Case C-446/21

Summary of the request for a preliminary ruling pursuant to Article 98(1) of the Rules of Procedure of the Court of Justice

Date lodged:

20 July 2021

Referring court:

Oberster Gerichtshof (Austria)

Date of the decision to refer:

23 June 2021

Applicant:

Maximilian Schrems

Defendant:

Facebook Ireland Ltd

Subject matter of the main proceedings

General Data Protection Regulation – Facebook – General terms of service – Data processing – Consent – Personalised advertising – Personal data manifestly made public by the data subject – Question of how such data must have been manifestly made public

Subject matter and legal basis of the request

Interpretation of EU law, Article 267 TFEU

Questions referred for a preliminary ruling

1. Are the provisions of Article 6(1)(a) and (b) of the General Data Protection Regulation ('the GDPR') to be interpreted as meaning that the lawfulness of contractual provisions in general terms of service for platform agreements such as that in the main proceedings (in particular, contractual provisions such as: 'Instead of paying ... by using the Facebook Products covered by these Terms you agree

that we can show you ads … We use your personal data ... to show you ads that are more relevant to you.') which provide for the processing of personal data with a view to aggregating and analysing it for the purposes of personalised advertising must be assessed in accordance with the requirements of Article 6(1)(a) of the GDPR, read in conjunction with Article 7 thereof, which cannot be replaced by invoking Article 6(1)(b) thereof?

2. Is Article 5(1)(c) of the GDPR (data minimisation) to be interpreted as meaning that all personal data held by a platform such as that in the main proceedings (by way of, in particular, the data subject or third parties on and outside the platform) may be aggregated, analysed and processed for the purposes of targeted advertising without restriction as to time or type of data?

3. Is Article 9(1) of the GDPR to be interpreted as applying to the processing of data that permits the targeted filtering of special categories of personal data such as political opinions or sexual orientation (for advertising, for example), even if the controller does not differentiate between those types of data?

4. Is Article 5(1)(b) of the GDPR, read in conjunction with Article 9(2)(e) thereof, to be interpreted as meaning that a statement made by a person about his or her own sexual orientation for the purposes of a panel discussion permits the processing of other data concerning sexual orientation with a view to aggregating and analysing the data for the purposes of personalised advertising?

Provisions of EU law relied on

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), in particular Article 5(1)(b) and (c), Article 6(1)(a) and (b) and Articles 7 and 9.

Succinct presentation of the facts and procedure in the main proceedings

1 The defendant is a company incorporated under the law of the Republic of Ireland with its registered office in Dublin, Ireland. It does not have a branch in Austria. Facebook is an online platform and content-sharing social network that allows users to upload various content (for example, text posts, images, videos, events, notes or personal information) and share it with other users depending on the settings selected. That content can also be enriched by other users with further content (for example by adding comments, 'likes' or tags in photos or other content). Users can also communicate directly with other users and 'chat' with them or exchange data via direct messages and emails.

2 The defendant does not generate any content itself, but receives it, for its services, from private and commercial users without paying them for it. It provides its

services to its users free of charge and generates revenue by processing user data in order to sell advertisers the facility of customised and targeted advertising. In addition to relatively static advertising (displayed to every user in the same way), the defendant offers 'personalised' advertising, which allows the advertiser to target specifically individual groups of people (by location, age, gender or interests, for example) or even individuals. It therefore offers advertisers the opportunity to present their advertisements to a tailored audience. More than 2.2 billion users worldwide (as of November 2018) have registered with Facebook. Companies can also financially support ('sponsor') their content so as to ensure that it is displayed to more users.

3 The defendant makes 'Facebook Business Tools' available to commercial users. Rating and analytics services provided by the defendant allow advertisers to determine the effectiveness of their advertising or how users engage with content on their websites. The analytics systems use algorithms to examine large volumes of data, look for correlations and patterns and draw appropriate conclusions. The use of those tools is subject to the relevant terms of service.

4 Prior to the entry into force of the GDPR, Facebook users gave their explicit consent to the processing of their data in accordance with the defendant's terms of service at the time (entitled 'Statement of Rights and Responsibilities'). Before transmitting personal data, potential new users were informed that, by registering, they agreed to the Statement of Rights and Responsibilities and that they had read the Data Policy, including the Cookie Policy. They could change or withdraw their consent at any time by changing their settings, deleting their personal data or closing their account. For example, a user could at any time stipulate that the defendant could not use the user's activities on the Facebook service to optimise personalised advertisements.

5 Owing to the full entry into force of the GDPR on 25 May 2018, the defendant completely redrafted its previous Terms of Service and data use policies and presented them to Facebook users for their consent. After his account had been blocked previously, the applicant (actively) accepted the new Terms of Service of 19 April 2018 by clicking 'I accept' in order to be able to continue using Facebook. Consent was necessary in order to continue to access the account and use the services.

6 The defendant has set up various tools to enable users to view and control their stored data. Those tools do not show all the data processed, but only those that the defendant considers to be of interest and relevance to the users. For example, the applicant can see in the tools that he has opened an app, visited a website, searched for something, bought something, added something to a wish list or clicked on an advertisement on Facebook. The tools were created to give users access to up-to-date data within – what the defendant considers to be – reasonable limits.

7 The defendant uses cookies, social plug-ins and pixels. The defendant can ascertain the source of visits by means of cookies. Many of the defendant's services cannot be used without activating the cookie function. The defendant's social plug-ins are 'embedded' by website operators into their pages. The most widely used is the defendant's 'like button'. Technically speaking, a 'window' (iframe) is embedded into a website, and the defendant then fills that window with the social plug-in. Each time such websites containing the defendant's 'like button' are visited, the cookies stored, the URL of the page visited and various log data (e.g. IP addresses, time data) are transmitted to the defendant. In that respect, it is not necessary that the user has interacted with (for example by clicking or similar) or perceived the 'like button'. Loading a page with such a social plug-in is sufficient for those data to be transmitted to the defendant.

8 Like social plug-ins, pixels are software that a website operator can integrate into the website and that enables relevant information about website users to be collected. Pixels are commonly used to help websites measure and optimise advertising. For example, when website operators integrate a Facebook pixel into their own websites, they can receive reports from the defendant about how many people saw their advertising on Facebook and then subsequently went to the operators' own website to make a purchase or perform a certain predefined action.

9 Users can choose whether to allow the defendant to use data that it receives from advertisers and other partners about activity outside Facebook products for the purpose of customising advertisements ('Ads based on partner data'). As the applicant did not consent to this, the defendant does not process any of his personal data obtained from partners about activities outside Facebook products for the purpose of displaying personalised advertising for him. However, the applicant's data obtained via cookies, social plug-ins and comparable technologies on third-party websites are stored by the defendant and also used for the purpose of personalisation, improvement of Facebook products, 'to promote safety, integrity and security' and also to offer events to him.

10 The defendant also uses the data that the applicant provides to it and the data that it receives about him as a result of his actions in order to display to him what it considers to be relevant personalised content, including personalised advertising. This includes the use of the applicant's age, interests and Facebook usage. It also includes the use of information about the applicant's location in order to estimate where he might be in order to display content relevant to his location.

11 The applicant is also shown personalised advertising on the basis of the 'Custom Audience' tool. In order to be able to use Custom Audience, an advertiser must accept the Custom Audience Terms of Service, which explain that the advertiser acts as the 'controller' (within the meaning of the GDPR) and the defendant acts as the advertiser's 'processor' (within the meaning of the GDPR).

12 It is not clear whether, when and in what way advertisers who used 'Custom Audience' or the other business tools obtained consent from the applicant to transfer the data to the defendant within the framework of those tools.

13 Facebook tracks the applicant's 'click behaviour' and therefore 'knows' when he interacts with an advertisement or video. The defendant tracks the applicant's mouse movements in order to ensure, for example, that a human and not a bot is using the Facebook service. Accordingly, the applicant received the message 'You've been temporarily blocked' and was indeed blocked for a short period of time because he quickly and/or repeatedly clicked on the 'Why Am I Seeing This Ad' function. The defendant prevents excessive clicking on certain functions because it considers that this is necessary to ensure the security of data. The defendant does not use mouse movements to personalise advertising. The content of messages is not analysed for the purposes of personalised advertising.

14 The applicant did not add any sensitive data to his profile. Only his 'friends' can see his posts on his timeline; his 'friends list' is not public. The applicant also chose not to allow the defendant to use information from the 'relationship status', 'employer', 'job title' and 'education' fields for the purposes of targeted advertising.

15 The defendant processed the applicant's personal data (such as his IP address) in order to determine and process his whereabouts as accurately as possible ('last location'). In 2011, the defendant stored his exact longitude and latitude when calculating his 'last location'.

16 The defendant's data processing does not distinguish between 'simple' personal data and 'sensitive' data. The defendant carried out processing (including in the case of the applicant) in relation to interest in 'sensitive topics' such as health, sexual orientation, ethnic groups and political parties. It is possible to define a target group for advertising on the basis of those interests also.

17 For example, the applicant was shown an advertisement for a politician on the basis of the analysis that he was similar to other 'customers' who had 'liked' that politician. The applicant regularly received advertisements targeting homosexual persons and invitations to corresponding events, even though he had not shown an interest in the specific event beforehand and did not know the venue. Such advertisements and invitations were not based directly on the applicant's sexual orientation or his 'friends', but on an analysis of their interests.

18 The applicant commissioned an analysis from which conclusions could be drawn from his friends list; it showed that he had done civilian service with the Red Cross in Salzburg and that he is homosexual.

19 The applicant could and can delete (even if he wishes to keep his account) certain content, such as messages and photos, from his account by initiating a deletion process. This excludes, for example, name and email address and declined friend requests and removed friends, which are deleted only when the account is deleted.

Old passwords and previous names are not deleted either – at least not before the account is deleted.

20 By ‘deletion’ (in the case of an existing account), the defendant means that the data are detached from the account, that is to say, the data are ‘depersonalised’. In addition to the possibility of deleting data, there is also the possibility of removing and hiding them. A message sent via Messenger can be removed within ten minutes. This makes the message invisible to everyone, including the recipient. After ten minutes, the message can be removed from the recipient’s own messages; the message remains with the recipient. A post by someone else cannot be deleted, only hidden.

21 In the case of old messages or posts, only the individual deletion of each element or deactivation of the entire account is possible. The applicant does not want to make use of the option to delete his account permanently, because he wants to continue using Facebook.

22 With regard to the deletion of data, the defendant states the following in its Terms of Service, in point 3.1:

‘*You can delete content individually or all at once by deleting your account. … When you delete content, it’s no longer visible to other users; however, it may continue to exist elsewhere on our systems where:*

. Immediate deletion is not possible due to technical limitations (in which case, your content will be deleted within a maximum of 90 days from when you delete it);

. your content has been used by others in accordance with this licence and they have not deleted it (in which case, this licence will continue to apply until that content is deleted); or

. Where immediate deletion would restrict our ability to:

. investigate or identify illegal activity or breaches of our Terms and Policies (for example, to identify or investigate misuse of our Products or systems);

. comply with a legal obligation, such as the preservation of evidence; or

. comply with a request of a judicial or administrative authority, law enforcement or a government agency; in which case, the content will be retained for no longer than is necessary for the purposes for which it has been retained (the exact duration will vary on a case-by-case basis).

In each of the above cases, this licence will continue until the content has been fully deleted.’

23 The defendant states (in its current terms) that it does not initiate a permanent deletion of data from the servers until 30 days after the deletion of an account. It justifies this on the grounds that a deleted account cannot be reactivated and this leads to the permanent loss of content uploaded by the user on Facebook, which is why it grants the user a 30-day waiting period to change his or her mind and cancel his or her request, whereby, however, once deletion has been requested, the user's personal data are no longer accessible to other users. After the 30-day waiting period, the defendant starts the deletion process and the user's personal data are permanently deleted from the defendant's servers within 90 days, whereby the personal data are permanently deleted but the remaining metadata are only de-identified and anonymised. After the 90 days, some data may remain, for a limited period, in inaccessible back-ups carried out for the purposes of recovery in the event of a disaster.

24 The applicant made personal data public on the website 'Europe versus Facebook' in the form of sample data, for instance as an example of the 'last location' function, the GPS data of his university, from where he logged in. The applicant is homosexual and also communicates this to the public. However, he did not indicate his sexual orientation in his profile.

25 In the present proceedings, a request for a preliminary ruling has already been made to the Court of Justice of the European Union ('the Court'). Following the Court's judgment of 25 January 2018 in *Schrems* (C-498/16, EU:C:2018:37), the applicant amended the form of order sought by him. With heads of claim 4 to 9, the applicant now requests, in essence, that the Court

– (4) order the defendant to conclude with the applicant a written contract that meets the requirements of Article 28(3) of the GDPR, between the applicant as controller and the defendant as processor, with regard to the data applications operated by the applicant himself via the facebook.com portal for his personal purposes (profile, timeline – including likes and comments – events, photos, videos, groups, personal messages, friend lists and applications);

– (4.1.) in the alternative, declare, with effect for the relationship between the defendant and the applicant, that an effective contract that complies with Article 28(3) of the GDPR does not exist between the applicant as controller and the defendant as processor with regard to the data applications operated by the applicant himself via the facebook.com portal for his personal purposes (profile, timeline – including likes and comments – events, photos, videos, groups, personal messages, friend lists and applications);

– (5) declare, with effect for the relationship between the defendant and the applicant, that the applicant's consent to the defendant's Terms of Service in the version of 19 April 2018 and in the version of 31 July 2019 together with the associated data use policies (data policy, cookie policy) and his consent to (future) equivalent clauses in terms of service of the defendant ('tied' declarations of consent) do not constitute effective consent, given to the

defendant as controller, to the processing of personal data pursuant to Article 6(1) of the GDPR, read in conjunction with Article 7 thereof;

– (5.1.) in the alternative, declare, with effect for the relationship between the defendant and the applicant, that the applicant's consent to the defendant's Terms of Service in the version of 19 April 2018 and in the version of 31 July 2019 together with the associated data use policies (data policy, cookie policy) does not constitute effective consent, given to the defendant as controller, to the processing of personal data pursuant to Article 6(1) of the GDPR, read in conjunction with Article 7 thereof;

– (6) order the defendant to refrain from processing the applicant's personal data for personalised advertising and for the aggregation and analysis of data for advertising purposes;

– (7) declare, with effect for the relationship between the defendant and the applicant, that the applicant has not given effective consent to the processing, for the defendant's own purposes, of his personal data which the defendant has received from third parties;

– (8) order the defendant to refrain in the future from using the applicant's data concerning visits to, or the use of, third-party sites (in particular through the use of social plug-ins and similar techniques), unless technical data are processed solely for the purpose of displaying website elements and the applicant has without any doubt freely given his informed and unambiguous consent in advance to a specific processing operation ('opt-in'; for example by clicking on a social plug-in);

– (9) order the defendant to refrain in the future from processing, for the defendant's own purposes, the applicant's personal data which the defendant has received from third parties, unless the applicant has without any doubt freely given his informed and unambiguous consent in advance to a specific processing operation ('opt-in').

26 By judgment of 30 June 2020, the court of first instance dismissed the action. It stated the following: due to his private use, the applicant is not a 'controller' within the meaning of the GDPR, because the latter does not apply to him. For heads of claim 5 and 7, the applicant does not have a legal interest in the declaration sought. Nor is the applicant entitled to seek injunctive relief (heads of claim 6 and 8 to 10). As an integral part of the service offered by the defendant, the personalisation and the personalised advertising result from the Terms of Service and the policies linked thereto, which were made part of the contract. There is no infringement of Article 9 of the GDPR. The question of whether the established invitations to events and advertisements disclosed the applicant's homosexuality can remain open, because the applicant had made it public himself, with the result that there is an exception to the requirement to give explicit consent

(Article 9(2)(e) of the GDPR). The applicant's 'interest' in various parties and politicians reveals only his interest in politics, not a political opinion.

27 The appellate court did not uphold the applicant's appeal on the merits, in so far as it is relevant to the present case. It stated the following: the contract between the parties is a contractual relationship that is not expressly regulated in the Austrian legal system, that is to say, it is an atypical contractual relationship. Its content consists, in essence, in the fact that the defendant provides the Facebook user with access to a 'personalised' platform – that is to say, one that is individually tailored to his or her interests and settings – on which he or she can communicate with other Facebook users. Although the Facebook user does not owe any money for the access provided to that forum, he or she tolerates the defendant's exploitation of all the user's personal data made available to it. The purpose of the processing of those data is to send personalised advertising to the user. To that end, the defendant does not pass the data of its users on to third parties without their explicit consent, but, rather, sends advertising on behalf of advertisers to specific target groups which remain anonymous to the advertisers and which it filters out from the data. The essence of that Facebook business model is explained in the terms and conditions in such a way that any reasonably attentive reader can easily understand. The model is neither contrary to accepted principles of morality nor unusual. The processing of the user's personal data is a cornerstone of the contract concluded between the parties to the dispute. Therefore, the processing of the applicant's personal data is 'necessary' for the performance of the contract within the meaning of Article 6(1)(b) of the GDPR.

28 The applicant lodged an appeal on points of law against that judgment with the Oberster Gerichtshof (Supreme Court), maintaining heads of claim 4 to 9.

Essential arguments of the parties in the main proceedings

29 The applicant submits the following: even if the defendant now concedes that he did not give consent within the meaning of Articles 6 and 7 of the GDPR to data processing and bases its processing on the contractual necessity of such processing, there is an interest in the declaratory finding sought in heads of claim 5 and 7, in particular due to the 'tied' declarations of consent in the Terms of Service. The defendant's data processing infringes the GDPR in several respects. There is a danger of repetition and therefore a right to injunctive relief. In particular, despite the fact that a deletion process had been initiated, the data are not actually deleted; a search for the applicant's data would be possible without his consent, and data within the meaning of Article 9 of the GDPR would be processed without consent within the meaning of Article 7 of the GDPR. There are doubts as to whether previously purchased data of the applicant has now been deleted and also as to whether the defendant does not have the applicant's biometric data and is tracking his mouse movements.

30 The defendant's partners did not obtain the applicant's consent to the transfer of data to, and/or the further use by, the defendant. The defendant also failed to comply with its duty to provide information.

31 The defendant opposes the form of order sought. It submits that the processing of the applicant's data is carried out in accordance with the agreed policies and terms, which are in line with the GDPR. The data processing is lawful and is not based on the applicant's consent within the meaning of Articles 6 and 7 of the GDPR, but on other justifying circumstances, primarily on contractual necessity.

Succinct presentation of the reasoning in the request for a preliminary ruling

32 Article 6 of the GDPR regulates the cases that justify the processing of data. The defendant bases its processing not on the applicant's consent (Article 7 of the GDPR), but on the fact that the data processing is an integral part of the contractual purpose of 'personalisation' and is necessary for the performance of the contract. According to the defendant, the applicant concluded the contract in full knowledge of that content, which is why the data processing is permissible as long as the applicant does not delete his account and thus terminate the contract with the defendant.

33 According to Article 6(1)(b) of the GDPR, the processing of personal data is permitted if it is necessary for the performance of the contract in the broad sense (thus including ancillary obligations). The decisive factor is the purpose of the contract – which emerges from the content of the contract – and what is necessary for the performance of the contractual obligations or the exercise of rights or in order to take steps prior to the conclusion of the contract.

34 The appellate court took the view that the processing of the user's personal data is a cornerstone of the contract concluded between the parties to the dispute. It stated that this is because only such use of data enables customised advertising, which significantly shapes the 'personalised experience' required of the defendant and at the same time provides it with the income required to maintain the platform and make a profit. Such processing is therefore 'necessary' for the performance of the contract within the meaning of Article 6(1)(b) of the GDPR.

35 However, the referring court considers that that view is by no means compelling. A core question in the present case is whether the declaration of intent to process the data can be subsumed by the defendant under Article 6(1)(b) of the GDPR so as thereby to deprive the applicant of the significantly higher level of protection offered to him by the legal basis of 'consent' (Article 7 of the GDPR).

36 In its current guidelines on Article 6 of the GDPR, the European Data Protection Board (EDPB) proceeds on the assumption that, as a general rule, processing of personal data for behavioural advertising is not necessary for the performance of a contract for online services (EDPB Guidelines 2/2019, paragraph 52). However, in respect of online services, the EDPB acknowledges that personalisation of

content may (but does not always) constitute an intrinsic and expected element of certain online services, and therefore may be regarded as necessary for the performance of the contract with the service user in some cases.

37 In paragraph 30 of the EDPB Guidelines 2/2019, it is stated in that respect that processing under Article 6(1)(b) of the GDPR can enter into consideration only in respect of certain obligations under a contract. Merely being 'mentioned in the small print' is not sufficient. The assessment of 'necessity' must take into account not only the controller's perspective, but also the data subject's perspective. Although in that respect the obligations may also include ancillary contractual obligations, the storage of data for marketing purposes should not be included in this. It is explicitly stated that 'behavioural advertising is not a necessary element of online services'. The legal literature also takes a restrictive position on this.

38 The objective purpose of the contract is the decisive factor for the interpretation of the contract under data protection law and the question of whether data processing is 'necessary' within the meaning of Article 6(1)(b) of the GDPR. This cannot include artificially or unilaterally imposed services. The necessity of data processing for the performance of a contract depends on whether there is a direct factual connection between the intended data processing and the specific purpose of the contractual obligation. Article 6(1)(b) of the GDPR must be interpreted narrowly in that respect and does not apply to situations where the processing is not actually necessary for the performance of a contract. The fact that the purposes of the processing are covered by contractual clauses formulated by the provider does not automatically mean that the processing is necessary for the performance of the contract.

39 In the case of the applicant, data on his political beliefs and sexual orientation are also processed. He receives advertising for events targeting homosexual persons on the basis of an analysis of his 'interests' and not his sexual orientation or that of his friends. His list of activities includes apps and websites that are targeted at homosexual users or operated by political parties.

40 Article 9(1) of the GDPR provides for a general prohibition on the processing of such sensitive data, except where at least one of the cases of Article 9(2) of the GDPR applies. Sensitive data includes data on racial and ethnic origin, political opinions, religious beliefs or sexual orientation.

41 Article 9(2)(e) of the GDPR permits the processing of sensitive personal data relating to the data subject where the data have been manifestly made public by the data subject. The rationale behind the provision is that personal data which have been freely made available to the public by the data subject do not pose a significant risk to privacy, with the result that they do not require the higher level of protection afforded by Article 9 of the GDPR. The provision covers data that are freely available on the internet or in public registers and directories that can be viewed by anyone or that are disseminated via the media. However, the mere fact that data are publicly accessible is not sufficient to dispense with the protection

afforded by Article 9 of the GDPR. Rather, the circumstance of the data having been made public must be manifestly attributable to an act of will on the part of the data subject.

42 According to the findings, the applicant (voluntarily) communicated his sexual orientation publicly, but did not indicate it in his Facebook profile. During a panel discussion, the applicant stated, for example, that although he had never indicated on Facebook that he was homosexual, his sexual orientation could be inferred from his friend list. He did not speak about it in public because he wanted to be associated in public primarily with his fight for data protection.

43 The referring court concludes from this that the applicant made that statement with the intention of questioning and publicly criticising the data processing already carried out by the defendant. Consent within the meaning of Article 9 of the GDPR therefore cannot be inferred from that statement.

44 The question therefore arises as to how the applicant's sensitive data would have had to be made public in order for Article 9(2) of the GDPR to apply.