Legal Update from the field of

Autumn 2021

Weinhold Legal

Use of cookies only with prior consent

The amendment brings changes from January 1st, 2022

The Government Bill amending Act No. 127/2005 Coll., On Electronic Communications and on Amendments to Certain Related Acts (the Electronic Communications Act), as amended, and certain other acts (**the Amendment**) was approved by the Chamber of Deputies. A fundamental change brought about by the amendment is **the obligation to have** the user's prior **provable consent to the use of cookies**. Cookies are small data files that are exchanged between a user's device and the site he or she visits. With the help of cookies, the operator of the website or app receives information that can then be used for marketing, statistical or even analytical purposes. Therefore, they are considered personal data under 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 Regulation on the protection of personal data, "**GDPR**").

The need for an amendment arises due to the imperfect implementation of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (**ePrivacy Directive**). The current interpretation of the Electronic Communications Act regarding the processing of cookies has derived the so-called opt-out principle. That is, it is possible, for the fulfillment of the information obligation of the operator as the controller of personal data, to process all types of cookies until the user withdraws his consent. However, this interpretation is not in line with the intention of the ePrivacy Directive. EU regulations provide for the use of the so-called opt-in principle, where the user must give prior consent to the use of cookies (there is, however, an exception for some technical and necessary cookies). According to the Amendment, an entity that intends to use or use electronic communications networks to store data or gain access to data stored in subscribers 'or users' terminals will be required to obtain **prior provable consent to the scope and purpose of cookie processing**. At the same time, the consent must comply with the requirements of the GDPR.

Max Schrems makes complaints about the processing of cookies in violation of EU rules

Max Schrems, a well-known privacy activist, and his None Of Your Business ("NOYB") initiative, which addresses privacy issues, also address the issue of misused cookies and granting consents to their processing. The NOYB initiative has filed 422 complaints with European supervisory authorities against websites that, according to its survey, processed cookies in violation of GDPR requirements. This was preceded by a screening of up to 10,000 websites. Subsequently, the initiative sent 516 website operators a notification of their errors in the processing of cookies and related obligations, together with a proposal for a complaint that the initiative intended to send to the relevant supervisory authorities in the event of persistent errors. As a result of this intervention, NOYB has seen some improvement in the sites concerned, adding, for example, the ability to refuse processing of non-necessary cookies or removing pre-filled checkboxes that conflict with the GDPR's free and active consent requirement, or adding an icon to revoke a consent that has already been granted. However, only 42% of the notified sites took corrective action, but even these were not consistent in their actions. Therefore, the NOYB initiative has filed 422

Legal Update from the field of

Autumn 2021

Weinhold Legal

complaints with supervisors all across Europe.

In addition, NOYB also focused on the websites of large players (eg Twitter, Amazon, Google, Facebook) and checked the settings of their cookie banners – i.e. bars notifying the processing of cookies by the relevant website. As the NOYB initiative found that the setting of cookie processing is not in accordance with EU law, another 36 complaints are planned to be submitted to the supervisory authorities.

Decison making

Overview of inspections by the Office for Personal Data Protection in the first half of 2021

The Office for Personal Data Protection ("**OPDP**") has published an overview of the first half of 2021 inspections carried out on the basis of the OPDP Control Plan for 2020. Among other things, it carried out inspections in connection with making and keeping copies of identity cards („**ID**“) verification of the client's identity pursuant to Act No. 253/2008 Coll., on Certain Measures against the Legalization of Proceeds from Crime and Terrorist Financing (the “**AML Act**”). The result of the inspection confirms that the OPDP proceeds during the inspections according to the summary material for proving the identity and processing of personal data, which the OPDP published in May 2021 here.

During the inspection, the OPDP found out that the inspected person was copying the client's ID, on the basis of the AML Act, because as a liable person he must perform the identification and inspection of the client. The inspected person distinguishes between two possible variants during this inspection:

1. concluding a contract exclusively by means of distance communication. The client is obliged to send a copy of his identity card and other supporting document to the inspected person in accordance with § 11 par. 7 of the AML Act, from which his identification data can be ascertained in accordance with the AML Act. The legal basis for obtaining a copy of the identity card is therefore **the fulfillment of a legal obligation**.

2. concluding a contract which is not concluded exclusively by means of distance communication. The client presents his identity card to the inspected person, from which the inspected person records his identification data. In these cases, the inspected person obtains a copy of the identity card **only with the client's prior consent**, and **the consent is voluntary; the conclusion of the contract is not conditioned by this consent.**

The retention period of personal data by the inspected person is 10 years and is based on the maximum length of the limitation period pursuant to Act No. 89/2012 Coll., The Civil Code and the AML Act. The inspected person provides information on the protection of personal data, including their processing, on its website, further assessed the severity and probability of risks associated with the processing of personal data and subsequently took technical and organizational measures to ensure a level of security appropriate to the risk. The OPDP did not find any violation of the GDPR.

Unfortunately, in this case, the OPDP does not comment on the "generality" of making copies of IDs by the liable person or on setting up making copies of IDs with regard to the risks of the service provided, i.e. issues addressed in its interpretation of the Financial Guidance Office (FAU) here. In the assessed case, the OPDP assessed the risks only in connection with the technical and organizational measures taken. Nevertheless, the OPDP provides certain guidelines for entities from the financial services and insurance sectors regarding the copying of IDs in the identification and control of the client according to the AML Act.

Legal Update from the field of

Autumn 2021

Weinhold Legal

Fine for WhatsApp

The instant messaging service WhatsApp, as part of Facebook Ireland Ltd, failed to meet its GDPR obligations and was fined EUR225 million by the Irish Supervisory Authority (compared to the original proposal for a sanction in the range of 30-50 million EUR, for which the Irish authority faced criticism from other supervisors). The investigation against WhatsApp has been conducted by the Irish Supervisory Authority since 2018.

The fine alleges breach of the principle of transparency under Article 5 (1) (a) of the GDPR in relation to Articles 12, 13 and 14, where WhatsApp did not properly and clearly inform users how it processes their personal data, including with whom it shares it – specifically, whether and how they share them with other Facebook-owned companies and what rights users have.

The application of Article 83 (3) of the GDPR, which concerns the calculation of fines in the event of a breach of several provisions of the GDPR in the same or related processing operations, was also clarified. That provision provides that the total amount of the administrative fine may not exceed that fixed for the most serious infringement. However, this does not mean that the sanction should be set only for the most serious infringements found and should not take into account other infringements, but these must also be explicitly sanctioned. Therefore, although the overall sanction may not exceed the statutory maximum rate as set out in Article 83 (4) and (5) of the GDPR, infringements of several provisions of the GDPR must be taken into account when determining the amount of the final sanction to be imposed. The decision thus signals a greater move towards establishing uniformity in the enforcement of the GDPR and setting sanctions for its violation in all Member States.

Martin Lukáš
Partner
Martin.Lukas@weinholdlegal.com

Tereza Hošková
Vedoucí advokát
Tereza.Hoskova@weinholdlegal.com

Daša Aradská
Advokátka
Dasa.Aradska@weinholdlegal.com