OVERVIEW OF DATA PROTECTION ISSUES

Jeseniova 1151/55 130 00 Praha 3 +420 212 246 725 info@ak-haven.cz www.ak-haven.cz

HAVEN
ADVOKÁTNÍ KANCELÁŘ

In the following overview, we would like to inform you about the recent decisions of the Office for Personal Data Protection (ÚOOÚ), the conclusions of its inspections and other new developments in the area of personal data protection. We will inform you about further information on the legal protection of personal data in the next edition of this overview or in the legal news overview.

Opinions

+ EDPB on credit card data

The European Data Protection Board (EDPB) has adopted a Recommendation on the legal basis for the retention of credit card data for the sole purpose of facilitating other transactions. In this document, the EDPB concluded that even in the case of credit cards, the controller must have a valid legal basis for processing personal data under Article 6 of the General Data Protection Regulation (GDPR). However, not all processing titles mentioned in Article 6 are applicable. **The processing of data relating to the client's credit card is necessary to make the payment and fulfil the contract**, but its further storage is only useful to facilitate other possible transactions and sales. Such a purpose cannot be considered necessary for the fulfilment of a contract for the supply of goods or services that have already been paid for. In addition to the processing of data for the purpose of the performance of a contract, the EDPB allows, in the case of credit cards, the processing of data only on the basis of the consent of the cardholder, which, moreover, must not be implied by the controller and must be given by the cardholder in a clear act reflecting the fact that he has given his consent freely, definitely, informedly and unambiguously. At the same time, the data subject shall always have the right to withdraw the consent thus given.

+ ÚOOÚ on the issue of making copies of ID cards under the AML Act

In relation to the interpretative ambiguities that arose in connection with the issuance of the Financial analytical office's (FAÚ) methodological instruction on the issue of making copies of identity cards for the purposes of anti-money laundering measures, which should have been issued with a positive opinion of the ÚOOÚ, the ÚOOÚ stated that the FAÚ's methodological instruction concerned the state of the legal regulation of the Anti-Money Laundering Act before the amendment. After the amendment of the AML Law, the ÚOOÚ's position is that the **acquisition of a copy of an identity card is merely an option and not an obligation. The obliged entity must always carry out a risk assessment beforehand and only after that, if necessary, proceed to obtain a copy of the identity card** if it becomes aware that there are risks in providing the service to the client. The ÚOOÚ clearly concludes that making copies of identity cards at any time and in any circumstances is not a desirable practice, particularly when concluding current account contracts.

HAVEN
ADVOKÁTNÍ KANCELÁŘ

+ Summary material of the ÚOOÚ on proving identity and processing personal data

On the basis of a number of audits, the ÚOOÚ compiled and published a summary material on the issue of identity proofing and personal data processing. The following conclusions, among others, can be drawn from this document:

- **Consent to take a copy of the ID card must be given on a separate document** - if the contract contains a provision that by signing it the data subject grants the other party the right to take a copy of his/her ID card, the provision does not meet the requirement of a duly given consent.
- Anyone who is asked to allow a copy of their identity card to be made should first of all ask whether the request is made by law/regulation or whether the copy is to be made on the basis of voluntary consent, what the controller's reasons are for doing so and what the consequences of withholding consent are. He may also enquire whether mere production of the identity card is not sufficient without making a copy of the same.
- The municipal office of the municipality with extended jurisdiction is competent to hear a complaint about the unauthorised acquisition of a copy of an identity card. However, a violation of the principle of minimisation by storing a complete copy of the ID card is a violation of the GDPR and the ÚOOÚ is therefore competent to assess it.

From the decision-making practice of the ÚOOÚ

+ TV reports from the school environment

The decision of the President of the Office of 15 March 2021, No. UOOU-04272/20-17, confirmed the decision by which Czech Television (ČT) was found guilty of an offence under the Personal Data Processing Act for violating the GDPR by broadcasting a report entitled "*Some schools handing out report cards*" on the ČT24 programme in the morning hours at the end of June 2020, which was subsequently made available on the ČT website. The report was filmed live, during which the camera took a close-up of a particular pupil's report card, which showed her name, surname, date and place of birth, birth number and grades in each subject for each term. The minor's parents stated that they had been informed in advance of the filming but had not given their consent to the publication of their daughter's personal data. ČT defended itself by saying that it had already removed the report from its website and that, by setting up its internal procedures, it had made every effort that could be required to prevent the offence. However, in the opinion of the Office, ČT had not made such efforts when, despite its internal procedures, the incident occurred. The fact that the reportage was not negative and that the filming took place in the presence of a teacher does not affect ČT's liability. The **school establishment is not liable for such misconduct**.

HAVEN
ADVOKÁTNÍ KANCELÁŘ

+ Liability for unsolicited commercial communications sent due to human error

The complainant contacted the ÚOOÚ, stating that he had sent an e-mail to the accused company objecting to the processing of his personal data and at the same time requesting its deletion. Despite this, he was subsequently sent an SMS with a marketing offer. The company defended itself by saying that it had deleted the complainant's data from the automated systems as he had requested, but that the re-sending of the marketing offer was due to human error, when the company had the commercial communication sent manually, without the use of automated systems, for operational reasons. The President of the ÚOOÚ ruled on the company's appeal on 31 May 2021 in his decision, No. UOOU-03580/20-23, that there was clearly no destruction of the complainant's personal data when the company re-contacted him with the marketing offer, even though this was due to human error. The President of the Office pointed out that, according to Article 4 (2), processing means any operation on personal data, whether or not it is carried out with the aid of automated systems. Processing of personal data therefore includes the manual sending of commercial communications by SMS.

In practice, such incidents happen quite often. Therefore, the ÚOOÚ recommends that companies verify before each mailing whether their database of electronic contacts for sending commercial communications actually contains only contacts of their customers who have not at the same time refused to receive commercial communications. At the same time, each commercial communication must contain information on how to refuse the commercial communication free of charge and easily. Failure to do so could result in a fine of up to hundreds of thousands of crowns.

From the audit activities of the Office of the Inspector General for the Protection of Human Rights and Fundamental Freedoms

+ Camera system installed in the kindergarten

On the initiative of one of the parents, the ÚOOÚ inspected the CCTV system installed inside the kindergarten building so that the cameras were covering the area of the changing rooms where the children were changing clothes. The ÚOOÚ found that by installing the cameras in this way, the kindergarten had violated the controller's obligation to process personal data on the basis of one of the permitted titles under Article 6 of the GDPR. By processing the personal data of children and their parents without a legal title, the kindergarten violated the principle of lawfulness of processing enshrined in Article 5 of the GDPR. The school removed cameras from all changing rooms during the inspection and no remedial action was imposed.

HAVEN
ADVOKÁTNÍ KANCELÁŘ

+ Involvement of the Data Protection Officer

In the course of an audit at a certain ministry, the ÚOOÚ found a breach of Articles 38 and 39 of the GDPR, according to which the controller is to ensure that the Data Protection Officer is properly and timely involved in all matters related to the protection of personal data and to provide him/her with the resources necessary for the performance of his/her tasks, as well as to allow him/her access to personal data and processing operations. The audit found that the Data Protection Officer in the Ministry concerned was not involved in the envisaged processes. He was not provided with the information necessary for the performance of his duties (e.g. audit reports). In addition, the Ministry did not provide the delegate with sufficient staff and time resources to carry out his duties, nor did it ensure that his expertise was maintained when he was consistently assigned other tasks unrelated to his work. The Ministry has already taken steps to remedy the deficient situation.

NEJSTE NA TO SAMI
YOU'RE NOT ALONE
SIE SIND NICHT ALLEIN

www.ak-haven.cz