Legal Update
from the field of

Winter 2021/2022

Weinhold Legal

Guidelines on local jurisdiction and transfer of personal data

The European Data Protection Board ("EDPB") issued **Guidance 5/2021** on the interaction between the application of Article 3 and the provisions on transfers of personal data to third countries outside the EU/EEA under Chapter V of the General Data Protection Regulation ("GDPR"). A public consultation on the Guidelines was held until 31 January 2022.

The Guidelines are intended to assist controllers and processors in the EU in identifying whether a processing operation constitutes a transfer of personal data to third countries, as the GDPR does not provide a legal definition of the term "transfer of personal data to a third country or international organisation". The criteria are three and must be met simultaneously:

1. the data exporter, i.e. the controller or processor, is subject to the GDPR for the processing in question;
2. The exporter transfers or discloses personal data to the data importer (another controller, joint controller or processor);
3. The importer is located (established) in a third country or is an international organisation.

The processing will be considered a transfer, regardless of whether the importer established in the third country is subject to the GDPR under Article 3.

However, the EDPB considers that the collection of data outside the EU/EEA directly from data subjects on its own initiative does not constitute a transfer of personal data outside the EU/EEA.

Guidance on the right of access to personal data

The EDPB has issued Guidelines on Right of Access 1/2022. They analyse different aspects of the data subject's right of access to data processed about him or her and provide guidance on how the data controller should provide access to the data subject in different situations. The guidelines clarify, inter alia, the scope of the right of access, the information that the controller must provide to the data subject, the format of the access request, the main ways of providing access and the concept of manifestly unfounded or unreasonable requests. A public consultation on the guidelines is open until 11 March 2022.

Guidance on examples of personal data breaches

The EDPB issued Guidance 1/2021 on examples of security breaches after public discussion. The guidance is intended to assist data controllers in deciding how to handle personal data breaches and what factors they need to consider when assessing the risks.

Status of entities in the provision of financial intermediation services

(Judgment of the Supreme Administrative Court of the Czech Republic of 7 October 2021, Case No. 7 As 146/2021)

Legal Update
from the field of

Winter 2021/2022

Weinhold Legal

The Supreme Administrative Court of the Czech Republic ("SAC") decided on the cassation complaint of SMS finance, a.s. ("the claimant" or "the complainant") against the decision of the Municipal Court in Prague ("the Municipal Court"), in which it dismissed the claimant's administrative action against the decision of the Office for Personal Data Protection ("OPPD") for lack of merit. It dealt with the question whether the administrative authorities were justified in considering the claimant to be a personal data controller under Article 4(7) of the GDPR.

In this respect, the SAC agreed with the opinion of the Municipal Court. That is to say, with the opinion that **the claimant was in the position of a controller of personal data in the given case, as it determined the purposes and means of processing personal data.**

The claimant designated the person Ing. L. Š., as a bound agent within the meaning of Section 15 of Act No. 170/2018 Coll., on the distribution of insurance and reinsurance, who mediated the claimant's services, in the context of which personal data of potential clients were collected and processed precisely for the purposes determined by the claiment. The processing of personal data prior to the introduction of the complainant's services is already carried out for the purpose of offering those services. The complainant had with Ing. L. Š. only concluded a commercial representation contract, not a processing contract, and argued that she was an independent entrepreneur and that, at the initial stage of approaching a client, she processed the personal data of the data subjects in order to build up her own customer network, which she would then offer her own services (financial advisory services) as part of her business activities, whereas the offering of the complainant's services only took place subsequently and not always.

By the appeal, the claimant contested the legal opinion of the OPCU that he is a data controller. The OPCU imposed remedies on the claimant, namely the obligation to secure the legal titles for the processing of personal data of all data subjects in respect of whom it is a controller, i.e. where it has itself determined the purpose and means of processing in accordance with Article 6 GDPR, and in the event that such security is not possible for a data subject, then it is to erase the personal data of that data subject within 3 months of the legal force of the decision. The OPCD also ordered the claimant to conclude processing contracts with the entities that perform personal data processing tasks for him, so that they have the proper legal title for the personal data processing tasks.

The remonstrance was rejected and the claimant challenged the decision on the remonstrance by administrative action. The decision was subsequently upheld by the municipal court, against which the complainant lodged a cassation complaint. The SAC recalls that the reason for **regulating the relationship between the controller and the processor** (in particular on the basis of a specific contract pursuant to Article 28(3) GDPR) is precisely the fact **that it is a relationship between two otherwise independent entities**. The legislation considers the controller to be the one who determines the purposes and means of the processing of personal data. The processor is then the one who processes the personal data for the controller. It is only to the complainant's detriment that he did not effectively ensure that Ing. L. Š. to transmit the personal data.

The SAC thus confirmed the conclusion of the OPPD that the **complainant is in the position of a controller also in relation to the personal data processed for it by the so-called independent financial services intermediary, as it has determined the purpose of such processing**.

Legal Update
from the field of

Winter 2021/2022

Weinhold Legal

Liability for data leakage is not always absolute

(Judgment of the Supreme Administrative Court of the Czech Republic of 11 November 2021, Case No. 1 As 238/2021)

The SAC considered the question of whether the applicant had committed an offence under Section 45(1)(h) of Act No.101/2000 Coll. on the Protection of Personal Data ("PDPA") by failing to take measures to ensure the security of the personal data processed pursuant to Section 13(1) of the PDPA, which stipulates that the controller and the processor are obliged to take such measures to prevent unauthorised or accidental access to personal data, their alteration, destruction or loss, unauthorised transfers, other unauthorised processing, as well as other misuse of personal data. This obligation continues to apply after the processing of personal data has been terminated. In the present case, the OPPD found the applicant, Internet Mall, a.s. ("the claimant" or "the complainant"), guilty of an offence by failing to take measures to ensure the security of the personal data processed. Specifically, it failed to secure the personal data of at least 735,956 customers (in the scope of their name, surname, email address, user account password, or telephone number) from unauthorised access in the period from at least 31 December 2014 to August 2017, which resulted in their disclosure by an unknown hacker on the website www.ulozto.cz between 27 July 2017 and 25 August 2017. For the commission of the above offence, the OPPD imposed a fine of CZK 1,500,000. The applicant lodged an remonstrance against the first-instance decision, which was rejected.

Subsequently, the applicant defended himself by bringing an administrative action, which was dismissed by the Municipal Court. In the cassation complaint lodged with the Supreme Administrative Court, the applicant (the complainant) argued that the municipal court proceeded on the basis that the offence under the cited provision is construed as liability for the consequence of compromising the security of the personal data processed. That interpretation is contrary to the text of the law and the intention of the legislator. The provision in question is based on the norms of European law, whose authors were aware that all security measures are always behind any threats, so that antivirus or other software means will never provide 100% protection. The interpretation applied by the City Court would mean that all entities that were victims of such [cyber] attacks would be guilty of an offence, regardless of the measures they actually took. The complainant argued that, under section 13 of the PDPA, **it was not the duty of the data controller to take all conceivable measures to protect the data.** This interpretation, according to the complainant, also corresponds to the text of the GDPR, which does not require the adoption of all possible measures but speaks in Articles 24 and 32 of the GDPR of appropriate measures and an appropriate level of security.

According to the SAC, in the present case it was not disputed that the complainant had not prevented unauthorised access to the personal data of more than 700 000 of its customers. He only discovered the theft of the data after a considerable time lag, following its publication on the website. However, he considered that both the defendant OPPD and the municipal court had misinterpreted the provisions of the PDPA and insisted that it was the OPPD's duty to **investigate what measures the complainant had taken to prevent unauthorised access to personal data.**

The SAC concluded that **the responsibility of personal data controllers and processors is not absolute, but**

emphasizes that the entities concerned must make reasonable efforts to protect personal data and cannot be held liable for any (often unlawful or even criminal) activity of other entities. The security measures taken can hardly be expected to be strong enough to repel a sophisticated and targeted cyber-attack. The Court of Cassation recalls that **the decisive factor for liability for an offence is not whether or not personal data are ultimately protected, but whether a deficiency in the adoption of the appropriate measures to protect them is established.** In the present case, the unauthorised access to personal data was clearly the result of a targeted unlawful act by another entity. While the complainant must have foreseen such conduct, he cannot automatically be held liable for it, irrespective of the measures he took to protect the personal data and the sophistication of the attack by the unknown person who stole the data from the database. The SAC therefore agreed with the complainant and proceeded to annul the contested administrative decision. It will thus be up to the OPPD to take into account all the **measures taken by the complainant** and to consider whether **they were sufficient in view of the level of protection available at the relevant time, the nature of the complainant's activities and the scope of the data processed by the complainant.**

We regularly inform you about other GDPR news on social media. Follow us on LinkedIn and Facebooku.

Martin Lukáš
Partner
Martin.Lukas@weinholdlegal.com

Tereza Hošková
Vedoucí advokát
Tereza.Hoskova@weinholdlegal.com