commercial activity. Conversely, that objective may justify processing by such an operator where it is objectively necessary for compliance with a legal obligation to which that operator is subject.

125 In the light of all the foregoing, the answer to Questions 3 and 4 is that point (b) of the first subparagraph of Article 6(1) of the GDPR must be interpreted as meaning that the processing of personal data by the operator of an online social network, which entails the collection of data of the users of such a network from other services of the group to which that operator belongs or from visits by those users to third-party websites or apps, the linking of those data with the social network account of those users and the use of those data, can be regarded as necessary for the performance of a contract to which the data subjects are party, within the meaning of that

provision, only on condition that the processing is objectively indispensable for a purpose that is integral to the contractual obligation intended for those users, such that the main subject matter of the contract cannot be achieved if that processing does not occur.

126 Point (f) of the first subparagraph of Article 6(1) of the GDPR must be interpreted as meaning that such processing can be regarded as necessary for the purposes of the legitimate interests pursued by the controller or by a third party, within the meaning of that provision, only on condition that the operator has informed the users from whom the data have been collected of a legitimate interest that is pursued by the data processing, that such processing is carried out only in so far as is strictly necessary for the purposes of that legitimate interest and that it is apparent from a balancing of the opposing interests, having regard to all the relevant circumstances, that the interests or fundamental freedoms and rights of those users do not override that legitimate interest of the controller or of a third party.

Question 5

127 In the first place, in so far as that question refers to points (c) and (e) of the first subparagraph of Article 6(1) of the GDPR, it must be recalled that, under point (c), processing of personal data is lawful if it is necessary for compliance with a legal obligation to which the controller is subject. In addition, under point (e), processing that 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 is also lawful.

128 Article 6(3) of the GDPR specifies, inter alia, in respect of those two situations in which processing is lawful, that the processing must be based on EU law or on Member State law to which the controller is subject, and that that legal basis must meet an objective of public interest and be proportionate to the legitimate aim pursued.

129 In the present case, the referring court seeks to ascertain whether the processing of personal data, such as that at issue in the main proceedings, may be regarded as justified in the light of point (c) of the first subparagraph of Article 6(1) of the GDPR, where it seeks to 'respond to a legitimate request for certain data', and, in the light of point (e) of the first subparagraph of Article 6(1) of that regulation, where its purpose is to 'research for social good' and it seeks to 'promote safety, integrity and security'.

130 However, it should be noted that the referring court has not provided the Court of Justice with any material enabling it to give a specific ruling in this respect.

131 It will therefore be for that court to ascertain, in the light of the conditions set out in paragraph 128 above, whether that processing can be regarded as being justified by the stated purposes.

132 In particular, given the observations made in paragraph 124 above, it will be for the referring court, inter alia, to inquire, for the purposes of applying point (c) of the first subparagraph of Article 6(1) of the GDPR, whether Meta Platforms Ireland is under a legal obligation to collect and store personal data in a preventive manner in order to be able to respond to any request from a national authority seeking to obtain certain data relating to its users.

133 Similarly, it will be for that court to assess, in the light of point (e) of the first subparagraph of Article 6(1) of the GDPR, whether Meta Platforms Ireland was entrusted with a task carried out in the public interest or in the exercise of official authority, in particular with a view of carrying

out research for the social good and to promote safety, integrity and security, bearing in mind that, given the type of activity and the essentially economic and commercial nature thereof, it seems unlikely that that private operator was entrusted with such a task.

134 In addition, the referring court will, if necessary, have to determine whether, in view of the scale of the data processing by Meta Platforms Ireland and of its significant incidence on the users of the social network Facebook, that processing is carried out only in so far as is strictly necessary.

135 As regards, in the second place, point (d) of the first subparagraph of Article 6(1) of the GDPR, that provision provides that the processing of personal data is lawful where it is necessary in order to protect the vital interests of the data subject or of another natural person.

136 As can be seen from recital 46 of that regulation, that provision covers the specific situation in which the processing of personal data is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. In that regard, the recital cites by way of example, inter alia, humanitarian purposes, such as monitoring epidemics and their spread, as well as situations of humanitarian emergencies, such as situations of natural and man-made disasters.

137 It follows from those examples and from the strict interpretation to be given to point (d) of the first subparagraph of Article 6(1) of the GDPR that, in view of the nature of the services provided by the operator of an online social network, such an operator, whose activity is essentially economic and commercial in nature, cannot rely on the protection of an interest which is essential for the life of its users or of another person in order to justify, absolutely and in a purely abstract and preventive manner, the lawfulness of data processing such as that at issue in the main proceedings.

138 In the light of the foregoing, the answer to Question 5 is that point (c) of the first subparagraph of Article 6(1) of the GDPR must be interpreted as meaning that the processing of personal data by the operator of an online social network, which entails the collection of data of the users of such a network from other services of the group to which that operator belongs or from visits by those users to third-party websites or apps, the linking of those data with the social network account of those users and the use of those data, is justified, under that provision, where it is actually necessary for compliance with a legal obligation to which the controller is subject, pursuant to a provision of EU law or the law of the Member State concerned, where that legal basis meets an objective of public interest and is proportionate to the legitimate aim pursued and where that processing is carried out only in so far as is strictly necessary.

139 Points (d) and (e) of the first subparagraph of Article 6(1) of the GDPR must be interpreted as meaning that such processing of personal data cannot, in principle and subject to verification by the referring court, be regarded as necessary in order to protect the vital interests of the data subject or of another natural person, within the meaning of point (d), or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, within the meaning of point (e).

Question 6

140 By Question 6, the referring court asks, in essence, whether point (a) of the first subparagraph of Article 6(1) and Article 9(2)(a) of the GDPR must be interpreted as meaning that consent given by the user of an online social network to the operator of such a network may be regarded as

satisfying the conditions of validity laid down in Article 4(11) of that regulation, in particular the condition that that consent must be freely given, where that operator holds a dominant position on the market for online social networks.

141 Point (a) of the first subparagraph of Article 6(1) and Article 9(2)(a) of the GDPR require the data subject's consent for the purposes of, respectively, processing his or her personal data for one or more specific purposes and processing special categories of data referred to in Article 9(1).

142 Article 4(11) of the GDPR, for its part, defines 'consent' as meaning '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'.

143 In the light of the referring court's questions, it is important to recall, in the first place, that, according to recital 42 of the GDPR, consent cannot be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.

144 In the second place, recital 43 of that regulation states that, in order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data where there is a clear imbalance between the data subject and the controller. That recital also clarifies that consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case.

145 In the third place, Article 7(4) of the GDPR provides that 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 performance of that contract.

146 It is on the basis of those considerations that Question 6 must be answered.

147 In that regard, it should be noted that, admittedly, the fact that the operator of an online social network, as controller, holds a dominant position on the social network market does not, as such, prevent the users of that social network from validly giving their consent, within the meaning of Article 4(11) of the GDPR, to the processing of their personal data by that operator.

148 The fact remains that, as the Advocate General observed, in essence, in point 75 of his Opinion, such a circumstance must be taken into consideration in assessing whether the user of that network has validly and, in particular, freely given consent, since that circumstance is liable to affect the freedom of choice of that user, who might be unable to refuse or withdraw consent without detriment, as stated in recital 42 of the GDPR.

149 Furthermore, the existence of such a dominant position may create a clear imbalance, within the meaning of recital 43 of the GDPR, between the data subject and the controller, that imbalance favouring, inter alia, the imposition of conditions that are not strictly necessary for the performance of the contract, which must be taken into account under Article 7(4) of that regulation. In that context, it must be borne in mind that, as stated in paragraphs 102 to 104 above, it does not appear, subject to verification by the referring court, that the processing at issue in the main proceedings is strictly necessary for the performance of the contract between Meta Platforms Ireland and the users of the social network Facebook.

150 Thus, those users must be free to refuse individually, in the context of the contractual process, to give their consent to particular data processing operations not necessary for the performance of the contract, without being obliged to refrain entirely from using the service offered by the online social network operator, which means that those users are to be offered, if necessary for an appropriate fee, an equivalent alternative not accompanied by such data processing operations.

151 Moreover, given the scale of the processing of the data in question and the significant impact of that processing on the users of that network as well as the fact that those users cannot reasonably expect data other than those relating to their conduct within the social network to be processed by the operator of that network, it is appropriate, within the meaning of recital 43, to have the possibility of giving separate consent for the processing of the latter data, on the one hand, and the off-Facebook data, on the other. It is for the referring court to ascertain whether such a possibility exists, in the absence of which the consent of those users to the processing of the off-Facebook data must be presumed not to be freely given.

152 Finally, it must be borne in mind that, pursuant to Article 7(1) of the GDPR, where processing is based on consent, it is the controller who bears the burden of demonstrating that the data subject has consented to the processing of his or her personal data.

153 It is in the light of those criteria and of a detailed examination of all the circumstances of the case that the referring court will have to determine whether the users of the social network Facebook have validly and, in particular, freely given their consent to the processing at issue in the main proceedings.

154 In the light of the foregoing, the answer to Question 6 is that point (a) of the first subparagraph of Article 6(1) and Article 9(2)(a) of the GDPR must be interpreted as meaning that the fact that the operator of an online social network holds a dominant position on the market for online social networks does not, as such, preclude the users of such a network from being able validly to consent, within the meaning of Article 4(11) of that regulation, to the processing of their personal data by that operator. This is nevertheless an important factor in determining whether the consent was in fact validly and, in particular, freely given, which it is for that operator to prove.

Costs

155 Since these proceedings are, for the parties to the main proceedings, a step in the action pending before the referring court, the decision on costs is a matter for that court. Costs incurred in submitting observations to the Court, other than the costs of those parties, are not recoverable.

On those grounds, the Court (Grand Chamber) hereby rules:

1. **Article 51 et seq. 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), as well as Article 4(3) TEU**

   must be interpreted as meaning that, subject to compliance with its duty of sincere cooperation with the supervisory authorities, a competition authority of a Member State can find, in the context of the examination of an abuse of a dominant position by an undertaking within the meaning of Article 102 TFEU, that that undertaking's general

terms of use relating to the processing of personal data and the implementation thereof are not consistent with that regulation, where that finding is necessary to establish the existence of such an abuse.

In view of this duty of sincere cooperation, the national competition authority cannot depart from a decision by the competent national supervisory authority or the competent lead supervisory authority concerning those general terms or similar general terms. Where it has doubts as to the scope of such a decision, where those terms or similar terms are, simultaneously, under examination by those authorities, or where, in the absence of an investigation or decision by those authorities, the competition authority takes the view that the terms in question are not consistent with Regulation 2016/679, it must consult and seek the cooperation of those supervisory authorities in order to dispel its doubts or to determine whether it must wait for them to take a decision before starting its own assessment. In the absence of any objection on their part or of any reply within a reasonable time, the national competition authority may continue its own investigation;

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

must be interpreted as meaning that, where the user of an online social network visits websites or apps to which one or more of the categories referred to in that provision relate and, as the case may be, enters information into them when registering or when placing online orders, the processing of personal data by the operator of that online social network, which entails the collection – by means of integrated interfaces, cookies or similar storage technologies – of data from visits to those sites and apps and of the information entered by the user, the linking of all those data with the user's social network account and the use of those data by that operator, must be regarded as 'processing of special categories of personal data' within the meaning of that provision, which is in principle prohibited, subject to the derogations provided for in Article 9(2), where that data processing allows information falling within one of those categories to be revealed, irrespective of whether that information concerns a user of that network or any other natural person;

3. Article 9(2)(e) of Regulation 2016/679

must be interpreted as meaning that, where the user of an online social network visits websites or apps to which one or more of the categories set out in Article 9(1) of that regulation relate, the user does not manifestly make public, within the meaning of the first of those provisions, the data relating to those visits collected by the operator of that online social network via cookies or similar storage technologies;

Where he or she enters information into such websites or apps or where he or she clicks or taps on buttons integrated into those sites and apps, such as the 'Like' or 'Share' buttons or buttons enabling the user to identify himself or herself on those sites or apps using login credentials linked to his or her social network user account, his or her telephone number or email address, that user manifestly makes public, within the meaning of Article 9(2)(e), the data thus entered or resulting from the clicking or tapping on those buttons only in the circumstance where he or she has explicitly made the choice beforehand, as the case may be on the basis of individual settings selected

with full knowledge of the facts, to make the data relating to him or her publicly accessible to an unlimited number of persons;

4. Point (b) of the first subparagraph of Article 6(1) of Regulation 2016/679

must be interpreted as meaning that the processing of personal data by the operator of an online social network, which entails the collection of data of the users of such a network from other services of the group to which that operator belongs or from visits by those users to third-party websites or apps, the linking of those data with the social network account of those users and the use of those data, can be regarded as necessary for the performance of a contract to which the data subjects are party, within the meaning of that provision, only on condition that the processing is objectively indispensable for a purpose that is integral to the contractual obligation intended for those users, such that the main subject matter of the contract cannot be achieved if that processing does not occur;

5. Point (f) of the first subparagraph of Article 6(1) of Regulation 2016/679

must be interpreted as meaning that the processing of personal data by the operator of an online social network, which entails the collection of data of the users of such a network from other services of the group to which that operator belongs or from visits by those users to third-party websites or apps, the linking of those data with the social network account of those users and the use of those data, can be regarded as necessary for the purposes of the legitimate interests pursued by the controller or by a third party, within the meaning of that provision, only on condition that the operator has informed the users from whom the data have been collected of a legitimate interest that is pursued by the data processing, that such processing is carried out only in so far as is strictly necessary for the purposes of that legitimate interest and that it is apparent from a balancing of the opposing interests, having regard to all the relevant circumstances, that the interests or fundamental freedoms and rights of those users do not override that legitimate interest of the controller or of a third party;

6. Point (c) of the first subparagraph of Article 6(1) of Regulation 2016/679

must be interpreted as meaning that the processing of personal data by the operator of an online social network, which entails the collection of data of the users of such a network from other services of the group to which that operator belongs or from visits by those users to third-party websites or apps, the linking of those data with the social network account of those users and the use of those data, is justified, under that provision, where it is actually necessary for compliance with a legal obligation to which the controller is subject, pursuant to a provision of EU law or the law of the Member State concerned, where that legal basis meets an objective of public interest and is proportionate to the legitimate aim pursued and where that processing is carried out only in so far as is strictly necessary;

7. Points (d) and (e) of the first subparagraph of Article 6(1) of Regulation 2016/679

must be interpreted as meaning that the processing of personal data by the operator of an online social network, which entails the collection of data of the users of such a network from other services of the group to which that operator belongs or from visits

by those users to third-party websites or apps, the linking of those data with the social network account of those users and the use of those data, cannot, in principle and subject to verification by the referring court, be regarded as necessary in order to protect the vital interests of the data subject or of another natural person, within the meaning of point (d), or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, within the meaning of point (e);

8. Point (a) of the first subparagraph of Article 6(1) and Article 9(2)(a) of Regulation 2016/679

must be interpreted as meaning that the fact that the operator of an online social network holds a dominant position on the market for online social networks does not, as such, preclude the users of such a network from being able validly to consent, within the meaning of Article 4(11) of that regulation, to the processing of their personal data by that operator. This is nevertheless an important factor in determining whether the consent was in fact validly and, in particular, freely given, which it is for that operator to prove.

[Signatures]