DAGITAL LEGAL
Privacy & Technology Law Firm

Report on Personal Data Protection 2020

Slovak Republic

Published 23.1.2021

Dear clients and colleagues,

We received several requests from you to summarize the events that took place in Slovakia in the field of personal data protection in 2020. We have decided to meet this challenge, especially as a demonstration of gratitude for our cooperation over the past year. We greatly appreciate the trust of our clients, which allow us to specialize in the field of law, which has a long-term perspective and which we enjoy specializing on professionally.

We believe that this gesture will also help move the discussion in this field in the right direction.

We wish you much success in 2021.

- Your Dagital Legal team

NAVIGATION

0911 195 133 jakub.berthoty@dagital.eu www.dagital.sk Nové Záhrady I/9, 821 05 Bratislava

As you surely know that the Office for Personal Data Protection of the Slovak Republic (the "**Office**") issues annual reports, which, however, cover the period between 25 and 24 May of the following year since the GDPR started to apply. These annual reports cover more-less statistics of the Office's activities. In this report, we look at developments from a broader perspective and describe, from our perspective, key events divided into the following categories:

(i) legislative events;
(ii) decisions of the Office;
(iii) case-law of the courts; and
(iv) other activities of the Office.

Our goal was to record as many events as possible, however it is not in our capacity to describe all events. Should you miss an interesting event in this report, please let us know. We will be happy to add it in.

1. Legislative events

The COVID-19 pandemic has brought much greater public and media pressure on the quality of legislation in general, but also in relation to the protection of personal data and privacy. In March, a group of opposition deputies challenged an amendment to § 63 of the Electronic Communications Act of Slovak Republic at the Constitutional Court of the Slovak Republic. Based on the Resolution of the Constitutional Court of the Slovak Republic, the scope of data provided by telecommunications operators to the Public Health Office of the Slovak Republic was narrowed.

The Slovak Public Health Protection Act (Act No. 355/2007 Coll.) has been amended several times during the year, with the largest amendment from the perspective of personal data protection concerning the use of mobile applications to monitor compliance with domestic quarantine and contact tracking. The new separate part of the Act (§ 60a to § 60e) was an attempt to introduce the requirements of legal regulations under Art. 6 (3) GDPR and at the same time an attempt to introduce guarantees for the protection of the rights and freedoms of the data subjects. This amendment was not challenged before the Constitutional Court of the Slovak Republic, nor was it challenged in practice by the Office. Later, based on this, the Office also made an inspection of the application of quarantine. Finally, this amendment attracted interest in the Czech Republic, when adopting a similar regulation.

Another intended amendment to the Electronic Communications Act, which planned to introduce an obligation for mobile operators to provide telephone numbers to the Public Health Office of the Slovak Republic and the high-risk countries visited by data subjects, the president did not sign.

By 21 December 2020, all Member States were required to implement Directive 2018/1972 called the "European Electronic Communications Code", which will serve as a basis for terminology and framework to be yet introduced by the new ePrivacy Regulation. Although we got information in April that there should be a working group working on the topic of ePrivacy at the Ministry of Transport, Posts and Telecommunications of the Slovak Republic, to this date the Directive 2018/1972 has not been implemented and neither the inter-ministerial comment procedure has been initiated.

Overlap between the GDPR, the Public Health Protection Act and the Electronic Communications Act over the past year reflected that there is no independent body in Slovak Republic with ability to ensure that national legislation complies with regulations such as the GDPR and the ePrivacy Directive. This agenda is addressed on an *ad hoc* basis, centrally unmanaged by the state and without a budget for public authorities, which was confirmed by the Supreme Audit Office of the Slovak Republic in its report. The Office's advisory role in adopting legislation is failing. In Slovakia there is a lack of a supervisory officer, following the example of the European Supervisory Officer (EDPS), who would assist the responsible state persons in a unified approach.
It is alarming that more than four years after the adoption of the GDPR, the legislative data protection impact assessment (DPIA) according to Art. 35 (10) GDPR is not part of Slovak legislative process. According to the Czech Office, it should be part of the general part of the explanatory memorandum.

2. Decisions of the Office

There is no comprehensive access to all decisions of the Office. Some of the decisions are published, but most of them do not reach the public, especially if the participants in the administrative proceedings do not use the appeal and then do not file an administrative court action. Through the public information access act, we managed to gather several decisions during the year, and we summarize selected ones below. Most of these decisions already concern the processing of personal data under the GDPR regime after 25th May 2018, but some processing activities have still begun under the previous regime of the Act No. 122/2013 Coll. In case of private entities, we prefer not to mention their business names. However, if you are interested in a decision, we are happy to send a copy of the decision by request.

Party	Summary of the decision	Fine
Bratislava Public Transport Company	The fine was reduced from the original EUR 29,800 after the appeal and was imposed in connection with CCTV systems in public transport vehicles and public transport passenger stops. The infringements concerned: a) the failure to link the simple 'monitored space' notice to more detailed privacy policy on the website; b) retention period unduly long - in one case the record was stored 23 days with a retention period of 15 days; c) the range of the monitored area was reportedly unnecessarily wide and also covered the surrounding public space and non-passengers. The Office did not accept the public transport company's objection that: a) it is the only and notoriously known public transport provider in Bratislava and therefore every passenger knows where to find additional information; b) it was the only one case of non-erasure, not a a system-wide fault; c) the technical standard stipulates the length of platforms and it is not possible for cameras not to detect the boarding edge of passenger stops. It is interesting that in the decision the Office also tried to question the right of the transport company itself to ensure public order and prevent crime, however Office did not impose a fine for the lack of a legal basis.	EUR 20,000
Bratislava Public Transport Company and debt collection company	In November 2017, during the public tender, the Bratislava Transport Company made available to four applicants and the auction administrator a list of 30-40 thousand company claims with the personal data of individual debtors (unpaid travel tickets). After public tender the claims were transferred (sold) to the company, which began recovery debt. The fine was imposed for the absence of a legal basis for the given disclosure pursuant to Section 9 of Act No. 122/2013 Coll. The public transport company was not able to prove that the given disclosure of data was executed on the legal basis of a special regulation, to which the registration sheet of the information system referred without its specification. Neither the transport company nor the Office have dealt in detail with the existence of a public or legitimate interest, while being practically the only usable legal basis.	EUR 10,000
Insurance company	Insurance company received a fine for violation of Section 12 (3) GDPR on the grounds that company did not handle the request of the data subject without undue delay, at the latest within one month from the submission. Delayed response was caused by the negligence and failure of a particular employee. The Office also imposed a corrective action to retrain employee. The original fine of EUR 10,000 was reduced to EUR 9,000.	EUR 9,000

Party	Summary of the decision	Fine
Private company	The part of the accounting documents of a private company intended for shredding was found by a citizen in a readable form near the waste collection yard, while it was freely accessible to the public and contained a large amount of personal data. The Office assessed the procedure as a data protection breach and at the same time a breach of an adequate level of security in the destruction of personal data.	EUR 7,000
Primary school	A fine was imposed to a primary school for: a) publishing a video on YouTube with pupils of a school without a legal basis; b) providing third parties with photographs of pupils without a legal basis, as a result of which they could be found on other foreign websites; c) publishing the names and surnames of eleven pupils on the cover of the motivational school CD without parental consent; d) lack of documented instructions pursuant to Art. 29 GDPR in relation to the publication on YouTube; e) not handling the requests of the data subjects - parents.	EUR 6,000
Grocery retail chain	The grocery retail chain was fined for violating Art. 12 (3) GDPR on the grounds that it did not handle the data subject request without undue delay, at the latest within one month from the submission. Delayed response was caused by the negligence and failure of a particular employee. However, in the decision, the Office did not question the legal basis of the performance of the contract and the legitimate interest in relation to the personal data on the loyalty card. The same fine for a similar violation was confirmed by the Office to another grocery retail chain.	EUR 3,500
Municipality	According to the Office, a municipality without a legal basis published on its website the personal data of a person with a position in the municipality and at the same time the municipality did not fulfill its obligation to nominate and publish contact details of the data protection officer. The Office acknowledged that the citizens of the municipality had the right to be informed about the dismissal of the person from public office, but in order to fulfill this purpose, according to the Office, it was not necessary to disclose the person's place of permanent residence. In another municipality, the office imposed a fine of EUR 4,000 for the publication of birth numbers as part of the obligation to publish agreements in public sector.	EUR 3,000
The auction company	The auction company, which operated a website with an overview of auctioned real estate was fined by the Office for publishing photographs of the interior of a family house, which captured photographs of family members placed above the fireplace without a legal basis. The concerned photographs were also part of the expert opinion. The auction company did not correct this failing by the request of the data subject.	EUR 3,000

Party	Summary of the decision	Fine
Financial agent	The financial agent violated the principle of legality by not having a legal basis for telephone nuisance call to a person, who was not an existing client. During the telephone conversation, the financial agent allegedly had information on the data subject´s existing insurance products, but later denied this information in a statement. The financial agent apparently obtained contact information by informal recommendation from other clients and recorded it only on paper (without keeping it in electronic form). The legal basis should have been a legitimate interest with reference to Section 5 (2) of the Financial Intermediation Act, which defines a "potential client". The Office did not accept this argument as there were no reasonable expectations of the data subject about possible processing of data. At the same time, the financial agent violated Art. 12 (5) GDPR by requiring a certified signature on the data subject request. Interestingly, the fine was imposed only for the certified signature, not for the legal basis. It is possible that the Office did not impose fine due to § 62 of the Act on el. communications, which should fall within the power of the "telecommunications office". This provision is not even mentioned in the decision of Office.	EUR 2,600
Municipality	The municipality was fined for publishing through the minutes of the municipal council meeting, the birth number of the data subjects with whom the municipality concluded a donation contract, without a legal basis. These minutes were published on the municipality's website as well as on the municipality's official notice board. The original fine of EUR 3,000 was reduced by an appeal.	EUR 2,500
E-shop	The controller was fined for not having a legal basis for processing of personal data of unregistered visitors to its e-shop for marketing purposes. The pre-marked box from the newsletter was not accepted by the Office as a valid consent. In this decision, the Office also confirmed that lawyers and law firms with reference to Section 18 (6) of the Advocacy Act typically act as independent controllers, not data processors.	EUR 2,500
Provider of aesthetic medical services	The controller was fined, among other things, for not providing information to data subjects during obtaining consent, including the possibility to withdraw consent at any time, for the lack of purpose of processing in the data processing agreement and for failure during "giving consent to use photo documentation" that was part of medical records.	EUR 2,100
City	The city published the personal data of the data subject on its website as part of the mandatory publication of contracts. The Office accessed the processing without a legal basis. The city admitted that it was a violation of personal data protection due to a technical error. The Office also imposed a fine in a similar amount for the disclosure of personal data within the framework of compulsorily published contracts to other municipalities or cities.	EUR 1,000

Party	Summary of the decision	Fine
Bratislava Public Transport Company	The public transport company did not handle data subject request for access to data, in particular to camera recordings, due to inappropriate behavior of the ticket controller, as it followed other regulations and disciplinary procedures and not data subject request procedures. The Office assessed the procedure as non-compliance with the request of the data subject.	EUR 1,000
Grocery retail chain	The controller was fined for use of 4,500 employee emails by a third party as a result of a cyber phishing attack.	EUR 1,000
Political party	The Office imposed a fine on a political party for failing to manage the data subject request within the required time limit.	EUR 700

It seems that the most frequently fined entities by the Office in 2020 were municipalities and cities. This is probably related to the fact that municipalities and cities were one of the first in the Office's control plan after GDPR entered into force. These decisions only entered into force in 2019 and 2020. According to our information, the highest fine imposed to the city in 2019 was in amount of EUR 10,000 and was related to transparency and information obligations in relation to the CCTV system.

In addition to the above, municipalities and cities were also fined (in the range of EUR 300 to EUR 3,000) for breaches related to the disclosure of personal data in mandatorily published contracts, municipal magazines or information portals and bulletin boards. Municipalities often publish information for example on jubilees, newborns or deceased persons, without having specific purpose of data processing, legal bases and information obligations adapted to these processing activities. This decision-making practice does not mean that the GDPR prohibits such processing activities in general. However, it is problematic for municipalities to ensure standard compliance in similar situations.

The Office also imposed several disciplinary fines for repeated non-compliance with the request for assistance in the amount of EUR 500.

At the same time, decisions of the Office show that many controllers do not use legal representation by attorneys during inspections and proceedings. In several cases, there was no appropriate legal argumentation that would make it difficult for the Office to make a decision and therefore it is not necessary to generalize all the Office's conclusions from decision-making practice. Rather, they need to be taken as an illustration of the Office's initial approach in practice. The second-instance decisions of the Office Chairman generally confirmed the first-instance decisions, while at the same time they usually slightly reduced the imposed fines.

3. Case-law of the courts

Having regard to the average length of Slovak courts proceedings, it still premature to expect case-law with interpretation of GDPR as early as in 2020. However, there are some indications that such case-law will gradually come. These would primarily be decisions of administrative courts arising from administrative actions against decisions of the Office or other administrative acts[1], but it is possible to expect decisions of courts in civil and commercial disputes in the future. We should not forget that the right to an effective judicial remedy directly against the controller and the processor is stipulated in Art. 79 GDPR[2]. However, in Slovak case-law, the conflict between the Access to Public Information Act (the right to information) and the personal data protection is still the most significant source of disputes. Until now this case-law has most shaped the perception of the definition of personal data by the courts.

Regional Court in Bratislava (1S / 280/2017): Info-request for access to data from the vehicle register of the Ministry of the Interior of the Slovak Republic

Brief summary: The law of another Member State applicable to a foreign controller cannot be the legal basis for the provision of personal data by a Slovak controller, if Slovak law requires the consent of the data subject.

Summary: On 12 March 2020, the Regional Court in Bratislava resolved a dispute concerning access to personal data of motor vehicle holders from the vehicle register of the Ministry of the Interior of the Slovak Republic through an application based on the Access to Public Information Act. The requested personal data included name, surname, address of permanent residence and date of birth, as well as other information about the vehicle. The Ministry of the Interior of the Slovak Republic rejected this request with reference to Section 113 of the Road Traffic Act and Section 9 }(2) of the Access to Public Information Act, according to which the consent of the data subject would be required for such a procedure. The applicant was a Hungarian legal entity established by the Hungarian Road Traffic Act, according to which the applicant is authorized to collect tolls for the use of motorways and roads, respectively recover the debts. The applicant argued that the above cited article with restrictions should not been applied, because the Ministry of the Interior of the Slovak Republic shall provide personal data from these records directly on the basis of Section 10 (2) and Section 10 (3) (g) of Act No. 122/2013 Coll. on the protection of personal data which take precedence. The applicant wanted to include Hungarian Road Traffic Act in the legal bases defining its status as a controller, in accordance with those provisions. The Regional Court in Bratislava dismissed the action and supported the Ministry of the Interior of the Slovak Republic. We select interesting quotes from the decision:

"The relationship between the obliged entity and the applicant is a vertical relationship and proceedings within the meaning of the Access to Public Information Act are a special type of administrative proceedings. It is based on the principle of a general clause with a negative enumeration, which means that obliged entity may disclose all information, except for those for which this is prohibited by law. However, the prohibition need not be explicitly given directly by the Access to Public Information Act, but may also result from other public law."

1) The Supreme Administrative Court of the Czech Republic in its judgment file no. 9 Azs 49 / 2018-50 of 9 August 2018 ruled that the measure of the Ministry of the Interior of the Czech Republic, by which it rejected the data subject request, is a measure that can be reviewed by an administrative court action. What was important, however, was that it was a public authority which dealt with the request of the person concerned in the exercise of official authority. Of course, a private controller's decision would not be subject to review by an administrative court action. The question is whether the same conclusion would apply if it were a public authority but the request would relate to purposes unrelated to the exercise of public authority (for example PR or marketing purposes).
2) Art. 79 GDPR (Right to an effective judicial remedy against a controller or processor): 1. Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation. 2. Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.

"*The right to information is one of the guarantees of legality in relation to public administration, which would be considerably limited in the case of an extensive interpretation. Obviously, this right is not absolute, but is limited by the restrictions arising from the need to protect legitimate public interests, including the protection of personal data.*"

'The right to the protection of personal data also guarantees the right of an individual to decide at his own discretion, whether at all, or to what extent, method and under what circumstances information about its person should be made available to another entity. This aspect of this right is reflected in Article 19 (3) of the Constitution guaranteeing the individual the right to protection against unauthorized collection, disclosure or other personal data abuse. Thus defined fundamental right, together with personal freedom in the area dimension and other constitutionally guaranteed fundamental rights, completes the personal sphere of the individual, whose individual integrity shall be respected and protected. If an individual is not guaranteed the ability to control the content and scope of personal data and information provided by him or her to be disclosed, stored or used for purposes other than original, he or she will not be able to recognize and assess the credibility of the potential communication partner and adapt the behavior accordingly. This i will be inevitably followed by restriction or even suppression of his rights and freedoms, which is not acceptable in a free and democratic society (Federal Constitutional Court of the Federal Republic of Germany of 15.12.1983, file no. BVerfGE 65, 1 Volkszählungsurtel. In: Pl. ÚS ČR 42 / 11)."

Supreme Court of the Slovak Republic (6Sžik / 3/2019): Info-request for access to data on pending consumer disputes before the district court

Brief summary: If certain information is related to limited liability company with a sole shareholder and managing director, which would be the same natural person, in a certain context, then it could be personal data if the information in everyday life concerns in fact only this natural person. However, this depends on the circumstances of the specific case and the intended use of the data. (taken from 10Sžik/2/2017)

Summary: Pursuant to the info-law, the civic association for consumer protection requested the Bratislava IV District Court for information on pending court proceedings against selected banks, including personal data of natural persons in consumer disputes. The District Court did not comply with this request with the argument that it is not a request under the Info-Act rather a request aimed at the administration of justice, which is to be administered by Decree No. 543/2005 Coll. The applicant argued that the other party to the dispute is a legal person (at least), it should not be personal data that would be subject to the consent required under the info-law. By a judgment of 15 October 2020, the Supreme Court of the Slovak Republic confirmed the judgment of the district court and dismissed the action in full range. In argumentation of Supreme Court basically took over an earlier judgment of the Supreme Court of the Slovak Republic in the same matter against another court as another obliged entity (10Sžik / 2/2017 of 19 June 2019):

We select interesting quotations from the judgment - taken from 10Sžik / 2/2017:

„When providing information relating to legal persons it is, of course, necessary to evaluate whether the information is ultimately relating to identifiable natural persons. It is therefore necessary to apply a reasonable probability test and to answer the question whether there is a reasonable probability that the data provided will be used to identify a natural person (this test was interpreted by the Court of Justice of the European Union in its judgment of 19 October 2014 in Case C-582/14, in the case of Patrick Breyer vs Bundesrepublik Deutschland). The answer to such a question depends on a number of factors in a particular case and is likely to vary depending on whether the information provided relates to multi-person companies or to a single-person limited liability company."

"For example, if the information should relate to a limited liability company with a sole shareholder and managing director, which would be the same natural person, in a certain context, it could be personal data if the information in everyday life concerns in fact only this natural person. On the other hand, if the information related to a legal entity with number of shareholders, directors or employees (e.g. a joint stock company), it would not necessarily

be information relating to a specific natural person. However, these examples may not be absolute, as they must be assessed in the context of the situation, by means of a test of reasonable probability under recital 26 of Directive 95/46 EC as well as recital 26 of the GDPR. It is being understood that an unforgettable criterion in such a case should also be the reason for the publication of data, i.e the fulfillment of the purpose of the Access to Public Information Act. As the Supreme Court has already stated, those questions have not been the subject of dispute in the present case, but it may be considered that the obliged entity applied the reasonable probability test and whether addressed disclosed information related primarily to a legal person or led to the identification of a natural person."

Supreme Court of the Slovak Republic (6Sžik / 1/2020): Info-request for access to the protocol of the Ministry of the Interior of the Slovak Republic, which control the police procedure during the pending criminal proceedings

Brief summary: The right of access according to the Access to Public Information Act shall not interfere in the activities of courts and law enforcement authority. The obliged entity shall make available the partial decisions or decisions on the merits after issuing the final decision not during the proceedings, even if the decisions do not contain personal data.

Summary: Based on the Access to Public Information Act, the civil association requested a protocol from the Ministry of the Interior of the Slovak Republic based of which was terminated the proceedings of the Department of control and inspection in the matter of verifying the police's procedure in the case of assaulted person. By judgment of 15 October 2010, the Supreme Court dismissed the action, pointing out the concept of implicit restriction of access to information which developed in Slovak case-law, according to which the Access to Public Information Act cannot be applied as an isolated legal regulation to assess the obligation to disclose information, but it is also necessary to assess whether the disclosure of the information would not jeopardize another interest of the State. According to the court of cassation (in Slovakia represented by the Supreme Court), the protocol in the present case was a partial decision and not a decision on the merits.

We select interesting quotes from the judgment:

"*The right to information is limited by the requirement not to interfere in the actual decision-making activity of courts or law enforcement authorities during the proceedings. The situation should be different in the case of a decision in the main proceedings if there are no grounds for restricting access to concerned decisions, provided that such decisions do not contain personal data protected by the Personal Data Protection Act*."

Regional Court in Bratislava (14CoCsp / 24/2020): Court injunction by which the bank shall correct the data on the termination of a loan in the non-banking register of client information (NRKI)

Brief summary: The date of termination of obligations under the consumer credit agreement pursuant to Section 7 (13) of the Consumer Credit Act is not the date of the declaration of early maturity of the loan but the date of actual repayment of the loan (although to another person - the assignee). Statement of this later date in NRKI is not a processing of incorrect personal data and cannot be corrected by ordering a court injunction after several years.

Summary: The bank's client (natural person) has demanded court injunction to be issued by the district court against the bank to adjust the loan termination dates approximately 3 years earlier than the registered data. According to Section 7(13) of the Consumer Credit Act, data in the register are registered for 5 years after extinguishment of debt. The lawsuit was preceded by a refusal to correct the data by the non-bank register. According to the applicant, the decisive date for the termination of the contract listed in register was the date on which the claim was transferred to the debt collection company. Applicant later claimed that this date should be the declaration of early repayment of the loan. However, the loans were repaid after the claim was transferred to the debt collection company. The information in the register was alleged to prevent the applicant from obtaining

mortgage refinancing. The applicant demonstrated the risk of a delay in the current situation on the mortgage market with lowest interest rates - and the failure to correct personal data should therefore be a threated as missed opportunity. The bank argued that the data were correct, as the obligation expired only upon full repayment, and at the same time objected to its passive legitimacy, as the claims had already been transferred to another person. By a resolution of 10th September 2020, the Regional Court in Bratislava upheld the rejection resolution of the district court and ruled in favor of the bank. However, if the applicant would be legally correct (termination of the obligation) and brought the action without delay and not after a few years, the court could, in a similar case, order the correction of personal data by a court injunction.

District Court in Komárno (13C/33/2020): Court injunction to refrain from using CCTV system on a family house

Brief summary: It is not possible to demonstrate the need to order a court injuction to prevent the use of the CCTV system only by submitting unexplained photographs.

Summary: The applicant claimed that the CCTV system at a neighboring house was processing her personal data unlawfully, without providing the necessary information and without her consent, thereby interfering with her private life. She claimed that the CCTV system monitored the premises of her property, which are not premises accessible to the public. For support of arguments, she submitted 4 photographs of the CCTV system to the court, however according to the district court, these were not sufficient to prove the facts necessary for order a court injunction. The District Court dismissed the application by resolution of 14th October 2020.

We select interesting quotes from the judgment:

"*It is not clear from the photographs that this is a camera placed on a house owned by the defendants. However, it is clear from them that the camera captures the space along the side wall of the house of the unknown owner, on which it is located, undoubtedly for the personal purposes of the owner of the house. At the same time, monitoring of premises for the purpose of property protection is possible. It is not clear from the photographs that the installed camera also captures the space owned by the applicant and therefore the camera also records the applicant's personal data. In addition, it is not even clear that the camera taken in the photographs is a functional camera or only its imitation. According to the Court, the applicant has not shown the need to adjust the relationship between the parties without delay by a court injunction to the proposed scope, nor the merits and duration of the right shall be protected. Therefore, the court rejected the application in its entirety.*"

'In addition, the applicant did not even specify what should be the subject of the main proceedings, in particular when she emphasized the role of the Office for Personal Data Protection of the Slovak Republic, which is authorized to inspect facilities of controlled person that may, should or are used for processing of personal data.(§93 of Act No. 18/2018 Coll., In connection with § 3 paragraph 5 letter a / of the cited Act)."

4. Other activities of the Office

In 2020, the Office did not publish any new methodological guidelines, except of the February update of its older guideline no. 3/2018 on the obligations of the e-shop operator. However, it contains only minor changes such as removal of legitimate interest as a legal basis for cookie marketing purposes.

At the end of April, at the government proposal, the parliament removed the Office Chairman. Office is still represented by the Vice-Chairman. Prior to her dismissal, the Office Chairman was questioned by the Human Rights Committee of the National Council of the Slovak Republic which was mostly interested in a request for cooperation sent by the Office to an independent Czech journalism center. It was controversial in this case that the Slovak Office acted directly against a Czech entity, which seemed not outside of the its jurisdiction. According to the provisions on cooperation, mutual assistance and cross-border cooperation under Art. 60 to 62 GDPR, the Czech Office should have probably been contacted first.

Another external activity of the Office was dominated by the development of a pandemic. The Office issued several short reports, notices and preliminary opinions in this regard, in particular through its website. Initially, the Office only referred to the European Data Protection Board guidelines and other European sources on personal data protection and COVID-19, but later commented on specific issues.

However, already during April it was evident that the cooperation between the Office and the new Government is not ideal. On April 16th, the Office publicly objected to the speech Ministry Remišová that the Office was allegedly delaying the intelligent quarantine project, claiming that the Public Health Office of the Slovak Republic does not need the Office's "permit" to launch the application.

In May, the Office published Eight basic questions for controllers recommended to be consider for contact tracking applications (based of model of the Global Privacy Assembly, which the Office is part of).

In August, the Office published an information document on the rights of the data subjects, together with model applications for their exercise.

In September, based on the media information provided by company Nethemba relating the security incident in the “my eHealth” application, the Office initiated separate administrative proceedings against National Health Information Center and Public Health Authority of the Slovak Republic and entrusted the inspection department with performing inspections in both cases. These proceedings are ongoing.

On October 21st, as part of the national testing, the Office stated that it considered the national testing as "logistically demanding" and provided an overview of the basic obligations that the controller shall fulfill (at that time it was allegedly not clear who would be controller). The Office stated that only healthcare professionals and other regulated entities from the presented teams have a sufficient legal basis for the processing of personal data in accordance with the Health Care Provision Act and the Public Health Protection Act. Finally, the controllers were healthcare providers, with the Ministry of Defense, in cooperation with the military who performed the registration of medical volunteers.

The following day, the Office updated the "Frequently Asked Questions" document in relation to coronavirus situation. Interestingly, the Office acknowledged that a physical control of an identity card in order to verify the age at entry into promises might not necessarily fall under the GDPR. A positive effect for future practice is that historically it has been one of the first, if not the very first negative interpretation of the term filling system in the sense of Art. 2 (1) GDPR by the Office. However, if such operation does not fall under GDPR then the last sentence of the opinion seemed redundant: "*In the event when sellers require proof of identity with an identity card only, we recommend you to cover other data (by fingers, palms) that are on the identity card and are not necessary for assessing age by employees of store. „*

At the end of October, the Office commented on the question of using streaming from municipality cameras to inform the public about the amount of persons queuing in front of sampling points in the national testing,

concluding that this would probably be a new incompatible purpose of processing. In such a case, the Office recommended that municipalities ensure that persons are not identifiable in the images, for example by blurring the image, or alternatively inform public about the approximate number of people and the waiting time on the website or on the radio.

Clients as well as the professional public accepted very negatively two "preliminary" opinions of the Office regarding their obligation check a negative test at the workplace and in the premises from 29th and 30th October. In the first opinion, the Office stated that a government resolution could not be a legal basis, nor could the Labor Code or any other legal regulation known by the Office. In the second opinion, in which the Office assessed the Decree of the Public Health Authority of the Slovak Republic that provided the obligation in such question, the Office limited itself to a very brief and incomprehensible statement:

"*The Office performed a legal analysis with regard to the protection of personal data, which was sent to Public Health Authority of the Slovak Republic. Based on this analysis, it came to the conclusion that the provisions of Act no. 355/2007 Coll., which the Decree should implement, are not reflected in the proposed version of the Decree. In view of the above, the Office remains with its previous opinion from 29/10/2020 that Government Resolution no. 678, as well as 693, do not pose sufficient legal basis for the processing of health data.* "

By this statement the Office practically recommended to controllers not to check negative tests on entry, as there is allegedly no legal basis for this. It is interesting that in this case the Office no longer took a similar position as in the case of control the age on identity cards through a negative interpretation of the term filling system. Apart from the legal standpoint and in view of the declared state of emergency, we consider these Office's two opinions as its two biggest professional mistakes in 2020. Due to legal uncertainty for clients and short time, we publicly criticized this approach and provided a free sample mini privacy policy for entry control together with presentation aimed to help explaining the legal standpoint of the problem. The Office's approach was not free without severe criticism from the Office of the Government of the Slovak Republic.

Last but not least, even in 2020, the Office has not yet managed to ask the European Data Protection Board for approval of accreditation criteria for monitoring bodies pursuant to Art. 41 (3) GDPR and thus not even adopted a decree, which is provided for in Section 87 (12) of the Slovak Data Protection Act already from 25th May 2018. A similar conclusion applies to certifications under Art. 42 GDPR or Section 88 of Slovak Data Protection Act. In practice, it is not possible in Slovakia to apply for accreditation of a monitoring body and thus the sectors are unable to reach the full application of codes of conduct. It is unbelievable that because of the inaction of the Office it is not possible in practice to use all the institutes and benefits of the GDPR even two years after the beginning of GDPR application. Especially if there were two years to prepare before that.

Summary

With hindsight, it may be surprising that COVID-19 agenda has kept us so busy also in the field of personal data protection. The basic issues concerning the nature and function of the legal bases such as legal obligation, public and legitimate interest – which caused most of the problems – should have been clarified a long time ago. However, it is obvious from our legal system or from the approach of the Office that these legal bases are still misunderstood and still cause us problems in practice. However, these are not the only problematic institutes.

The Chairman of the Czech Office allegedly said at the conference in 2020 that he has not yet seen in practice a correctly carried out impact assessment pursuant to Art. 35 GDPR. At the same time, he noted that the number of previous consultations requested by the Czech authority pursuant to Art. 36 GDPR were close to zero. We have a similar problem with the understanding of data protection impact assessment as a human rights analysis in Slovakia. In Slovakia, there is zero methodological support in relation to DPIAs, as is evidenced by the Decree of the Office No. 158/2018 Coll.

In other EU countries, cross-border transfers to the US and the UK were the overarching theme of the year, due to the abolition of the EU-US Privacy Shield and Brexit. Foreign supervisory authorities assessed the use of products such as Microsoft 365 Office, Google Analytics, targeting advertising via social networks and processing cookies in the context of the forthcoming ePrivacy Regulation. These tools are used by almost all companies in Slovakia as well, and the sensitivity of these processing activities is incomparable with the COVID-19 agenda, CCTV systems, birth numbers and similar “evergreen” topics, which our Office has traditionally dealt with. However, these are undoubtedly more complex topics that require a much more demanding interpretation, which the Office's practice has not yet reached.

To evaluate positively the activity of our regulator, the overall state management of this area or the legislative process itself, it would be a deception of oneself. There are still Member States where only now the first GDPR fines are imposed. However, if we look at Western European countries, we will find that although Slovakia has some administrative activity, we are in fact at the very beginning in developing this field in practice.

However, what we rate positively is the decision-making of our courts. Unlike the Office, the courts are unable to choose the agenda by initiating proceedings based on their own initiative. The case-law in this area suffers from the lack of claimants. However, there is no explicitly incorrect, controversial or somewhat unusual court decision in the field of personal data protection. On the contrary, we can see that case-law is being stabilized in recurring matters such as the conflict of personal data protection with the Access to Public Information Act. At the same time, the first attempts of bolder interpretations of the definition of personal data should be appreciated, as well as cases where courts have simply maintained common sense instead of unnecessary legal theorizing.