The Supreme Court, as the court of appeal, by the President of the Senate, Hon.-Prof. Dr. Gitschthaler, as Chairman, the Court Councillors Univ.-Prof. Dr. Kodek and Dr. Nowotny, the Court Councillor Dr. Faber and the Court Councillor Mag. Pertmayr as further judges in the case of the plaintiff Maximilian Schrems,

represented by Lansky, Ganzger & Partner Rechtsanwälte GmbH, Vienna, against the defendant PartyFacebookIreland Limited, Dublin, 4 Grand Canal Square, Ireland, represented through 1. [redacted] Lawyers GmbH in Vienna, 2. [redacted] Lawyers GmbH, Vienna, for declaratory judgment, injunction and conclusion of a contract, on the appeal of the plaintiff against the judgment of the Vienna Higher Regional Court as the court of appeal of 7 December 2020, GZ 11 R 153/20f, 11 R 154/20b-99, whereby the judgment of the Vienna Regional Court for Civil Matters of 30 June 2020, GZ 3 Cg 52/14k-91, was upheld in closed session . 2020, GZ 3 Cg 52/14k-91, was confirmed in closed session.

Description

captured:

I. The following questions are referred to the Court of Justice of the European Union for a preliminary ruling pursuant to Article 267 TFEU:

1. Are the provisions of Article 6(1)(a) and (b) of the GDPR to be interpreted as meaning that the lawfulness of contractual provisions in general terms of use of platform contracts such as the one in the main proceedings (in particular contractual provisions such as:
"In lieu of paying for [...], by using the Facebook Products to which these Terms of Use apply, you agree that we may show you ads .... We will use your personal data [...] to show you ads that are more relevant to you"), which involve the processing of personal data for aggregation and analysis of data for the purposes of personalised advertising, must be assessed in accordance with the requirements of Article 6(1)(a) in conjunction with Article 7 of the GDPR, which cannot be replaced by relying on Article 6(1)(b) of the GDPR?

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 at issue in the main proceedings (in particular by the data subject or by third parties on and off the platform) may be aggregated, analysed and processed for the purposes of targeted advertising without any restriction as to the time or nature of the data?

3. Is Art 9(1) GDPR to be interpreted as applying to the processing of data which permits the targeted filtering of special categories of personal data such as political opinion or sexual orientation (for example, for advertising), even though

the controller does not differentiate between these data?

4. Is Article 5(1)(b) in conjunction with Article 9(2)(e) of the GDPR to be interpreted as meaning that a statement about one's sexual orientation for the purposes of a panel discussion permits the processing of other data on sexual orientation for the purposes of aggregating and analysing data for the purposes of personalised advertising?

II. The proceedings before the Supreme Court on the applicant's appeal against the dismissal of points 5 to 9 of the application are suspended until the preliminary ruling of the Court of Justice of the European Union has been received pursuant to section 90a(1) GOG.

D e s c r i p t i o n :

[1] I. Facts

[2] The Defendant is a company incorporated under the laws of the Republic of Ireland with its registered office in Dublin, Ireland.

It has no branch office in Austria. A significant proportion of the world's population (excluding China and Russia in particular) regularly communicates via the "closed" communication network of the defendant or its parent company Facebook Inc., whereby users in the European Union are provided with the Facebook service by the defendant.

[3] The Facebook service is an online platform and social network for sharing content. It allows users to upload various content (e.g. text posts, pictures, videos, events, notes or personal information) and share it with other users depending on the settings selected. This

Content can also be enriched by other users with further content (e.g. by adding comments, "likes" or markings in photos or other content). Users can also communicate directly with other users and "chat" with them or exchange data via direct messages and e-mails.

[4] The defendant does not generate any content itself, but receives it for its services from private and commercial users without direct reimbursement of costs or without paying a specific "fee" for it. It limits itself to the provision and administration of the infrastructure and offers functions for the automatic aggregation of user data. The defendant's economic model is to generate revenue through tailored advertising and commercial content based on the same preferences and interests. It generates its profit primarily through advertising, which is placed in various forms in the defendant's services. It provides its services to its users free of charge and generates revenue by processing user data to sell advertisers the opportunity to tailor and target advertising. In addition to relatively static advertising (displayed equally to each user), the defendant offers "personalised" advertising, which allows the advertiser to precisely target individual groups of people (e.g. by location, age, gender, interests) or even individuals. It therefore offers advertisers the opportunity to present their ads to a tailored audience. More than 2.2 billion users worldwide (as of 11/2018) have signed up for Facebook. Companies can also present their

Support content financially ("sponsoring") and thus ensure that this content is displayed to more users.

[5] The defendant provides Facebook **Business Tools** to commercial users. Defendant's rating and analytics services allow advertisers to determine the effectiveness of their advertising or how website users engage with content on their websites. The analytics systems use algorithms to examine large amounts of data, look for correlations and patterns, and draw appropriate conclusions.

[6] TheBusinessToolsallow advertisers to create ads and reach the relevant audiences. There are three ways to define the audience: the Custom Audience Tool, the Look-A-Like Audience Tool or the
"Core Audience Function". The Terms of Use for F acebook Business Tools, the Terms of Use for Custom Audiences, the Terms of Data Processing and the Advertising Policy apply to the use of these tools.

[7] Prior to the entry into force of the GDPR, Facebook users gave express consent to the processing of their data in accordance with the defendant's then terms of use (entitled "Statement of Rights and Responsibilities"). Potential new users were informed before submitting personal data 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 consent at any time by changing their privacy settings, deleting their personal data or closing their account. For example, a user could at any time

set his privacy settings so that the defendant could not use the user's activities on the F acebook service to optimise personalised advertisements.

[8]]Due to the full effectiveness of the GDPR as of 25. 5. 2018, the defendant has amended its previous terms of use ("Statement of Rights and Obligations" of15. 11 . 2013) anditsprevious Data Use Policy of 15. 11. 2013 completely redrafted and presented to Facebook's users for approval. The plaintiff, after his account had previously been suspended, accepted the new terms of use of 19 4. 2018 by clicking on them (actively), knowing the linked data policy, cookie policy and legal basis information, so that he could continue to use Facebook. Consent was required to continue to access the account and use the services.

[9] The defendant has set up various tools to enable users to view and control their stored data. These tools do not show all the data processed, but only the data that the defendant considers interesting and relevant for the users. For example, the plaintiff sees there that he has opened an app on Facebook, visited a website, searched for something, bought something, added something to a wish list or clicked on an advertisement. The tools were created to give users access to up-to-date data in what the defendant considers to be a reasonable framework.

[10] The defendant uses cookies, social plugins and pixels as stated in its terms/policies. Through the cookies, the Defendant can identify the source of the calls to

assign. Many of the defendant's services cannot be used without activating the cookie function. The defendant's "social plug-ins" are integrated by website operators into their pages.

"built in". The most widespread is the so-called "Like Button" of the defendant. Technically, a "window" (iframe) is cut into a website and this window is then filled with the "social plug-in" by the defendant. Each time such websites containing a "Like Button" of the defendant are called up, the stored cookies, the URL of the visited page and various log data (e.g. IP addresses, time data) are transmitted to the defendant. It is not necessary that the user interacts with the "Like Button" (e.g. by clicking or similar) or has noticed it. Loading a page with such a "social plug-in" is sufficient to transmit this data to the defendant .

"Plug-ins" are also found on pages of political parties, on medical pages or on pages for homosexuals, which the plaintiff visited. Due to the

"plug-in" on fpoe.at, the defendant was able to track the specific surfing behaviour of the plaintiff and a data flow to the defendant was triggered.

[11] Like social plug-ins, pixels are software that a website operator can integrate into the website and enable to collect relevant information about the website users. Pixels are often used to help websites measure and optimise advertising. For example, when integrating a Facebook pixel into one's website, website operators can receive reports from the defendant about how many people have seen their advertisements on Facebook and then click on its

own website to make a purchase or perform a certain predefined action.

[12]] Social plug-ins and pixels work hand in hand with cookies to transmit information to the web server. They are building blocks of internet advertising, with the vast majority of content available on the internet today being funded by advertising. Internet advertising enables billions of users around the world to communicate online at zero cost and access news, information, education, entertainment and other services. Plug-ins are used to deliver relevant ads to users. Pixels have come to play an important role in internet advertising because they allow advertisers to measure campaign performance and conversation events and gain audience insights.

[13]] The Respondent relies on its users' consent to data processing in the Data Policy in the following cases:

"- *For processing data with special protection (e.g. your religious views, your political opinions, who you are 'interested in' or your health when you share this information in your Facebook profile fields or under life events) so that we can share it with the people you choose and personalise your content.*

- *For the use of facial recognition technology*
- *For the use of data that advertisers and other partners provide to us about your activity outside of Facebook Companies' products to help us personalise the ads we serve to you on Facebook Companies' products.*

Facebook companies and on websites, apps and devices that use our advertising services.

• *For sharing personally identifiable information (information such as your name or email address that can be used in itself to contact or identify you) with advertisers; for example, when you instruct us to share your contact information with an advertiser so that they can contact you, such as to send you additional information about a highlighted product or service.*

• *To collect information that you allow us to obtain through the device-based settings you enable (such as access to your GPS location, camera or photos) so that we can provide the features and services described when you enable the settings."*

[14] The plaintiff did not give consent to the aforementioned data processing. The defendant collected information about the plaintiff's whereabouts when taking a photo that was later uploaded because he had set the relevant device-based settings of the recording device.

[15]] Users can choose whether to allow the Defendant to use data it receives from advertisers and other partners about activity outside of Facebook Products for the purpose of customising ads ("ads based on partner data"). Because the Plaintiff has not consented to this, the Defendant does not process any of the Plaintiff's personal data received from partners about activity outside of Facebook Products for the purpose of displaying

personalised advertising for the plaintiff. However, the plaintiff's data, which is obtained via cookies, social plug -ins and comparable technologies on third-party websites, is stored by the defendant and also for the purpose of personalisation, improvement of Facebook products,
used "to promote protection, integrity and security" and also to offer events to the plaintiff.

[16] The defendant explains that in the settings for advertisements based on partner data, which give the option "do not allow": "*We do not delete data if you do not allow the use of this data for advertising. You will continue to see as many ads as before. However, these will be based on your activity in Facebook company products or may come from specific companies you've shared your contact information with (if we've matched your profile to their customer list).*"

[17]] The Defendant also uses the data that the Plaintiff provides to the Defendant and the data that the Defendant obtains about the Plaintiff as a result of the Plaintiff's actions to display to the Plaintiff what it considers to be relevant personalised content, including personalised advertising. This includes the use of the Claimant's age, interests and Facebook usage. It also includes using information about the plaintiff's location to assess where the plaintiff may be in order to display content relevant to the plaintiff's location (e.g. an ad promoting an upcoming concert in his city).

[18] The plaintiff is also shown personalised advertising based on the "Custom Audience" tool. The hashed data is deleted after a maximum of 48 hours, after the

The advertiser will be deleted after the matching process has been completed. In order to use Custom Audience, an advertiser must accept the Custom Audience Terms of Use, which explains that the advertiser is considered to be the "controller" (within the meaning of the GDPR) and the defendant as "processor" (within the meaning of the GDPR) of the advertiser.

[19]] Whether, when, in which way advertisers, who are "Custom Audience" or the other business tools, obtained consent from the plaintiff to transfer the data to the defendant in the context of these tools is not established.

[20] Facebook tracks the plaintiff's "click behaviour" as governed by the Data Policy and therefore "knows" when he interacts with an advertisement, video, etc. The defendant tracks the plaintiff's mouse movements for integrity purposes. The Defendant tracks the Plaintiff's mouse movements for integrity purposes, for example, to ensure that a human and not a bot is using the Facebook service. Thus, the Plaintiff received the message "You have been temporarily blocked" and was also briefly blocked for clicking quickly and/or repeatedly on the "Why Am I Seeing This Ad" feature. The Respondent prevents excessive clicking on certain features because it considers this necessary to ensure the security of the data. The Respondent does not use mouse movements to personalise advertising. The content of messages is not analysed for the purposes of personalised advertising.

[21]] The plaintiff has not added any sensitive data to his profile. Only his "friends" can see his future posts or posts on his timeline; his "friends list" is not public. The plaintiff has also chosen not to provide the defendant with the

Allow use of information on the profile fields relationship status, employer, job title and education for targeted advertising.

[22] The defendant processed personal data of the plaintiff (e.g. the IP address) in order to determine and process his whereabouts as accurately as possible ("Last Location"). In 2011, the defendant stored the exact longitude and latitude as part of the calculation of the plaintiff's "last location".

[23] Partner Categories was a product that allowed advertisers to target audiences using data from marketing partners, such as LiveRamp. This product was discontinued in the European Union in May 2018. It is not clear whether all of the plaintiff's data that the defendant had processed in the course of this product was irretrievably deleted.

[24] The defendant's data processing does not distinguish between "simple" personal data and "sensitive" data (special categories of personal data) insofar as it does not allocate data, i.e. it does not extract whether data are sensitive or not.

[25]] The defendant processed (also in the plaintiff) the interest in "sensitive topics" such as health issues, sexual orientation, ethnic groups and political parties. It is possible to define a target group for advertising also according to these interests. The defendant therefore allows to advertise to men on the basis of interest in men, to people on the basis of interest in homosexuality, in political parties or in diseases and also allows to select as target group people who do not live in their home country.

[26] The plaintiff was shown an advertisement for the Neos politician Beate Meinl- Reisi nger, based on the analysis that he resembles other "customers" who have marked this politician with "like me". The plaintiff regularly received advertisements targeting homosexual persons and invitations to relevant events, although he was not interested in the specific event beforehand and did not know the location of the event. T hese advertisements or invitations were not directly oriented to the sexual orientation of the plaintiff or his "friends", but to the analysis of their interests.

[27] It is indicated tothe client that the client's friend has marked a product with "I like" and vice versa.

[28] The plaintiff has commissioned an analysis,
The list revealed that he had done civilian service at the Red Cross in Salzburg and that he was homosexual.

[29] On the list of semer activities outside of
Faceboo k sc heinen ua Apps or Websi tes
and the FPÖ. The address of the
E-May l address is the same .

that do not exist and its
E-mail adress ed he did not m se mem
The defendant had used the profile he had given, but he had used it in his enquiries to the defendant.

(30] The plaintiff could and can (even if he wishes to keep the account) delete certain contents, such as news and photos, from his account by triggering a deletion process. Excluded from this are, for example, name and e-mail address and rejected applications.

Friend requests and removed friends that are only deleted when the account is deleted. Old pokes, if deleted by the user, are only hidden to avoid further harassment. Old passwords and old names are also not deleted - at least before the account is deleted.

[31] By "deletion" (if the account is still open),

the defendant means that the data is detached from the account, i.e. unlinked. The data is "depersonalised". In addition to the possibility of deletion, there is also the possibility of removal and concealment. If you send a message via Messenger, you can remove this message again within ten minutes. This makes the message invisible to everyone, including the recipient. After these ten minutes, you can remove this message from your own messages, but the message remains with the recipient. You cannot delete a post that someone else has posted, you can only hide it.

[32] In the case of old messages or postings,

only the individual deletion of each element or a deactivation of the entire account is possible. The plaintiff does not want to make use of the option to permanently delete his account because he wants to continue using Facebook.

[33] With regard to the deletion of data, the defendant states in its terms of use point 3.1...:

"You can delete content individually or all at once (by deleting your account). ... When you delete content, it is no longer visible to other users. However, it is possible that it is still available elsewhere in our systems if you delete it.

. immediate deletion is not possible due to technical limitations (in which case your

Content deleted within max. 90 days after deletion by you);

. your Content has already been used by others in accordance with this Licence and they have not deleted it (in which case this Licence applies until the Content is deleted); or

. immediate deletion would restrict us in the following actions:

. Investigate or detect illegal activity or violations of our terms of use and policies (e.g., admitting or investigating misuse of our products or systems);

. Fulfilment of a legal obligation, e.g. preservation of evidence; or

. Fulfilment of a requirement by a judicial or administrative body , a law enforcement agency or a public authority; in such a case, the content shall be maintained only for as long as is necessary for the purposes on which the maintenance is based (the exact duration depends on the individual case).

In all the above cases, this licence shall continue to apply until the content has been deleted in its entirety."

[34] The defendant states (in its current terms and conditions) that it will not initiate a permanent deletion of data from the servers until 30 days after the deletion of an account. It justifies this by stating that a deleted account cannot be reactivated and that this would lead to the permanent loss of content uploaded by the user to F acebook, which is why it grants the user a 30-day waiting period (i.e. a "cooling-off period") to

change his mind and cancel his request, but with the deletion request, the user's personal data would no longer be accessible to other users. Then, after the 30-day waiting period, the defendant would start the deletion process and the user's personal data would be permanently deleted from the defendant's servers within 90 days, with the personal data permanently deleted but the remaining metadata only de-identified and anonymised. Some data might remain for a limited period after 90 days in inaccessible backups for disaster recovery purposes.

[35]] The plaintiff has made personal data public on the Europe versus Facebook website as sample data, such as the example of the "Last Location" function, the GPS data of his university, from which he logged in.

However, he did not indicate his sexual orientation in his profile.

[36] II. submissions of the parties

[37] The plaintiff raises, inter alia, the following claim:

"The defendant is obliged to conclude a written contract with the plaintiff in accordance with the requirements of Article 28 (3) of the GDPR between the plaintiff as the data controller and the defendant as the data processor within 28 days in the case of the data applications operated by the plaintiff himself via the facebook.com portal for his personal purposes (profile, chronicle - including likes and comments - events, photos, videos, groups, etc.),

personal messages, friends list and applications).

4.1 In the alternative: It is established with effect between the defendant and the plaintiff that an effective contract in accordance with Article 28(3) of the GDPR does not exist between the plaintiff as controller and the defendant as processor with regard to the data applications operated by the plaintiff himself via the portal facebook.com for his personal purposes (profile, chronicle - including likes and comments - events, photos, videos, groups, personal messages, friends list and applications).

5. It is hereby declared with effect between the defendant and the plaintiff that the plaintiff's consent to the defendant's terms of use in the version of 19 April 2018 as well as in the version of 31 July 2019 including the associated data use guidelines (data guideline, cookie guideline), as well as the consent to (future) identical clauses in the defendant's terms of use (coupled declarations of consent) is not an effective consent to the processing of personal data pursuant to Art. 6 (1) in conjunction with Art. 7 DSGVO to the defendant as the controller.

5.1. In eventu: It is determined with effect between the defendant and the plaintiff that the plaintiff's consent to the defendant's terms of use in the version of 19 April 2018 as well as in the version of 31 July 2019 (in eventu: in the version of 19 April 2018) together with the associated data use guidelines (data guideline, cookie guideline) is not an effective consent to the processing of personal data pursuant to Art. 6 (1) in conjunction with Art. 7 DSGVO to the defendant as controller.

6. The defendant is owed to refrain from processing personal data of the plaintiff for personalised advertising, aggregation and analysis of data for the purpose of advertising, in case of other execution.

7. It is hereby determined with effect between the Defendant and the Plaintiff that no effective consent has been obtained from the Plaintiff for the processing of the Plaintiff's personal data obtained by the Defendant from third parties for the Defendant's own purposes as set out in the Data Policy/AN in

• Lines 69-74 ('Activities of others and information they provide about you. We also receive and analyse content, communications and information that others provide when they use our products. This may include information about you, such as when others share or comment on a photo of you, send you a message, or upload, sync or import your contact information'),

• Lines 126-143 ('Advertisers, app developers and publishers may send us information through the Facebook business tools they use, including our social plugins (such as the <like> button), Facebook Login, our APIs and SDKs, or the Facebook Pixel.' and 'We also receive information about your online and offline actions and purchases from third-party data providers who are authorised to provide us with your information.') and

• Lines 166-168 ('This is based on the data we collect and learn from you and others [including any special protection data you provide to us for which you have given your explicit consent]').

described is present.

8. The defendant is obliged to refrain from the use of the plaintiff's data regarding the visit or use of third party websites (in particular through the use of 'social plugins' and similar technologies), unless technical data are processed solely for the purpose of displaying website elements, and unless the plaintiff has freely, informedly and unambiguously consented to a specific processing operation in advance ('opt-in'; e.g. by clicking on a 'social plugin').

9. The defendant shall, in the event of other execution, be obliged to refrain in future from processing for the defendant's own purposes personal data of the plaintiff which the defendant has received from third parties, unless the plaintiff has given his unambiguous, free, informed and unambiguous prior consent to a specific processing operation ('opt-in')".

[38] In summary, the plaintiff argued that even if the defendant now conceded that he had not given his consent within the meaning of Article 6f of the GDPR to the processing of data and relied on the contractual necessity of the processing, there was an interest in declaratory relief in accordance with claims 5 and 7, in particular because of the linked declarations of consent in the terms of use. The defendant's data processing violated the GDPR in several areas. There was a risk of repetition and therefore a claim for injunctive relief as in claims 6, 8 to 10. In particular, data was not actually deleted despite the initiation of a deletion process, a search for the plaintiff's data was possible without his consent, and data as defined in Article 9 of the Data Protection Regulation was not deleted.

The defendant argued that the biometric data of the plaintiff could not be processed without consent pursuant to Article 7 of the GDPR. It was doubted that previously purchased data of the plaintiff had been deleted in the meantime and that the defendant did not have the plaintiff's biometric data and tracked his mouse movements.

[39] The defendant's partners had not obtained the plaintiff's consent for the transfer of data to and/or further use by the defendant. The defendant had also not fulfilled its duty to provide information.

[40] The **defendant** contested the claim. The processing of the plaintiff's data was carried out in accordance with the agreed guidelines and conditions, which were in line with the GDPR. The data processing was lawful and was not based on the plaintiff's consent within the meaning of Art 6 f of the GDPR, but on other grounds of justification, predominantly on contractual necessity.

[41] III. procedure to date

[42] In the present proceedings, a reference for a preliminary ruling has already been made once to the European Court of Justice (C-498/16 *Schrems v. Facebook Ireland*). Subsequently, the plaintiff amended his claim.

[43] In its judgement of 30 June 2020, the court **of first instance** dismissed the claim (point III of the judgement).

Due to his private use, the plaintiff was not

The plaintiff was not a "controller" within the meaning of the GDPR because it did not apply to him. The plaintiff lacked a legal interest in the requested declarations for claims 5 and 7. The request for injunctive relief (claims 6 and 8 to 10) was not justified. Personalisation and also personalised advertising as an essential component of the services offered by the defendant were not justified.

The terms of use of the service and the linked guidelines, which were made part of the contract. There was no violation of Article 9 of the GDPR. It could be left open whether

so that an

Reason for exception From which Requirement of a ex plicit

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

[44] The **Court of Appeal** did not uphold the plaintiff's appeal in this respect. The contract between the parties in dispute was an atypical contractual relationship not expressly regulated in the Austrian legal system. The content of the contract essentially consisted of the defendant providing the Facebook user with a
"personalised", i.e. individually tailored to his interests and preferences, platform on which he can communicate with other Facebook users. Although the Facebook user did not owe any money for access to this forum, he tolerated the defendant's use of all the user's personal data available to it. The processing of this data served to send personalised advertising to the user. For this purpose, the defendant does not pass on the data of its users to third parties without their express consent, but sends advertising on behalf of advertisers to specific target groups which remain anonymous vis-à-vis the advertisers and which it filters out from the data. The essence of this Facebook business model was explained in the terms and conditions in a way that was not understandable to anyone.

easily understandable to the average attentive reader. This model was neither immoral nor unusual. The processing of personal user data was a fundamental pillar of the contract concluded between the parties. Therefore, the processing of the plaintiff's personal data was "necessary" for the performance of the contract within the meaning of Art 6(1)(b) of the GDPR.

[45] The plaintiff **appealed** against this judgement to the Supreme Court, seeking a grant of the action with regard to the aforementioned points 4 to 9.

[46] IV. Legal assessment

[47]]A. Applicable Union law

Article 5 GDPR:

Principles for the processing of personal data

(1) Personal data must be

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

b) collected for specified, explicit and legitimate purposes and shall not be further processed in a way incompatible with those purposes; further processing for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes shall not be considered incompatible with the original purposes in accordance with Article 89(1) ('purpose limitation');

c) adequate and relevant to the purpose and limited to what is necessary for the purposes of the processing ("data minimisation");

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data which are inaccurate in relation to the purposes of their processing are erased or rectified without delay ("accuracy");

e) be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed; personal data may be kept for longer periods insofar as the personal data are stored, subject to the implementation of appropriate technical and organisational measures required by this Regulation to protect the rights and freedoms of the data subject, solely for archiving purposes in the public interest

or processed for scientific and historical research purposes or for statistical purposes pursuant to Article 89(1) ("storage limitation");

f) processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage by appropriate technical and organisational measures ("integrity and confidentiality");

(2) The controller is responsible for compliance with paragraph 1 and must be able to demonstrate compliance ("accountability").

Article 6 DSGVO:

Lawfulness of the processing

(1) Processing is only lawful if at least one of the following conditions is met:

a) The data subject has given consent to the processing of personal data concerning him or her for one or more specific purposes;

b) the processing is necessary for the performance of a contract to which the data subject is party or for the implementation of pre-contractual measures taken at the data subject's request;

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

d) the 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 of the controller or of a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the 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.

(2) Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation in relation to processing to comply with points (c) and (e) of paragraph 1 by specifying more precisely specific requirements for processing as well as other measures to ensure lawful and fair processing, including for other specific processing situations referred to in Chapter IX.

(3) The legal basis for the processing operations referred to in points (c) and (e) of paragraph 1 is determined by

a) Union law or

b) the law of the Member States to which the controller is subject. The purpose of the processing must be specified in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, must be necessary for the performance of a task carried out in the public interest or in the exercise of public authority vested in the controller.This legal basis may contain specific provisions adapting the application of the provisions of this Regulation, including provisions on the general conditions governing the lawfulness of the processing by the controller, the types of data processed, the persons concerned , the entities to which and the purposes for which the personal data may be disclosed, the purpose for which they are to be kept, the period for which they may be kept and the processing operations and procedures that may be applied, including measures to ensure lawful and fair processing, such as those for other specific processing situations in accordance with Chapter IX. Union or Member State law shall pursue an objective in the public interest and be proportionate to the legitimate aim pursued.

(4) Where processing for a purpose other than that for which the personal data were collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall - in order to determine whether the processing for another purpose is compatible with that for which the personal data were originally collected - take into account, inter alia

a) any link between the purposes for which the personal data were collected and the purposes of the intended further processing,

b) the context in which the personal data were collected, in particular with regard to the relationship between the data subjects and the controller,

c) the nature of the personal data, in particular whether special categories of personal data are processed pursuant to Article 9 or whether personal data relating to criminal convictions and offences are processed pursuant to Article 10,

d) the possible consequences of the intended further processing for the data subjects,

e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Article 7 GDPR:

Conditions for consent

(1) If the processing is based on consent, the controller must be able to prove that the data subject has consented to the processing of his or her personal data.

(2) Where the data subject's consent is given by means of a written statement which also concerns other matters, the request for consent shall be made in an intelligible and easily accessible form in clear and plain language in such a way that it can be clearly distinguished from the other matters. Parts of the statement shall not be binding if they constitute a breach of this Regulation.

(3) The data subject has the right to withdraw his/her consent at any time. The revocation of consent shall not affect the lawfulness of the processing carried out on the basis of the consent until the revocation. The data subject shall be informed of this before giving consent. The withdrawal of consent shall be as simple as giving consent.

(4) In assessing whether consent has been freely given, the greatest possible account must be taken of the fact whether, inter alia, the performance of a contract, including the provision of a service, is dependent on consent to the processing of personal data which is not necessary for the performance of the contract.

Article 9 GDPR:

Processing of special categories of personal data

(1) The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as the processing of genetic data, biometric data 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 in the following cases:

a) The data subject has given his or her explicit consent to the processing of the personal data referred to above for one or more specified purposes, unless, under Union or Member State law, the prohibition in paragraph 1 cannot be lifted by the data subject's consent,

b) processing is necessary to enable the controller or the data subject to exercise his or her rights and comply with his or her obligations under labour law and social security and social protection law, in so far as it is necessary under Union law or Member State law or a collective agreement under Member State law providing appropriate safeguards for the

fundamental rights and the interests of the data subject is permissible,

c) the processing is necessary to protect the vital interests of the data subject or another natural person and the data subject is physically or legally incapable of giving consent,

d) the processing is carried out on the basis of appropriate safeguards by a political, philosophical, religious or trade union foundation, association or other non-profit organisation in the course of its legitimate activities and provided that the processing relates solely to the members or former members of the organisation or to persons who have regular contacts with it in connection with its purposes and that the personal data are not disclosed to outside parties without the consent of the data subjects,

e) the processing relates to personal data which the data subject has manifestly made public,

f) processing is necessary for the establishment, exercise or defence of legal claims or in case of actions by the courts in the exercise of their judicial functions,

g) the processing is necessary for reasons of substantial public interest on the basis of Union law or the law of a Member State which is proportionate to the aim pursued, respects the essence of the right to data protection and provides for adequate and specific measures to safeguard the fundamental rights and interests of the data subject,

h) the processing is necessary for the purposes of preventive health care or occupational medicine, the assessment of the employee's fitness for work, medical diagnosis, health or social care or treatment, or the management of health or social care systems and services on the basis of Union law or the law of a Member State or on the basis of a contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3,

i) the processing is necessary for reasons of public interest in the area of public health, such as protection against serious cross-border threats to health or to ensure high standards of quality and safety in healthcare and medicinal products and medical devices, on the basis of Union law or the law of a Member State which lays down appropriate and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy, or

j) processing is necessary for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes as referred to in Article 89(1) on the basis of Union law or the law of a Member State which is proportionate to the aim pursued, respects the essence of the right to data protection and provides for adequate and specific measures to safeguard the fundamental rights and interests of the data subject.

(3) The personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 where those data are processed by or under the responsibility of a specialised staff member and that specialised staff member is subject to an obligation of professional secrecy under Union law or the law of a Member State or the rules of national competent authorities, or where the processing is carried out by another person who is also subject to an obligation of secrecy under Union law or the law of a Member State or the rules of national competent authorities.

(4) Member States may introduce or maintain additional conditions, including restrictions, as far as the processing of genetic, biometric or health data is concerned.

[48] B. Grounds for the questions referred

[49] Article 6 of the GDPR regulates the circumstances that justify the processing of data. Pursuant to Art 6(1)(1) of the GDPR, several permissions can exist side by side (arg "at least one of the following conditions"). This means that, in principle, all circumstances are equivalent and consent does not have to be fulfilled in addition to another circumstance (*Kastelitz/Hötzendorfer/Tschohl* in *Knyrim*, DatKomm Art 6 DSGVO Rz 14 f).

[50] The defendant does not rely on the plaintiff's consent, but on the fact that the data processing is an essential part of the

the purpose of the contract of "personalisation" and necessary for the performance of the contract. The plaintiff concluded the contract with knowledge of this content, which is why - according to the court of first instance - the data processing was permissible as long as the plaintiff did not delete his account and thus terminate the contract with the defendant.

[51]] 2.1 According to the findings, the economic model of the defendant is to generate revenue through tailored advertising and commercial content based on the same preferences and interests. It generates its profit primarily through advertising, which is placed in various forms in the defendant's services. It provides its services to its users free of charge and generates revenue by processing the user data to sell advertisers the opportunity of customised and targeted advertising.

[52] According to Art 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 also of ancillary obligations) (*Kastelitz/Hötzendorfer/Tschohl* in *Knyrim*, DatKomm Art 6 DSGVO Rz 33). The decisive factor is the purpose of the contract, which emerges from the content of the contract, and what is necessary for the fulfilment of the contractual obligations or the exercise of rights or for the implementation of pre-contractual measures (*Kastelitz/Hötzendorfer/Tschohl* in *Knyrim*, DatKomm Art 6 DSGVO Rz 36).

[53] According to the Court of Appeal, the processing of personal user data is a fundamental pillar of the contract concluded between the parties. Only this use of data enables tailor-made advertising, which the defendant's

personalised experience" owed to it and at the same time provides the defendant with the income necessary for maintaining the platform and making a profit. This data processing is therefore necessary for the performance of the contract.

"necessary" within the meaning of Art 6 (1) (b) DSGVO.

[54] However, this view is by no means self-evident. A core question of the present proceedings is whether the declaration of intent to process can be shifted by the defendant under the legal concept according to Art 6 (1) lit b DSGVO in order to thereby "undermine" the significantly higher protection that the legal basis "consent" offers to the plaintiff.

[55] In its current guidelines on Art 6 GDPR, the European Data Protection Board (EDSA) generally assumes that the processing of personal data for behavioural advertising is not necessary for the performance of a contract for online services (EDSA Guidelines 2/2019 para 52). However, for online services, the EDSA assumes that personalisation of content can be (but is not always) an essential and expected element of certain online services and can therefore in some cases be considered necessary for the performance of the contract with the user.

[56] Working Paper 217 of the Art 29 Working Party and paragraph 30 of Guideline 2/2019 of the EDSA, which is responsible for the uniform application and interpretation of the GDPR in the EU pursuant to Art 70 of the GDPR and thus succeeds the "Art 29 Working Party", state that processing pursuant to Art 6 (1) (b) of the GDPR is only possible for certain obligations of a contract. The mere "naming ... of processing activities ...

in the small print" is not sufficient (WP 217, p 16). In order to assess the "necessity", not only the perspective of the controller must be taken, but also the perspective of the data subject (EDSA, Guidelines 2/2019 on the Processing of personal data under Article 6(1)(b) GDPR in the context of the Provision of online Services to data subjects, Version 2.0, para 32; cited in *Kastelitz/Hötzendorfer/Tschohl* in *Knyrim*, DatKomm Art 6 DSGVO para 36). The obligations may also include secondary contractual obligations, which, however, do not include storage for marketing purposes (*Kastelitz/Hötzendorfer/Tschohl* in *Knyrim*, DatKomm Art 6 DSGVO Rz 36). It was explicitly stated that

"behavioural advertising is not a necessary element of online services".

[57] The literature also takes a restrictive position in this regard. *Jan Albrecht/Florian Jotzo* (Das neue Datenschutzrecht der EU, Art 6, Rz 44) state: "The GDPR sets narrow limits to such business models of many online providers. Art 6(1)(b) of the GDPR is not usually a legal basis, as providers such as Facebook typically use data about their users for advertising purposes, which is not necessary for the performance of the contract in the strict sense. “

[58] *Kühling/Buchner* (DSGVO- BDSG², Art 7, Rz 50) formulate similarly: "Nor is it necessary for the provision of the basic functions of a social network to evaluate clickstream, communication, contacts and other information about the users for commercial purposes and to transmit them to third parties".

[59] Also according to *Ehmann/Selmayr* (Datenschutz-grundverordnung, Art 6, Rz 13), the "storage of

Customer preferences for marketing purposes not necessary for the performance of the contract".

[60] 3.4 For the interpretation of the contract in terms of data protection law and the question of whether a data processing The objective purpose of the contract is decisive for the definition of "necessary" in the sense of Art. 6(1)(b) of the GDPR. Artificially or unilaterally imposed services cannot be subsumed under this. 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 legal obligation. Art 6(1)(b) DSGVO is to be interpreted narrowly in this sense and does not apply to situations in which 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 (European Data Protection Supervisor "EDPS", Opinion 4/2017, 19; cf. also *Kastelitz/Hötzendorfer/Tschohl* in *Knyrim*, DatKomm Art 6 DSGVO Rz 36).

[61] In the case of the plaintiff, data on his political beliefs and sexual orientation are also processed. The defendant processes, for example, the interest in "Alexander van der Bellen", "Die Grünen" or
"neos". The plaintiff was shown advertisements about neos politician Beate Meinl-Reisinger based on an analysis that he resembles other users who have marked this politician with "like" ("Lookalike Audience"). He receives advertisements on events targeting homosexual persons, based on an analysis of his
"interests" and not his sexual orientation or the

of his friends. His list of activities includes apps and websites aimed at homosexual users or from political parties.

[62] Article 9(1) of the GDPR provides for a general ban on processing such sensitive data, which can only be breached if at least one of the cases under Article 9(2) of the GDPR applies. If such a case exists, this leads to a breach of the general processing prohibition of Art 9 (1) GDPR. Sensitive data includes data on racial and ethnic origin, political opinions, religious beliefs or sexual orientation.

[63] Article 9(2)(e) of the GDPR permits the processing of sensitive personal data about the data subject if the data subject has obviously made the data subject public (*Kastelitz/Hötzendorfer/ Tschohl* in *Knyrim*, DatKomm Art 9 DSGVO Rz 41). The background to the regulation is that personal data which has been made accessible to the public by the data subject in his or her free self-determination does not represent a significant threat to privacy, so that it does not require the increased protection under Article 9 of the GDPR.

(*Kampert* in *Sydow*, European Data protection-basic ung [2] [2018] Art 9Rz 30). The regulation ordinance

Data that is freely available on the internet or in public registers and directories that can be viewed by anyone or that is disseminated via the media is subject to the GDPR. However, the mere fact that data is publicly accessible is not sufficient to waive the protection of Art 9 GDPR. Rather, the public access to the data must obviously be the result of an act of will on the part of the data subject (*Kampert* loc. cit., para. 31 f).

[64] According to the findings, the plaintiff (voluntarily) communicated his sexual orientation publicly, but did not indicate this on his Facebook profile. In the course of a presentation at the Representation of the European Commission in Austria, the plaintiff expressed:

"I'll give you a very banal example now: Based on my friend list, you can extrapolate my sexual orientation. I have never stated on Facebook that I am gay. That's been with me since I was 14, outed and stress-free and whatnot. But that's something that I don't tell all around in public, because I think, yes, I'd rather talk about data protection, otherwise you'll be in that category again. And that distracts from data protection.

[65] This shows that the plaintiff apparently made this statement precisely with the intention of questioning and publicly criticising the data processing already carried out by the defendant. No consent within the meaning of Article 9 of the GDPR can be inferred from this statement.

[66] This raises the question of how the plaintiff's sensitive data must have been made public in order for Art 9(2) GDPR to apply.

[67] The questions referred are necessary in order to clarify the interpretation of the applicable provisions of EU law.

[68] Until the matter is settled, the proceedings on the appeals of the parties shall be stayed pursuant to section 90a (1) GOG.

Supreme Court of
Vienna, on 23 June 2021

Electronic copy pursuant to section 79 GOG