Case C-252/21

Request for a preliminary ruling

Date lodged:

22 April 2021

Referring court:

Oberlandesgericht Düsseldorf (Germany)

Date of the decision to refer:

24 March 2021

Applicants:

Facebook Inc.

Facebook Ireland Ltd.

Facebook Deutschland GmbH

Defendant:

Bundeskartellamt

OBERLANDESGERICHT DÜSSELDORF (HIGHER REGIONAL COURT, DÜSSELDORF)

ORDER

[…]

At the hearing in the administrative proceedings in the cartel case

1. **Facebook Inc.**, […] USA,

2. **Facebook Ireland Ltd.**, […] Ireland,

3. **Facebook Deutschland GmbH**, […] Hamburg,

Applicants,

[…]

v

Bundeskartellamt (Federal Cartel Office), […] Bonn,

Defendant,

Other parties:

Verbraucherzentrale Bundesverband e. V., […] Berlin,

Joined party,

[…] **[Or. 2]**

on 24 March 2021, the First Cartel Chamber of the Higher Regional Court, Düsseldorf

issued the following

[…]

o r d e r:

I.

The proceedings are stayed.

II.

The following questions on the interpretation 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, 'the GDPR') and Article 4(3) TEU are referred to the Court of Justice of the European Union 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 German 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 **[Or. 3]** the meaning of Article 56(1) of the GDPR, is located is investigating the undertaking's contractual terms relating to data processing?

If the answer to Question 1 is yes:

2.

a) If an internet user merely visits websites or apps to which the criteria of Article 9(1) of the GDPR relate, such as flirting apps, gay dating sites, political party websites or health-related websites, or also enters information into them, for example when registering or when placing orders, and another undertaking, such as *Facebook Ireland*, uses interfaces integrated into those websites and apps, such as '*Facebook* Business Tools', or cookies or similar storage technologies placed on the internet user's computer or mobile device, to collect data about those visits to the websites and apps and the information entered by the user, and links those data with the data from the user's *Facebook.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 *Facebook Ireland* (social plugins such as 'Like', 'Share' or '*Facebook* Login' or 'Account Kit') constitute manifestly making the data about the visits themselves and/or the information entered by the user public within the meaning of Article 9(2)(e) of the GDPR?

3.

Can an undertaking, such as *Facebook Ireland*, which operates a digital social network funded by advertising and offers personalised content and advertising, network security, product improvement and continuous, seamless use of all of its group products in its terms of service, justify collecting data for these purposes from other group services and [**Or. 4]** 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 with the user;

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

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

– research and innovation 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 links data from other group services and from third-party websites and apps with the user's *Facebook.com* account via integrated interfaces such as *Facebook* Business Tools or via cookies or similar storage technologies placed on the internet user's computer or mobile device and uses those data?

5.

In those circumstances, can collecting data from other group services and from third-party websites and apps via integrated interfaces such as *Facebook* Business Tools, or via cookies or similar storage technologies placed on the internet user's computer or mobile device, linking those data with the user's *Facebook.com* account and using them, or using data already **[Or. 5]** 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 *Facebook Ireland*?

If the answer to Question 1 is no:

7.

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

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

If the answer to Question 7 is yes, Questions 3 to 5 must be answered in relation to data from the use of the group's *Instagram* service. **[Or. 6]**

Grounds

I.

The second applicant ('*Facebook Ireland*') operates the digital social network *Facebook.com* in Europe, a network that is free of charge for private users. The first applicant is its US parent company. The third applicant is a German sister company of *Facebook Ireland* that provides it with advertising, communication and public relations support (jointly also '*Facebook*').

Private users can set up a personal *Facebook* page on *Facebook.com* which they can use to communicate with third parties. They can create their own posts in the 'Newsfeed' on their *Facebook* page and share them with their *Facebook* friends or publicly on the network as they wish; they can also receive communications in their Newsfeed from their *Facebook* friends or other content providers and undertakings represented on *Facebook.com* to which they have subscribed. In addition, they can show content from third-party websites and apps in their

Newsfeed, and that of their *Facebook* friends, by clicking or tapping on the social plugins (particularly 'Like' or 'Share'). With '*Facebook* Login' and 'Account Kit', users can log in or create a profile on third-party websites and apps using only their *Facebook* registration data.

Facebook offers undertakings the opportunity to integrate the social plugin buttons (particularly Like and Share) and *Facebook* Login and Account Kit into their websites and apps with predefined interfaces called '*Facebook* Business Tools'. These interfaces transmit user data to *Facebook.com*, regardless of whether or not the website and app users actually click or tap on the buttons.

Facebook.com is funded by online advertising, which is tailored to its individual users and aims to show them advertisements that might interest them on the basis of their consumer behaviour, interests, purchasing power and personal situation. Advertisers can use the 'Ads Manager' to specify their target audience and have advertisements displayed to users; they can also transmit their **[Or. 7]** customer lists to *Facebook* in encrypted form and optimise their advertising by comparing their data with data from the social network. *Facebook* offers other analysis and measurement tools (advertising reports and '*Facebook* Analytics'), also under *Facebook* Business Tools, which advertisers can use to measure the success of their advertising, analyse their own online services and obtain aggregated statistics in respect of their target audience. This is also done by integrating interfaces ('*Facebook* pixel' or 'SDK' (software development kit)), which record user behaviour on third-party websites and apps, regardless of whether the user takes any corresponding action.

The *Facebook* group provides other services beyond the social network, including *Instagram*, the free service funded by advertising for 'sharing' photos and short video clips, which is also operated in Europe by *Facebook Ireland*; *WhatsApp*, the free service for sending and receiving a variety of media such as text messages, images, videos, contacts, documents, locations, voice messages and calls, which is not funded by advertising and is operated in Europe by *WhatsApp* Ireland Ltd; and *Oculus*, which sells virtual reality glasses and software and is operated in Europe by another subsidiary, *Facebook Technologies Ireland Ltd*. Until 13 March 2020, *Facebook* also provided the *Masquerade* service for the editing and 'sharing' of photos.

By clicking on the 'Sign up' button on *Facebook.com*, private users in Europe enter into a contract for the use of the service and agree to *Facebook Ireland*'s terms of service. Under those terms, *Facebook Ireland* processes personal data; users are referred in particular to *Facebook Ireland's* data and cookies policies for further information. According to those policies, *Facebook Ireland* collects user- and device-related data about user activities on and off the social network and associates the data with the user's *Facebook.com* account. User activities off the social network are visits to third-party websites and apps connected to *Facebook.com* by programming interfaces (*Facebook* Business Tools), and the use of the other *Facebook* services *Instagram*, *WhatsApp* and *Oculus*, in respect of

which data are processed ‘across the other *Facebook* companies and products’. **[Or. 8]**

By decision of 6 February 2019, the Federal Cartel Office prohibited the applicants and their associated undertakings as referred to in Paragraph 36(2) of the Gesetz gegen Wettbewerbsbeschränkungen (Law against restrictions on competition, ‘the GWB’) from processing data as provided for in the terms of service, under Paragraphs 19(1) and 32 of the GWB and imposed measures to stop them from doing so. The prohibition covers the application of terms of service, including as further specified in data and cookies policies, according to which the use of the *Facebook.com* network by private users resident in Germany is dependent on *Facebook Ireland* being able to collect user- and device-related data from the use of *Instagram*, *WhatsApp*, *Oculus* and *Masquerade* and from visits to third-party websites or apps via *Facebook* Business Tools without the user’s consent, to link those data with the user’s *Facebook.com* data and to use them (point 1 of the operative part of the decision). Furthermore, the Federal Cartel Office prohibited the applicants and their associated undertakings as referred to in Paragraph 36(2) of the GWB from implementing those terms with the actual data processing operations performed by *Facebook Ireland* on the basis of the data and cookies policies (point 2 of the operative part of the decision) and obliged them to amend the terms of service and their implementation so as to make it absolutely clear that user- and device-related data from the use of *Instagram*, *WhatsApp*, *Oculus* and *Masquerade*, and from *Facebook* Business Tools, will not, or not without the user’s consent, be collected, linked to the user’s *Facebook.com* account and used (point 3 of the operative part of the decision). Finally, the Office made clear, in point 4 of the operative part of its decision, that no consent on the part of the user exists if the provision of *Facebook.com* is made conditional on consent being given.

On 11 February 2019, the applicants lodged an appeal against the decision of the Federal Cartel Office with the Higher Regional Court, Düsseldorf within the time limit and in the manner prescribed.

Facebook Ireland introduced new and essentially identical terms of service on 31 July 2019 on the initiative of the European Commission and the national consumer protection organisations of the Member States; point 2 of those terms states expressly that the user agrees to be shown advertisements instead of paying to use *Facebook* products. Since 28 January 2020, *Facebook* has provided the **[Or. 9]** ‘off-Facebook activity’ (‘OFA’) tool worldwide. *Facebook* users can use the tool to view a summary of the information obtained by *Facebook* about their activities on other websites and apps and disconnect these data about past and future activities from their *Facebook.com* account if they so wish.

II.

The provisions of German law relevant to the assessment of the appeal proceedings are worded as follows:

Paragraph 19(1) of the GWB, in the version in force until 18 January 2021:

(1) The abusive exploitation of a dominant position by one or more undertakings is prohibited.

Paragraph 19(1) of the GWB, in the version in force since 19 January 2021:

(1) The abuse of a dominant position by one or more undertakings is prohibited.

Paragraph 32(1) of the GWB:

(1) 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 of the Treaty on the Functioning of the European Union.

III.

The success of *Facebook Ireland*'s appeal – which, following the withdrawal of the *Masquerade* service and the Federal Cartel Office's statement that it no longer derives any rights from the contested decision in that regard, is directed only against the remainder of the decision – depends on the answers to the preliminary questions raised in the operative part of the decision. Consequently, before deciding on the substance of the appeal, the proceedings must be stayed and a preliminary ruling obtained from the Court of Justice of the European Union under Article 267 TFEU.

1. First of all, the Federal Cartel Office based its order under Paragraphs 19(1) and 32 of the GWB solely on the ground that the processing of data from the group services provided separately from *Facebook.com*, and from *Facebook* Business Tools, as set out in the terms of service and implemented, constitutes the abusive exploitation of a dominant position on the market for social networks for private users in Germany, in the form of an abuse of terms under the general provision that is Paragraph 19(1) of the GWB, **[Or. 10]** because such processing is a result of market power and therefore breaches the GDPR, since it lacks sufficient justification under Article 6(1) and Article 9(2) of the GDPR. Furthermore, the abuse creates an impediment to the detriment of competitors on the social networks market and on third markets. An additional assessment of the balance of interests with regard to competition is superfluous and would in any case lead to the same result as the assessment with regard to data protection interests. Since the concept of protection developed in the German case-law in relation to the general provision of Article 19(1) of the GWB has as yet no counterpart in European case-law or in practice, the decision is based solely on Paragraph 19(1) of the GWB, which is stricter in that regard than Article 102 TFEU.

While the order of the Federal Cartel Office must be annulled in so far as it is directed against the first and third applicants and all of their associated undertakings in accordance with Paragraph 36(2) of the GWB, since the latter

were not involved in the administrative proceedings and were not given a hearing, and since the order does not include any discretionary consideration of the grounds for involving the first and third applicants, and the discretion required under Paragraph 32(1) of the GWB may not be exercised for the first time in the appeal proceedings, the Chamber will proceed, with respect to *Facebook Ireland*, on the basis of the following considerations:

a) *Facebook Ireland* is dominant on the relevant market for the provision of digital social networks for private users which, for the purposes of monitoring abuse, can be defined as national since, according to the uncontested findings of the Federal Cartel Office, its network effects are confined primarily to Germany; it is therefore *Facebook Ireland* that is addressed by Paragraph 19(1) of the GWB.

b) A breach of the GDPR by *Facebook Ireland*'s terms of service and their implementation may constitute an abuse of terms detrimental to private users under the general provision of Paragraph 19(1) of the GWB, since that paragraph, like Article 102 TFEU, protects consumers not only indirectly from distortion of the rules of competition through market power, but also directly from exploitation by a dominant undertaking, while having no impact on the structure of competition (see judgment of 15 March 2007, *British Airways*, C-95/04, paragraph 106, available from JURIS; Bundesgerichtshof (Federal Court of Justice; 'the BGH'), **[Or. 11]** judgment of 7 December 2010, *Entega II*, KZR 5/10, paragraph 55, available from JURIS). This harms competition by infringing the right of users, protected by the GDPR, to control their personal data. A comparative market analysis and determination of a substantial deviation from the comparative conditions, such as would be carried out to establish an abusively excessive price within the meaning of Paragraph 19(2)(2) of the GWB, are not undertaken if the alleged abusive conduct is a relevant breach of the law (see BGH, judgment of 6 November 2013, *VBL-Gegenwert I*, KZR 58/11, paragraph 66, available from JURIS). Nor is there any scope for the assessment of the balance of interests also required under the general provision of Paragraph 19(1) of the GWB (see BGH, judgment of 7 June 2016, *Pechstein* v *International Skating Union*, KZR 6/15 [ECLI:DE:BGH:2016:070616UKZR6.15.0], paragraph 48, available from JURIS). The causal link between abuse and market power required under Paragraph 19(1) of the GWB and the first sentence of Article 102 TFEU (see judgment of 14 November 1996, *Tetra Pak*, C-333/94 [EU:C:1996:436], paragraph 27, available from JURIS; judgment of 14 February 1978, *United Brands*, C-27/76, [EU:C:1978:22], paragraph 248/257, available from JURIS; BGH, decision of 23 June 2020, *Facebook*, KVR 69/19 [ECLI:DE:BGH:2020:230620BKVR69.19.0] paragraph 73, available from JURIS) exists, both in terms of behavioural causality in the broader sense, since, if competition were functioning effectively it would not be advisable for *Facebook Ireland* to insist on conditions for data processing operations that are not permitted under the GDPR, and also in terms of the causality of results, since, although the GDPR can also be breached by undertakings that are not in a dominant position, users have scarcely any alternative when it is breached by an undertaking with a

virtual monopoly, such as *Facebook Ireland* (see also judgments of 5 October 1988, *Alsatel*, C-247/86 [EU:C:1988:469], available from JURIS and of 27 March 1974, *BRT and SABAM*, C-127/73 [EU:C:1974:25], available from JURIS, in which the Court of Justice of the European Union does not question the connection between abuse and market power). If abuse is demonstrated, *Facebook Ireland* cannot rely on a group privilege under Paragraph 36(2) of the GWB (see judgment of 24 October 1996, *Viho*, C-73/95 P, paragraph 17, available from JURIS; BGH, decision of 6 November 2012, *Gasversorgung Ahrensburg*, KVR 54/11, paragraphs 19 and 22, available from JURIS; judgment of 23 June 2009, *Entega I*, KZR 21/08, paragraph 16, available from JURIS).

c) The order is unlawful on procedural grounds since, contrary to the second sentence of Article 3(1) of Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty **[Or. 12]** (the Implementing Regulation), the Federal Cartel Office did not examine the first paragraph of Article 102 TFEU, although *Facebook Ireland*'s dominant position in Germany corresponds to a dominant position on a substantial part of the internal market within the meaning of the first paragraph of Article 102 TFEU (see judgment of 23 April 1991, *Höfner-Elsner*, C-41/90, paragraph 28, available from JURIS; judgment of 9 November 1983, *Michelin*, C-322/81 [EU:C:1983:313], paragraph 28, available from JURIS) and in view of the finding that the breach of the GDPR entails '*actual and potential impediments to the detriment of competitors*' (paragraph 885 of the Office's decision), the requirement under the first paragraph of Article 102 TFEU that trade between Member States be affected should also have been assumed to apply (see judgment of 23 April 1991, *Höfner-Elsner*, C-41/90, paragraph 32, available from JURIS; judgment of 9 November 1983, *Michelin*, C-322/81 [EU:C:1983:313], paragraph 104, available from JURIS). […] [amplification] Since […] it must be assumed that Paragraph 19(1) of the GWB and the first paragraph of Article 102 TFEU are consistent with each other (see BGH, judgment of 8 April 2014 *VBL-Versicherungspflicht*, KZR 53/12, paragraph 46, available from JURIS; judgment of 6 November 2013, *VBL-Gegenwert I*, KZR 58/11, paragraph 51, available from JURIS), the procedural error is, however, irrelevant if the order is lawful under Paragraph 19(1) of the GWB and, if it is unlawful under Paragraph 19(1) of the GWB, does not lead to any further significant contraventions.

d) That being the case, can the Federal Cartel Office determine whether *Facebook Ireland*'s terms of service and their implementation breach the GDPR, and impose measures to remedy that breach? **[Or. 13]**

aa) Question 1. a) of the request for a preliminary ruling seeks to clarify whether it is compatible with the competence, cooperation and consistency provisions of Article 51 et seq., and in particular Article 56(1), of the GDPR and the provisions in relation to powers of Articles 57 and 58 of the GDPR that, for the purposes of monitoring abuses of competition law, the Federal Cartel Office should determine that *Facebook Ireland*'s terms of service and their implementation breach the

GDPR and order measures to remedy that breach. The Federal Cartel Office is not a supervisory authority within the meaning of the GDPR, and the lead supervisory authority under Article 56(1) of the GDPR is the Irish supervisory authority, since *Facebook Ireland* is *Facebook's* main establishment in Europe, operates the social network in Europe, uses standard terms of service in all Member States of the European Union and is the controller for the processing of personal data for the entire territory of the European Union within the meaning of Article 4(7) of the GDPR.

In so far as the possibility of civil-law protection under Article 82 of the GDPR and, in particular, other penalties under Article 84(1) of the GDPR must also be taken into consideration in that context, the Chamber notes that Paragraphs 19 and 32 of the GWB are not among the provisions notified by Germany to the European Commission as required by Article 84(2) of the GDPR (paragraph 201 of the statement of grounds of appeal).

bb) If it is compatible with the competence rules of the GDPR that, for the purposes of monitoring abuses of competition law, the Federal Cartel Office determine that the terms of service and their implementation breach the GDPR and that it impose a penalty for that breach, Question 1. b) of the request seeks to clarify whether that is compatible with the principle of sincere cooperation enshrined in Article 4(3) TEU, if the lead supervisory authority under Article 56(1) of the GDPR is already examining that infringement, as in the case here of the Irish supervisory authority, which, according to *Facebook's* uncontested submission (paragraphs 188 and 217 of the statement of grounds of appeal), was already cooperating with other relevant supervisory authorities in the Union on an ongoing examination of a possible infringement of the GDPR by *Facebook Ireland* at the time of the Office's decision.

e) If the Federal Cartel Office can determine, for the purposes of monitoring abuses of competition law, that *Facebook Ireland*'s terms of service and their implementation breach the GDPR and order measures to remedy that breach, **[Or. 14]** do the terms of service (as further set out in the data and cookies policies) in relation to the processing of data from other group services and *Facebook* Business Tools (together also: 'off-*Facebook* data') and their implementation breach the GDPR, and can the Federal Cartel Office prohibit the terms of service and their implementation and order that the data may not be processed or may be processed only with the separate consent of users, to which the use of *Facebook.com* may not be made subject?

aa) The Federal Cartel Office rightly assumes that off-Facebook data are personal data within the meaning of Article 4(1) of the GDPR (see judgment of 19 October 2016, *Breyer*, C-582/14, paragraph 49, available from JURIS; judgment of 24 November 2011, *Scarlet*, C-70/10, paragraph 51, available from JURIS; BGH, reference to the Court of Justice of the European Union of 5 October 2017, *Cookie-Einwilligung I*, I ZR 7/16, [ECLI:DE:BGH:2017:051017BIZR7.16.0], paragraph 23, available from JURIS),

that the data are used to personalise the network, that the advertising constitutes 'profiling' within the meaning of Article 4(4) of the GDPR and that *Facebook Ireland* is the data processing controller within the meaning of Article 4(7) of the GDPR (see judgment of 29 July 2019, *Fashion ID*, C-40/17 [EU:C:2019:629], paragraph 84, available from JURIS).

bb) The Federal Cartel Office rightly assumes that – even in the light of point 2 of the new terms of service of 31 July 2019 – users do not consent to the processing of off-Facebook data in accordance with Article 6(1)(a) and Article 9(2)(a) of the GDPR by clicking on the 'Sign up' button (see judgment of 1 October 2019, *Planet49*, C-673/17 [EU:C:2019:801], paragraph 58 et seq.), and that the consent that *Facebook Ireland* obtains from users to the use of data from *Facebook* Business Tools to show personalised advertisements relates only to the *use* of the data for that purpose and not to the collection and linking of those data with the user's *Facebook.com* account in general. The Federal Cartel Office also rightly assumes that the possibility of blocking the placement of cookies on the user's device or web browser, or deleting them, the possibility of resetting advertising IDs in a mobile device's operating system and the OFA function introduced at the end of January 2020 do not fulfil the requirements for consent under Article 6(1)(a) and Article 9(2)(a) of the GDPR. **[Or. 15]**

cc) Since the processing of off-Facebook data, as provided for in the terms of service – including within the group – is lawful if it is justified by at least one of the grounds under Article 6(1)(a) to (f) of the GDPR, and the Court of Justice has already ruled that the identical provision of Article 7 of the preceding Data Protection Directive (Directive 95/46/EC) provides an exhaustive and conclusive list of cases in which the processing of personal data may be considered lawful and that Member States may neither introduce new principles for the lawful processing of personal data alongside this Article, nor impose additional conditions which would alter the scope of any of the principles provided for therein (see judgment of 29 July 2019, *Fashion Id*, C-40/17 [EU:C:2019:629], paragraph 55, available from JURIS; judgment of 19 October 2016, *Breyer*, C-582/14, paragraph 57, available from JURIS; judgment of 24 November 2011, *ASNEF and FECEMD*, C-468/10 and C-469/10, paragraphs 30 and 32, available from JURIS), is the processing of off-Facebook data as provided for in the terms of service only ever justifiable if consent is obtained? For only then could the Federal Cartel Office order that, for data protection reasons, such data may not be processed or may be processed only if consent is given .

(1) According to point 1 ('The services we provide') of its current terms of service (Annex Bf 9), the following contractual services relevant to this case are provided by *Facebook Ireland* as part of its social network: 1. personalised content, 2. personalised advertising, 3. user and network security, 4. product improvement and 5. consistent and seamless use of *Facebook*'s products.

Facebook Ireland collects the user- and device-related data listed in its Data Policy (Annex Bf 10) under the heading 'What kinds of information do we

collect?' from the use of its group services and from *Facebook* Business Tools; it links these data with the data collected and stored while *Facebook.com* is being used and, according to the section headed 'How do we use this information?', uses it to provide, personalise and improve its products, to provide measurement, analytics and other business services, to promote safety, integrity and security, to communicate with users and to research and innovate for social good; according to the **[Or. 16]** section headed 'How do the *Facebook* Companies work together?', it also uses it 'across the *Facebook* Companies.'

According to its Cookies Policy (Annex Bf 11), *Facebook Ireland* sets cookies or uses other storage technologies when users use the group's services and visit third-party websites and apps that have integrated *Facebook* Business Tools, and collects user- and device-related data without any further action by the user; it uses those data to provide its services and for security, advertising and analytics purposes.

The kinds of data collected and used are detailed in the Data Policy under the heading 'What kinds of information do we collect?' (Annex Bf 10) and in point 2(a) to (d) of the operative part of the Office's decision.

Facebook Ireland relies in the section of its Data Policy headed 'What is our legal basis for processing data?'(Annex Bf 10) on all of the grounds under Article 6(1) of the GDPR. Under the heading 'Learn more about these legal bases' (Annex Bf 12), *Facebook Ireland* relies on *consent* within the meaning of Article 6(1)(a) of the GDPR 1. for processing data with special protections that are provided by users in their *Facebook.com* profile, for sharing with persons they choose and to personalise content, 2. for using facial recognition technology, 3. for using data that advertisers and other partners provide about users' activity off *Facebook* Company Products to personalise advertising, 4. for sharing data that personally identifies users with advertisers, 5. for collecting information that users allow *Facebook* to receive through the device-based settings they enable (GPS location, camera, photos). *Facebook Ireland* obtains separate consent from users to process their data for these purposes or offers them the chance to object (in the case of facial recognition).

In the document referred to (Annex Bf 12), *Facebook Ireland* relies on the justification of necessity for the *performance of the contract* within the meaning of Article 6(1)(b) of the GDPR 1. to provide, personalise and improve its products, 2. to promote safety, integrity and security, 3. to **[Or. 17]** transfer and transmit data outside the EEA, 4. to communicate with users, 5. to provide consistent and seamless experiences across all Facebook Company Products.

Facebook Ireland relies on the justification of legitimate interest under Article 6(1)(f) of the GDPR 1. vis-à-vis minors, 2. for providing measurement, analytics and other business services, 3. for providing marketing communications, 4. to research and innovate for social good, 5. to share information with others including law enforcement agencies and to respond to legal requests.

Facebook Ireland further relies on the justification of compliance with a legal obligation (Article 6(1)(c) of the GDPR), the protection of vital interests (Article 6(1)(d) of the GDPR) and *tasks carried out* in the public interest (Article 6(1)(f) of the GDPR) (see Annex Bf 12 for detailed information).

(2) Consent would be required if and in so far as the collection and linking of data with the *Facebook.com* account and the use of off-*Facebook* data involved the processing of special categories of personal data within the meaning of Article 9(1) of the GDPR and no permission other than consent under Article 9(2)(a) of the GDPR could be given.

(a) Question 2. a) of the request seeks to clarify whether, as the Federal Cartel Office believes (paragraph 584 et seq. of its decision), the use of *Facebook* Business Tools, cookies and other storage technologies to collect data about visits to third-party websites and apps and/or the linking of those data with the user's *Facebook.com* account and/or the use of those data involves the processing of sensitive data for the purpose of Article 9(1) of the GDPR if those websites and apps are covered by the criteria of that provision, such as flirting apps, gay dating sites, political party websites and health-related websites (paragraph 587 of the Office's decision).

In that regard, is it sufficient for the data to relate to visits to the website or app alone, or must the user also have entered certain information, for example by registering or placing orders, and how should the terms 'data revealing …' within the meaning of the first data category and 'data' within the meaning of the second data category of Article 9(1) of the GDPR be interpreted **[Or. 18]**? The formulation of the first data category of Article 9(1) of the GDPR ('data revealing …') might support the argument that the processing of the 'source data', in other words visits to a website or the information entered by the user, is prohibited, and it is therefore a matter of determining when this 'reveals' sensitive data. Since, by contrast, the second data category of Article 9(1) of the GDPR appears to prohibit only the processing of sensitive data, can visits to relevant websites or the entry of information by the user in themselves be regarded as sensitive data, even though the distinction is further qualified, by the legal definition in Article 4(15) of the GDPR, for example, which states that data concerning health can also be data which '*reveal*' information about a person's health status. The question also seeks to clarify whether the purpose for which the data are used – in this case, for example, to personalise the social network and advertising, for network security, to improve services, to provide measurement and analytics services for advertising partners, to research for social good, to respond to legal requests and comply with legal obligations, to protect the vital interests of users and third parties and to carry out tasks in the public interest – is also relevant to the assessment.

(b) Question 2.b) of the request seeks to clarify, with regard to sensitive data for the purpose of Article 9(1) of the GDPR, whether the user has manifestly made those data public by visiting the website or app and/or entering information and/or

clicking or tapping on the buttons provided by *Facebook Ireland* and integrated into the websites or apps, such as the social plugins (Like, Share) or *Facebook* Login or Account Kit (Article 9(2)(e) of the GDPR), since he or she would then have lost the specific protection of Article 9(1) of the GDPR without any need for consent under Article 9(2)(a) of the GDPR. In view of the sector in which *Facebook* operates, the other grounds for permission under Article 9(2) of the GDPR do not apply, or at least are not claimed by *Facebook* or referred to in its terms of service.

(3) Where *Facebook Ireland* also uses cookies and similar storage technologies to collect data from users' devices when they use the other group services and visit websites and apps in which *Facebook* Business Tools have been integrated, Article 5(3) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the **[Or. 19]** electronic communications sector (Directive on privacy and electronic communications) also applies. Since, as the Federal Court of Justice ruled, the GDPR does not affect the application of this provision, the first sentence of Paragraph 15(3) of the Telemediengesetz (Law on telemedia), which implements Directive 2002/58/EC, still applies and must be interpreted in accordance with the directive as meaning that the user's consent is required for the use of cookies to produce user profiles for the purposes of advertising or market research (see BGH, judgment of 28 May 2020, *Cookie-Einwilligung II*, I ZR 7/16, paragraph 47 et seq., available from JURIS; see also judgment of 1 October 2019, *Planet49*, C-673/17 [ECLI: EU:C:2019:801], paragraph 38 et seq., available from JURIS; judgment of 29 July 2019, *Fashion ID*, C-40/17 [EU:C:2019:629], paragraph 88 et seq., available from JURIS). However, the question whether the consent obtained for the use of partner data to show personalised advertisements is adequate for this is of no further relevance here, since the Federal Cartel Office based its finding that *Facebook* had breached the prohibition on the competition-law abuse laid down in Paragraph 19(1) of the GWB only on a breach, by *Facebook*'s data processing operations, of the GDPR, and not on a breach of the first sentence of Paragraph 15(3) of the Law on telemedia.

(4) If and in so far as consent is not required under Article 9(2)(a) of the GDPR – in other words, for the processing of data from the other group services, with regard to which the Federal Cartel Office did not find any evidence of the processing of potentially sensitive data for the purpose of Article 9(1) of the GDPR, and the processing of non-sensitive data from *Facebook* Business Tools or data which have manifestly been made public by the user – can *Facebook Ireland* rely on other justifications under Article 6(1) of the GDPR for the processing of off-*Facebook* data, and, if so, to what extent? The Chamber assumes that, where data are manifestly made public within the meaning of Article 9(2)(e) of the GDPR, only the prohibition under paragraph 1 of that provision ceases to apply, and not the requirement for a justification under Article 6(1) of the GDPR (see the fifth sentence of recital 51).

(a) Question 3 of the request seeks to clarify whether, when *Facebook Ireland*, as referred to above, offers 1. personalised content, 2. personalised advertising, 3. user and network security, 4. product improvement and 5. consistent and seamless use of *Facebook* companies' products as contractual services, it can rely on the justification of necessity for the performance of a contract under Article 6(1)(b) of the GDPR, or on the **[Or. 20]** justification of legitimate interests under Article 6(1)(f) of the GDPR, if it collects off-*Facebook* data for these purposes, links those data with the user's *Facebook.com* account and uses them.

The Chamber believes that there is much in the case-law of the Court of Justice with regard to necessity (see judgment of 4 May 2017, *Rigas satiksme*, C-13/16, paragraph 30, available from JURIS) and the factors taken into consideration by the European Data Protection Board in its Guidelines 2/19 (paragraphs 2, 26 et seq., 48 et seq. and 57, Annex Bf 42B) to support the view that the processing of data for the purposes of personalised advertising, which does not require cookies, of user and network security and of product improvement, can certainly be regarded as being in the legitimate interests of the undertaking; the case-law also appears to suggest that the processing of data to personalise content and, in some cases, also to ensure the consistent and seamless use of *Facebook* companies' products can be regarded as necessary for the performance of *Facebook Ireland*'s contracts.

Accordingly, *Facebook Ireland* could have a legitimate interest, for example, in processing *WhatsApp* data for user and network security because, as it states in the section of the Data Policy headed 'How do the *Facebook* Companies work together?' (Annex Bf 10), it uses information from *WhatsApp* accounts sending spam to take action against those accounts on *Facebook.com*, although this is otherwise neither necessary for the performance of the contract nor likely to be justified by other legitimate interests, since *Facebook Ireland* does not use *WhatsApp* data for product and personalisation purposes on *Facebook.com* (paragraph 746 of the Office's decision).

The processing of *Instagram* data for the personalisation of content and the seamless use of *Facebook* products (so that users can be shown people or content on *Facebook.com* that might also be of interest to them there) could be necessary for the performance of the contract or at least be in the legitimate interests of *Facebook Ireland*. *Facebook Ireland* could also have a legitimate interest in processing these data for the purposes of personalised advertising, network security and product improvement. In particular, by its own account, *Facebook Ireland* uses *Instagram* data from accounts that behave inappropriately or are clearly involved in unlawful activity to ensure the security of *Facebook* users **[Or. 21]** (paragraph 465 of the statement of grounds of appeal). In principle, the same could apply to the processing of *Oculus* data, although there are not yet enough findings on the specific purposes for which those data are used on *Facebook.com*.

The processing of data from *Facebook* Business Tools, particularly the social plugins Like and Share, and from *Facebook* Login and Account Kit could be

necessary for the performance of the contract, or at least in *Facebook Ireland*'s legitimate interests, provided it is intended for the personalisation of content and the seamless use of *Facebook* products. This should require the user to click or tap on the relevant button and should be limited to the data processing operations required in a particular case. Irrespective of whether or not the user has clicked or tapped on the buttons, the collection of data and the linking of those data with the *Facebook.com* account could be in the legitimate interests of *Facebook Ireland* if the user has consented to the use of the data for the display of personalised advertisements. Data processing for the purposes of network security or product improvement could also be legitimate interests of *Facebook Ireland*. By its own account, *Facebook* uses data from social plugins to identify rapidly, from the many website visits, attempts by bots to open and operate *Facebook* accounts (paragraph 465 of the statement of grounds of appeal).

(b) Question 4 of the request seeks to clarify whether

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

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

– the provision of marketing communications to the user to enable *Facebook Ireland* 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; **[Or. 22]**

may constitute legitimate interests within the meaning of Article 6(1)(f) of the GDPR with regard to the collection of off-Facebook data for these purposes, the linking of those data with the user's *Facebook.com* account and their use.

In particular, can *Facebook Ireland* rely on the justification of legitimate interests under Article 6(1)(f) of the GDPR for the processing of data obtained from other group services and from *Facebook* Business Tools in the case of minors who have not yet reached the age of 16 required in order to give independent consent under Article 6(1)(a) of the GDPR (Article 8(1) of the GDPR) – no provision having been made in Germany for a lower age pursuant to the third sentence of Article 8(1) of the GDPR – who do not have parental consent and who the German commentaries (apparently unanimously) believe to be unable to enter independently into a valid contract within the meaning of Article 6(1)(b) of the

GDPR with a social network for the use of its services, since it does not involve only a legal benefit on account of the processing of the data (Paragraph 107 of the Bürgerliches Gesetzbuch (German Civil Code, 'the BGB'); see Klumpp in: Staudinger, *BGB*, Revised edition 2017, '§ 107', paragraph 30; Spickhoff in: *MüKoBGB*, 8th edition 2018, '§ 107', paragraph 82; Mansel in: Jauernig, *BGB*, 18th edition 2021, '§ 107', paragraph 3)?

It also appears doubtful whether the processing of off-*Facebook* data can be justified by the interests of 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 use of data from *Facebook* Business Tools to provide measurement, analytics and other business services to enable advertisers, developers and other partners to evaluate and improve their services could, by contrast, be in the legitimate interests of *Facebook Ireland* (and its partners) if users have consented to the use of partner data for the display of personalised advertisements. If, and in so far as, the processing of data from the other group services and/or *Facebook* Business Tools is justified for the purposes of product improvement, this could also apply to its use for the provision of marketing communications to the user to enable *Facebook* to improve its products and engage in direct marketing. **[Or. 23]**

Similarly, collecting those data, linking them with the *Facebook.com* account and using them, or using off-*Facebook* data already collected and linked by other lawful means to share information with law enforcement agencies and to respond to legal requests in order to prevent, detect and prosecute criminal offences, unauthorised use, breaches of the terms of service and policies and other harmful behaviour could be in the legitimate interests of *Facebook Ireland*.

The fact that third-party providers that have integrated *Facebook* Business Tools into their websites can wait until they have obtained the user's consent before transmitting data to *Facebook Ireland* (paragraph 868 of the Office's decision) and that, since 28 January 2020, *Facebook* has provided the OFA function, which allows *Facebook.com* users to view a summary of the information *Facebook* receives about their activities on other websites and apps, and to disconnect information about past and future activities from their *Facebook.com* account if they so wish, should perhaps also be taken into account here, in addition to the legal right to object under Article 21 of the GDPR (paragraphs 148 and 149 of the statement of grounds of appeal).

(c) Question 5 of the request seeks to clarify whether collecting those data, linking them with the *Facebook.com* account and using them, or using off-*Facebook* data already collected and linked by other lawful means, can be justified in individual cases under Article 6(1)(c), (d) and (e) of the GDPR, in order, 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)) as *Facebook*

Ireland claims in Annex Bf 12, since, even then, the processing of those data cannot always, without exception, be made conditional on the user's consent, or whether any justification for processing off-*Facebook* data for these reasons can generally be ruled out.

f) If the data processing policies and their implementation are unlawful or unjustified, the question whether they also constitute an exclusionary abuse for the purposes of the general provision of Paragraph 19(1) of the GWB **[Or. 24]** to the detriment of competitors on the market for social networks for private users or on other markets would no longer be relevant.

g) If, and in so far as, the processing of off-*Facebook* data can only be justified by consent, Question 6 seeks to clarify whether it is actually possible for users to give effective consent within the meaning of Articles 6(1)(a) and 9(2)(a) of the GDPR to a dominant undertaking such as *Facebook Ireland*, as required by the Federal Cartel Office in its order to remedy the alleged breach, or whether the requirement under Article 4(11) of the GDPR for consent to be given freely can never be met vis-à-vis a dominant undertaking, even when performance of the contract does not depend on consent to the processing of data. This might be suggested by the first sentence of recital 43.

2. Clarification of the questions referred is not rendered superfluous by the fact that the Federal Cartel Office based its order in the appeal proceedings 'additionally' (sentence 88 of the statement of defence) on the grounds of the Federal Court of Justice's decision in the preceding summary proceedings (Decision of 23 June 2020 KVR 69/19, available from JURIS – *Facebook* [ECLI:DE:BGH:2020:230620BKVR69.19.0]), according to which the processing of user data from other group services and *Facebook* Business Tools imposes additional services on *Facebook.com* users, which they 'may not want'; the terms of service objected to would not be imposed if competition were functioning effectively, but are likely to impede competition and, after a comprehensive assessment of the balance of interests, the additional services are considered to be abusive, particularly as they cannot not be justified under the GDPR. The order cannot be upheld on these grounds, largely because the Federal Cartel Office's findings did not provide the required evidence that the data processing operations are likely to impede competition. This could be considered a serious possibility only with regard to the processing of *Instagram* data; however Question 7, and possibly Questions 3 to 5, of the request must be clarified before a decision can be made on that point.

a) Since the Federal Court of Justice appears to assume that the Federal Cartel Office can include this justification in its order **[Or. 25]** in the appeal proceedings, although the allegation of abuse would then be based on facts other than a breach of the GDPR and the user consent required in the operative part would therefore not be consent within the meaning of the GDPR, but a different consent, possibly in addition to the consent to be granted under the GDPR, the Chamber will also take account of this justification in its examination of the order.

b) The Federal Cartel Office has, however, largely failed to make the necessary determination in respect of the requirement that the processing of off-*Facebook* data must be likely to impede competition. This would require evidence of a potentially anti-competitive effect – on the network market; on the network itself, because of increased network effects or product improvement, for example; on advertising, because of the detailed data held; or on advertising markets or third markets (regardless of how they are defined in individual cases) – while the practice of an undertaking in a dominant position cannot be characterised as abusive in the absence of any anti-competitive effect on the market (see judgment of 6 December 2012, *Astra Zeneca*, C-457/10 P, paragraph 112, available from JURIS ; judgment of 17 February 2011, *TeliaSonera*, C-52/09, paragraph 64, available from JURIS).

Since *Facebook Ireland* does not use the *WhatsApp* data of *Facebook.com* users on *Facebook.com* for personalisation and product purposes, and, by its own account, does not intend to do so in Europe either, it is not clear, and has not been established by the Federal Cartel Office, that the processing of *WhatsApp* data could in any way impede competition on the network market, on an advertising market or on a market for Messenger services. Nor has the Federal Cartel Office determined the extent to which *Oculus* data of *Facebook.com* users are used for the purposes of the *Facebook.com* network and would be likely to impede competition on the network market, on a relevant advertising market or on the market on which *Oculus* is provided. The processing of data from *Facebook* Business Tools 'may' really only 'not be wanted' by *Facebook.com* users who do not click or tap on the social plugins (Like, Share), do not use *Facebook* Login or Account Kit and have not consented to be shown personalised advertisements. However, the Federal Cartel Office has also failed to establish the extent to which data from *Facebook* Business Tools that are processed for purposes other than the personalisation of *Facebook.com*, the seamless use of *Facebook* products and **[Or. 26]** to show personalised advertisements, are likely to impede competition on the network market, on an advertising market or on third markets, particularly as users can also use the OFA function to disconnect these data from their *Facebook* account.

c) Only the processing of the *Instagram* data of *Facebook.com* users is really likely to impede competition, because it is used to personalise *Facebook.com* by suggesting people whom users follow on *Instagram* to them and, in that respect, can increase the network effects, and because it is used on *Facebook.com* in conjunction with the user's *Facebook.com* data, for example, for advertising purposes and for product improvement. The answer to the question whether data would be processed across services in this way, without the separate consent of users, if there were effective competition on the social networks market and, in particular, the comprehensive assessment of the balance of the interests required to establish whether *Facebook Ireland*'s conduct is abusive in terms of both user exploitation and restriction of competition (see BGH, decision of 23 June 2020, *Facebook*, KVR 69/19 [ECLI:DE:BGH:2020:230620BKVR69.19.0], paragraph 98 et seq. available from JURIS) hinges on whether the Federal Cartel Office can

establish that the processing of data, at least for this purpose, breaches the GDPR, which Question 7 seeks to clarify, and, furthermore, whether it breaches the GDPR because *Facebook Ireland* uses methods different from those governing normal competition between products or services on the basis of supplies by economic operators, which Questions 3 to 5 seek to clarify (see judgment of 6 October 2015, *Post Danmark*, C-23/14, paragraph 29 et seq.; judgment of 6 December 2012, *Astra Zeneca*, C-457/10, paragraphs 74 and 75, available from JURIS).

[…]