Legal Update from the field of

Spring 2022

Weinhold Legal

ÚOOÚ Annual Report 2021

The Office for Personal Data Protection (ÚOOÚ, the Office) has issued its annual report on its activities for 2021, which presents the most important results of the Office's supervisory activities in the area of personal data processing, illustrated by examples of selected inspections. We summarise some of them below.

Merchant loyalty programmes

The ÚOOÚ audited the loyalty programmes of retail chains. The audit found no serious misconduct. The scope of data collected (most often title, name, surname, date of birth, address, payment details, e-mail address, telephone number, customer card number), the period of storage of personal data and their security were checked. Other information held by the shops related to the goods purchased, the home store, the use of promotions, the amount of loyalty points and other data, which the Office found to be adequate in relation to the purpose of the processing. **However, errors alleged against the inspected sellers concerned the excessive and unjustified retention of personal data -** for example, the retention of data on the purchase of foodstuffs for a period of 3 years was found by the Office to be disproportionate. The Office has therefore recommended that this period be shortened in line with the purpose of the retention of the data (e.g. according to the time when the goods can be claimed).

Telemarketing and personal data

Another area of inspection carried out concerned telemarketing, where approximately a quarter of the complaints received by the Office were complaints about the processing of personal data for marketing purposes. One of the inspected telemarketing companies did not respond to the exercise of the data subjects' right of access to personal data under Article 15 of the General Data Protection Regulation ("GDPR"), or only mentioned the random generation of a telephone number as the source of personal data. Upon objection to the processing of personal data pursuant to Article 21 of the GDPR, or after exercising the right to erasure (or right to be forgotten) pursuant to Article 17 of the GDPR, the company either did not respond at all or promised to stop processing personal data for marketing purposes, but even after the expiration of the one-month period for taking action (pursuant to Article 12(3) of the GDPR), the data subjects were contacted again in the context of telemarketing.

In the course of the inspection of the telemarketing company, the Office found that it acted as a processor of personal data, not as a controller, when it carried out its activities according to the instructions of the controllers for whom it provided the telemarketing service. Furthermore, the company was found to have breached the obligation laid down in Articles 15-21 GDPR by failing to provide data subjects with relevant information concerning the processing of their personal data. Specifically, this breach consisted in the fact that, when providing information to data subjects, it responded in a uniform manner without taking into account the fact that it was in the position of a processor. The company also failed to indicate in its replies to the applicants the purpose of the call, i.e. that the telephone call was made for the purpose of providing a marketing offer to another entity (a contractual client); furthermore, most of the replies indicated that the legitimate interest of the audited person as a controller of personal data was the legal title for the use of the telephone number, which was not the case here.

Personal data protection impact assessment

A personal data protection impact assessment pursuant to Article 35 of the GDPR is to be carried out by **any controller whose processing intention can be assessed as high risk** in terms of interference with the rights and freedoms of natural persons in relation to the processing of their personal data. In its report, the Office draws attention to the mistakes made by controllers in this assessment:

- the balancing test is carried out in such a way that it is not possible to verify the necessity, suitability and proportionality of the processing of personal data;
- the description of the safeguarding of the rights of data subjects is missing or insufficiently elaborated;
- the description of the technical and organisational measures adopted is often general and it is often not clear how the administrator arrived at their design (the methodology developed by the OOOÚ is not used and the administrator's own methodology is not clear); the consequence is that it is not possible to verify whether the measures adopted are adequate and complete.

Legal Update from the field of

Spring 2022

Weinhold Legal

Guidelines EDPB 05/2022

The subject of a public consultation until 27 June 2022 is the European Data Protection Board's ("EDPB") Guidelines 05/2022 **on the use of facial recognition technology in the area of law enforcement** within the meaning of the Law Enforcement Directive (EU) 2016/680 ("the Directive"). The Guidance is based on the current situation where an increasing number of law enforcement authorities are using or intend to use facial recognition technology (e.g. to identify or verify a person). The guidelines also contain the EDPB's position on this issue, which is based on the joint opinion of the EDPB and the European Data Protection Supervisor 05/2021 on the draft Regulation on artificial intelligence. In the opinion, these institutions jointly call for a ban on the use of facial recognition technology for certain purposes (e.g. biometric identification of persons remotely in public space or assessment of a person's emotions).

The EDPB states that facial recognition technology involving the processing of biometric data constitutes a serious interference with privacy rights and also with the protection of personal data. The EDPB recalls that the data protection requirements of the Directive must of course be fully respected (clear legal basis; consultation of the data protection supervisory authority; necessity and proportionality assessment; data minimisation, etc.). It also recommends the publication of the results of the mandatory data protection impact assessment under Article 35 of the GDPR.

Guidelines EDPB 1/2021

EDPB adopts final version of Guidelines 1/2021 on examples regarding **Personal Data Breach Notification**. The guidelines are intended to help data controllers decide how to deal with personal data breaches and what factors to consider when assessing the risk. The contribution of the guidelines is that, for each practical example, they describe the measures taken by the controller before a breach occurs to avert the risk of a breach and the measures that will help to reduce the risk to the rights and freedoms of data subjects afterwards. In addition, each example includes a risk assessment, an evaluation of the steps to be taken to avert the risk and recommended organisational and technical measures to minimise the risk.

Martin Lukáš
Partner
Martin.Lukas@weinholdlegal.com

Tereza Hošková
Managing Attorney Tereza.Hoskova@weinholdlegal.com

Daša Aradská
Attorney
Dasa.Aradska@weinholdlegal.com