Legal Update in the field of

Summer 2021

Weinhold Legal

Privacy disputes with Facebook continue

Another Facebook is heard in ECJ

The Austrian Supreme Court has referred the case of Max Schrems v Facebook[1] to the Court of Justice of the European Union (CJEU) for a preliminary ruling under Article 267 TFEU.

The Austrian court referred four questions to the CJEU raising fundamental doubts about the legality of Facebook's processing and use of personal data relating to all its customers in the EU.

Question 1: Legal title – consent versus contract

According to Mr Schrems' argument, since the General Data Protection Regulation (GDPR) came into force, Facebook has stopped claiming that it relies on users' consent to process their personal data and target advertising. Instead, Facebook argued that the consent clause should be understood as a "contract" in which users "ordered" personalised advertising. In Facebook's view, this interpretation would allow it to deprive users of all rights relating to the processing of personal data on the basis of consent under Article 6 (1) (a) of the GDPR. The requirements of freely given or informed consent would no longer apply if interpreted as a contract within the meaning of Article 6 (1) (b) GDPR.

The Austrian Supreme Court seems to share Mr. Schrems' concerns and in its preliminary question to the CJEU asks whether Facebook can simply replace Article 6 (1) (a) with Article 6 (1) (b) of the GDPR:

“The fundamental question in these proceedings is whether the declaration of intent (purpose) to process personal data by the defendant (FB) can be moved under the legal title of Article 6(1)(b) of the GDPR to "undermine" the significantly higher protection of the legal basis of "consent" serving the claimant.“

Questions 2-4: Data minimisation and sensitive personal data

The CJEU will also have to decide on three other issues relating to the lawfulness of Facebook's processing of personal data and whether the use of all data on facebook.com and from myriad other sources such as websites or advertisements that use Facebook's "Like" buttons for any purpose complies with the "data minimisation" principle under the GDPR.

Two other questions concern Facebook's processing of so-called sensitive data, or special categories of personal data (such as political opinions or sexual orientation) for personalised advertising.

Final decision

The Austrian Supreme Court was also relatively clear about Facebook's claim that it had provided Mr Schrems with all the data it considered "relevant":

"The fact that the obligation to provide information to the data subject cannot depend on the mere self-assessment of the defendant ('relevant') does not require further explanation."

It follows that the data subject's right of access to personal data is not subject to the controller's assessment of what data is relevant for these purposes; all data must be provided.

The burden of proof is on Facebook

In addition, the Austrian Supreme Court issued a decision on certain claims that can be decided without having to be referred to the CJEU. Mr Schrems was awarded €500 for "lack of access to data and access that the court described as 'Easter egg hunting'“. The court ruled this way because Facebook had not given Mr Schrems full access to his personal data. Nor did he receive essential information such as the legal basis on which his data was processed. The court pointed out that the data Facebook offered through its online tool was scattered among more than 60

[1] Unofficial English translation here.

categories of data with hundreds, if not thousands, of data points, which would have taken several hours for the data subject to sort through. The court noted that Mr. Schrems "rightly points out that the GDPR is based on a one-time request by the data subject for access to personal data, not an 'Easter egg hunt' where the data subject must 'hunt' with the controller for information about his or her personal data and the scope of processing.

The Austrian Supreme Court has repeatedly emphasised that the burden of proof is on Facebook to prove that it has granted full access to personal data or that the processing is lawful on its part. Facebook, on the other hand, took the position during the proceedings that it was up to Mr Schrems to prove that Facebook had not provided him with all the data and refused to answer Mr Schrems' questions.

Who "owns" Facebook data?

The case also called into question the roles of players on the Facebook platform. Mr Schrems argued that he is responsible for personal data on his profile or in Facebook messages (as a controller), which means that Facebook must follow his orders, for example in deleting data (as a „mere processor"). Facebook has taken the view that it is the controller of all user data on Facebook - with certain exceptions. The Austrian Supreme Court sided with the lower courts on this part of the dispute, stating, with reference to the case law of the Austrian courts and the CJEU, that Mr Schrems is the data subject and Facebook is the controller of the data and also the addressee of the obligations under the GDPR. The mere use of Facebook does not make Mr Schrems a data controller within the meaning of Article 4(7) GDPR. Otherwise, every Facebook user would be a controller under the GDPR, which is not consistent with the intent of the GDPR. Further, the court in this case held that since Mr. Schrems' Facebook profile was set to private, i.e., his posts could only be seen by his friends, it was not shown that Mr. Schrems also used the social network for professional or commercial activities or that Mr. Schrems allowed the sharing of content, thereby making that content publicly available. Therefore, the Court finds that in this case, the use of Facebook falls under activities of a purely personal nature or activities carried out exclusively in the home within the meaning of Recital 18 of the GDPR and thus the GDPR does not apply to these situations.

○ ○ ○

Final version of the EDPB guidelines on the concepts of controller and processor

The European Data Protection Board (EDPB) has adopted the Guidelines 7/2020, which clarify the basic terms used by the GDPR. In the first part, the guidelines clarify the concepts of controller, processor, joint controllers and third parties or recipients, and the concepts and criteria on which the GDPR relies in defining the terms. The second part then describes the implications associated with the different roles, whether controller, processor or joint controller.

GDPR Codes of Conduct

The EDPB issued guidelines on 4/2021 on codes of conduct as tools for the transfer of personal data to third countries, which are open for public comment until 1 October 2021. The main objective of the guidelines is to clarify the application of Article 40 (3) and Article 46 (2) (e) of the GDPR.

The Guidelines provide that, subject to the approval of the relevant supervisory authority and after the Commission has decided on its general validity within the European Economic Area, the Code of Conduct may be observed and used by controllers and processors not covered by the GDPR under Article 40(3) to provide appropriate safeguards for the transfer of personal data outside the EU. The Guidelines complement the EDPB Guidelines 1/2019 on Codes of Conduct, which set out a general framework for the adoption of Codes of Conduct. These controllers and processors are required to make binding and enforceable commitments, through contractual or other legally binding instruments, to uphold the relevant safeguards and measures provided by the Code, including with respect to the rights of data subjects as

required by Article 40 (3) of the GDPR.

The first code of conduct since the GDPR came into force, which was approved by the Belgian Data Protection Authority in May 2021, concerns the cloud industry ("EU Cloud CoC"). The EU Cloud CoC aims to establish data protection best practices for cloud service providers and to contribute to better protection of personal data processed in the cloud in Europe. It is an element whereby the cloud provider, as a processor, demonstrates sufficient guarantees to implement appropriate technical and organisational measures pursuant to Article 28(1) and (4) of the GDPR in such a way that the processing complies with the requirements of the GDPR (including the involvement of subcontractors). The purpose is to make it easier and more transparent for customers to analyse whether cloud services are suitable for their use case. The approval results in a harmonised interpretation of the GDPR provisions in the cloud sector across the European Union. The EU Cloud CoC covers the entire spectrum of cloud services: software (SaaS), platform (PaaS) and infrastructure (IaaS). The EU Cloud CoC only applies to business-to-business (B2B) cloud services where the cloud service provider (CSP) acts as a processor. It therefore does not apply to business-to-consumer (B2C) services, nor to any processing activities where the CSP may act as a data controller. The EU Cloud CoC does not yet serve as a guarantee for transfers of personal data to third countries, but its extension for these purposes is under development.

On making copies of identity cards in the context of AML legislation

Following the ambiguities that arose around making copies of identity cards in connection with different conclusions and recommendations in the opinion of the Office for Personal Data Protection (OPDP) and in the methodological instruction of the Financial Analysis Office (FAO), the OPDP commented on the interpretation of Act No.253/2008 Coll., on Certain Measures against the Legalization of Proceeds from Crime and Terrorist Financing (AML Act).

According to the interpretation of the AML Act by the OPDP, it **provides for the making of copies of identity cards as an option and not a legal obligation**. Thus, it is not a desirable practice to make copies of IDs for every client and in a blanket and indiscriminate manner. It would be desirable for the obliged entity, as defined by the AML Act, to carry out a risk assessment in advance and set up the making of copies of ID cards taking into account the risks of the service provided, while taking into account the principles of proportionality and minimisation of the processing of personal data.

The OPDP has issued the following summary material on identity proofing and the processing of personal data on a general scale.