Legal Update

from the field of

Autumn - winter 2023

Weinhold Legal

EDPB Guidelines on the e-Privacy Directive

The subject of the public consultation are the Guidelines 2/2023 on the technical scope of Article 5(3) of the Directive 2002/58/ES of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector, which were adopted at the November plenary meeting of the European Data Protection Board ("EDPB"). The guidelines were created in response to new methods of tracking in the online environment. Article 5(3) imposes an obligation to ensure that the use of electronic communications networks to store or access information stored on a subscriber's or user's end device is only permitted on condition that the subscriber or user concerned has been clearly and fully informed in accordance with Directive 95/46/EC (on the protection of natural persons with regard to the processing of personal data and on the free movement of such data), among other things, the purposes of the processing, and that he or she is offered the right to refuse such processing by the data controller. While the application of Article 5(3) of the Directive to cookie-based tracking methods is already well established, the Guidelines aim to address new business solutions that are as well covered by this Article of the Directive, e.g. URL and pixel tracking, IP-based tracking, data collected by IoT (Internet of Things) devices, unique/permanent identifiers, etc. The Guidelines focus mainly on the technical analysis of the interpretation of the terms referred to in Article 5(3) of the Directive, such as *information retention*, *obtaining access* to them or *the subscriber's end device* and *electronic communications network*. A detailed analysis of each element is then provided with examples of use. The public has the opportunity to comment on the guidance until 28 December 2023.

The PDPO imposed fines for distribution of commercial communications

The Personal Data Protection Office („PDPO“, „Office“) imposed a fine of CZK 7 700 000 for sending commercial communications in favour of third parties. A shipping company had been engaging in this practice since 2015, when it sent commercial communications to the email addresses of its customers without the prior consent of the recipients.

The outreach was done via e-mail messages. The commercial messages were embedded in e-mail messages containing confirmation of purchase and the recipients had no option to refuse these commercial messages in any way. Other legal requirements arising from Section 7 of Act No. 480/2004 Coll. (on certain information society services), such as the clear and precise identification of such messages or the unambiguous identification of the subject for whose benefit the commercial messages are disseminated, were not complied with either. Due to the nature of the various third-party discount and voucher offers, prior consent of the recipients was required for such dissemination of commercial communications.

It is crucial to stress that the company did not promote its own products or services and therefore could not take advantage of the so called "customer exception", according to which commercial communications can only be disseminated without prior consent to electronic contacts obtained in connection with a previous sale of a product or service for the purpose of offering its own similar products or services.

CJEU on the conditions for imposing administrative fines

On 5 December 2023, the Court of Justice of the European Union (CJEU) issued a judgment in Case C-683/21 Nacionalinis visuomenės zdravot centras and a judgment in Case C- 807/21 Deutsche Wohnen, in which it dealt primarily with the conditions for the imposition of administrative fines by supervisory authorities under the General Data Protection Regulation (GDPR). The CJEU stated, inter alia, that:

On the concept of personal data processing

- Processing means the use of personal data for IT testing of a mobile application, unless the data has been anonymised in such a way that the data subject is not identifiable or the data is fictitious and does not relate to an existing natural person.

On the concept of administrator

- An administrator can be defined as an entity that has commissioned an enterprise to develop a mobile IT application and which, in this context, has been involved in determining

the purposes and means of the processing of personal data carried out through that application. This shall not be prevented by the fact that the subject has not itself carried out personal data processing operations, has not expressly consented to the performance of specific operations of such processing or to the making available of the mobile application to the public and has not acquired the mobile application, unless, prior to such making available to the public, the subject has expressly consented to such making available and the resulting processing of personal data.

On the concept of joint administrators

- In order to be considered a joint administrator, a natural or legal person must individually meet the definition of "administrator" set out in Article 4(7) of the GDPR. Participation in determining the purposes and means of processing may be of various forms and may result from a joint decision of two or more entities as well as from converging decisions of such entities. However, these decisions must be complementary so that each has a specific impact on the determination of the purposes and means of processing. The definition of 'joint administrators' does not assume the existence of a formal agreement between the entities concerned. However, if they are indeed joint administrators, they must establish their obligations by agreement pursuant to Article 26(1) of the GDPR.

On the concept of imposing administrative fines

- The supervisory authority may impose a fine on the controller under Article 83 of the GDPR only in the event of a culpable infringement, either intentional or negligent. If there is no culpability, the supervisory authority is not entitled to impose a fine.
- Sanctions may be imposed for conduct that falls within the scope of the GDPR where the controller could not have been unaware of the unlawful nature of its conduct, whether or not it knew that it was in breach of the provisions of the GDPR.
- A fine may be imposed on an administrator in relation to processing operations carried out by a processor on its behalf, unless that processor has carried out processing for its own purposes in the context of those operations or has processed the data in a manner incompatible with the processing framework or procedures as laid down by the administrator or in such a manner that the administrator cannot reasonably be regarded as having consented to it.
- If the administrator is a legal person, it shall be liable for breaches committed by its representatives, directors or managers, as well as for breaches committed by any other person acting within the scope of its activities and on its behalf. In addition, the imposition of an administrative fine on a legal person as data administrator cannot be conditioned by the prior finding that an identified natural person has committed an infringement. It is not necessary for the breach to have been committed by or be known to the governing body of the administrator.
- As regards the calculation of the fine, where the addressee of the fine is an undertaking or part of an undertaking, the supervisory authority must proceed on the basis of the concept of 'undertaking' as defined in competition law, i.e. any entity carrying on an economic activity, regardless of its legal status and the way it is financed. It denotes an economic unit, even if the economic unit is legally composed of several natural or legal persons. This economic unit consists of a unified organization of personal, tangible and intangible elements that pursues a specific economic objective over a long period of time. The maximum amount of the administrative fine shall be calculated on the basis of the percentage of the total worldwide annual turnover of the undertaking concerned for the preceding financial year.

The CJEU on automated processing

The CJEU issued a judgment in Case C-634/21, OQ v. Land Hessen, intervener SCHUFA Holding AG regarding credit scoring and a judgment in Joined Cases UF C-26/22, AB C-64/22 v. Land Hessen, intervener SCHUFA Holding AG regarding the processing and storage of personal data in cases of insolvency.

The cases concern SCHUFA, a German private company that provides credit information to clients, including banks, and the scoring and storage of debt settlement information extracted from public registers.

Legal Update

from the field of

Autumn - winter 2023

Weinhold Legal

On automated individual decision-making

The CJEU ruled that credit scoring must be interpreted as automated individualised decision-making under Article 22 GDPR, which is prohibited. The Court notes that exceptions are possible if such a decision is essential for credit decision-making, but it must comply with national legislation and the specific requirements set out in Article 22(3) and (4) of the GDPR (appropriate measures, human intervention, the right to express an opinion and challenge the decision) are met. An automated determination by a commercial information agency of a probability value based on personal data relating to a person and their ability to meet future payment obligations constitutes 'automated individual decision-making' if the probability value critically determines whether the third party to whom the probability value is communicated will enter into, perform or terminate a contractual relationship with that person.

On personal data relating to debt settlement

According to the CJEU, it is incompatible with the GDPR for private agencies, such as SCHUFA, to keep personal data relating to the approval of individuals' insolvency from the public register for the purpose of providing information on the creditworthiness of those individuals for a longer period than the period for which those data are kept in the public register. In Germany, this period is 6 months. The CJEU is of the opinion that after these 6 months, the rights and interests of the data subject take priority over the rights of the public to have access to this information. This therefore constitutes unlawful processing of personal data and the data subject has the right to request the erasure of personal data and the controller is obliged to comply without undue delay.

For further information, please contact the partner/manager whom you are usually in contact with.

Martin Lukáš
Partner
Martin.Lukas@weinholdlegal.com

Daša Aradská
Attorney
Dasa.Aradska@weinholdlegal.com