National Authority for Data Protection
and Freedom of Information

ANNUAL REPORT OF THE HUNGARIAN NATIONAL AUTHORITY FOR DATA PROTECTION AND FREEDOM OF INFORMATION (NAIH)

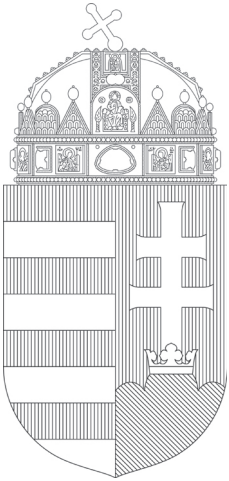
2019

Annual Report of the Hungarian National Authority for Data Protection and Freedom of Information (NAIH)

2019

B/8988

National Authority for Data Protection and Freedom of Information
Budapest, 2020



Preface

To the Reader

To rephrase Imre Madách „ The work, the great work is now completed,
Machine is running", but the creator is not resting. Despite the fact that the General Data Protection Regulation has been adopted in the European Union, two very important tasks remain to be done: the practical elaboration of the application of law and the transfer and sharing of knowledge to both professional and wider public.

As president of NAIH and a university professor, in 2019 I placed great emphasis on teaching knowledge related to data protection and freedom of information, and introducing it into university education. Unfortunately (I would add: despite our efforts) there is undeservedly little attention paid to knowledge about information rights in public education and higher education - despite the fact that minors should be seriously educated to protect privacy in the digital age! At the same time, in the field of university vocational training, there is a huge market demand and requirement for acquiring and deepening knowledge of data protection in the EU.

In 2014, the Institute of Postgraduate Legal Education of Eötvös Loránd University launched the training of data security and data protection lawyers: "The aim of the two plus one semester courses is to prepare lawyers for the professional conduct of authority procedures, contentious and non-contentious proceedings, building on the practice of the NAIH by raising awareness of the legal problems in the fields of data security, data protection, freedom of information and data processing in the public and private sectors, which are almost non-existent in basic education.. "

The aim of the specialized postgraduate training course for European Union data protection consultants launched at the National University of Public Service in 2019 is „to train data protection advisers who can apply the provisions of the GDPR through knowledge of the new data protection rules required in the EEA."

The trainings are mostly attended by students with a law degree (lawyers, judges, civil servants). Many of them working in the administration, but students also

come from law enforcement agencies, the military or even the private sector. What they have in common is that in their daily work they need to apply and interpret the legislation related to information rights. The transfer of the necessary knowledge is mainly ensured by experts of the NAIH.

The conference of data protection officers in 2019, which was conducted electronically for the first time, also served a similar purpose, transferring and sharing NAIH's professional knowledge and experience with professional audiences and the public, in the form of video presentations based on a preliminary needs assessment.[1]

In the field of freedom of information, in 2019 we tried to "explore" areas and provide comprehensive information about where the guidance of the supervisory authority is needed.[2]

In this connection, it should be noted that the system of constitutional right to access data of public interest has not changed in Hungary for a long time since the introduction of the concept of data accessible on public interest grounds (which does not mean that law enforcement does not constantly struggle with various old-new problems). Based on my decades of experience, I think that, in fact, access to data regarding the exercise of public authority and regarding the public financial management require a different approach - and these issues might and ought to be discussed in the context of academic debates.

The realized digital environment and the range of related challenges also create a new situation to both information rights, as the quality, speed and quantity of data processing here certainly stretches the framework of the old principles. It is enough to think about facilitating the searchability and availability of data of public interest, which, in the optimal case, reduces the working time that can take days or weeks by reviewing hundreds of paper-based files to a few seconds. And the digital tools and solutions available should be put at the service of constitutional fundamental rights - in the fullest and most self-evident way possible!

Finally, I need to refer to the so-called Article 7 procedure initiated by the European Parliament against Hungary alleging breaches of core EU values on 12 September 2018, in which civil society organizations repeatedly argued that the NAIH could not be considered an independent institution due to the procedure of appointing the President of the Authority. I would like to refute the accusation with one professional argument here: the procedure for appointing the President of the Authority fully complies with the requirements set out in Article

53 Section 1 of the GDPR. The procedure for the appointment of the head of the data protection supervisory authority under the Hungarian rules currently in force was thoroughly examined by the European Commission, just prior to the infringement procedure referred to by the civil society organizations, and no objections were raised. It considered it to be in accordance with European Union law and, moreover, that subject-matter did not form part of the alleged infringement procedure. On the part of the NAIH, therefore, I consider this allegation, although it is a recurring accusation, to be unfounded once and for all.

Budapest, 2 March 2020

Dr. Attila Péterfalvi

Honorary University Professor
President of the National Authority for Data Protection
and Freedom of Information

1 https://naih.hu/dpo-konferencia-2019.html
2 https://naih.hu/informacioszabadsaggal-kapcsolatos-tajekoztatok.htm

I. Statistics on the Activities of the Authority

I.1. The Statistical Features of Our Cases

Since the date of mandatory application of the GDPR (25.05.2018), 2019 is the first full calendar year for which statistical analysis of cases can provide information on the impact of the new regulatory environment in regards to the operation of the Authority.

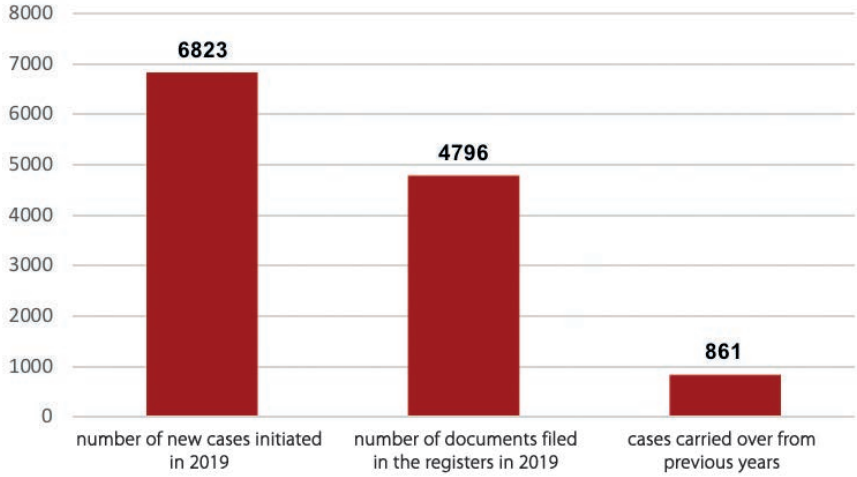
The quantifiable presentation of the operation of the Authority in 2018 was complicated due to changes in the legal environment and the partial transformation or termination of various professional tasks and registers of the Authority. When presenting the case statistics for 2019, we aimed to show the changes experienced in 2019.

In 2019, 6,823 new cases were registered in the Authority's electronic document management system. Together with cases carried over from previous years (861), 7684 cases were pending.

4796 documents have been received and registered in the transformed electronic registers.

In 2019, a total of 11,619 cases were initiated at the Authority, so 12,480 cases were pending, including cases carried over from previous years.

The number of cases with the Authority in 2019

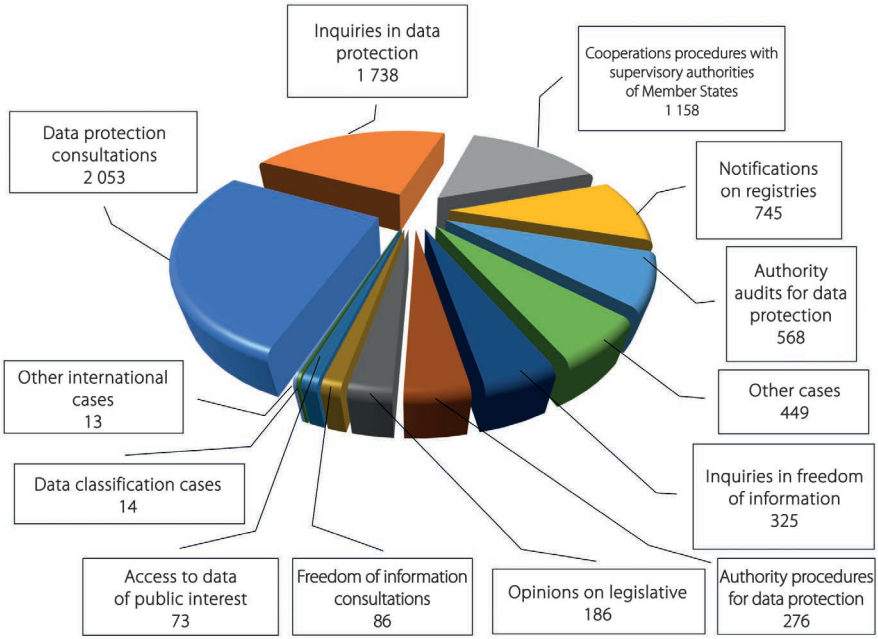


The number of cases with the Authority in 2019
(and its change compared to 2018) as per case types

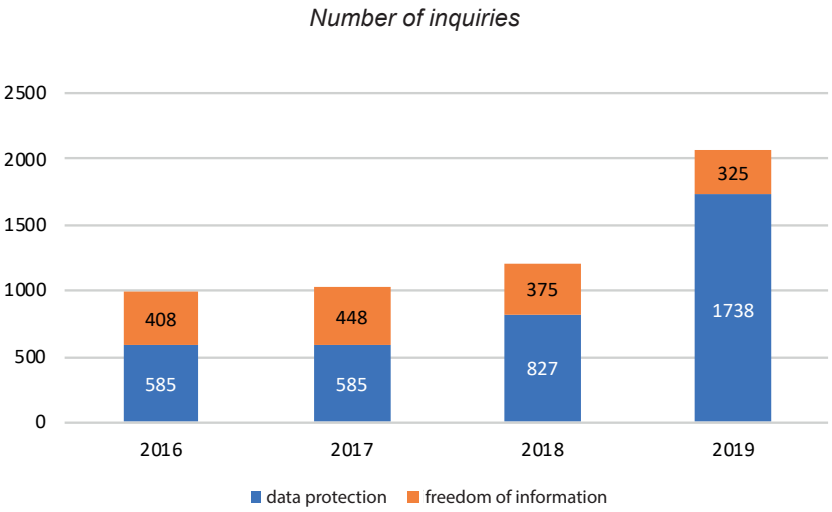
Types of cases	**2018**	**2019**
data protection consultations	2.409	2.053
inquiries in data protection	827	1.738
cooperation procedures with supervisory authorities of Member States	606	1.158
notifications on registries	1.305	745
authority audits for data protection	234	568
other cases	131	449
inquiries in freedom of information cases	375	325
authority procedures for data protection	67	276
opinions on legislative drafts	195	186
freedom of information consultations	88	86
NAIH access to data of public interest	74	73
data classification cases	15	14
other international cases	85	13
total number of pending cases:	**6.411**	**7.684**
electronic notifications received in the DPO notification system	1.786	4.796
Total annual case number:	**8.197**	**12.480**

The pending cases of the Authority in 2019

(without the DPO notification system)

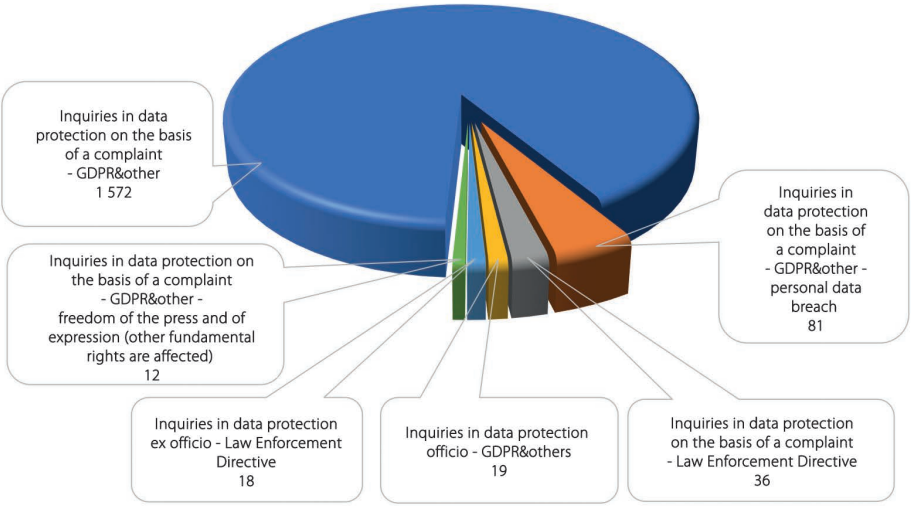


The number of submissions for consultation received by the Authority decreased by 20%, while the number of cases concerning inquiries in data protection doubled in comparison with 2018. The continuous increase in the number of inquiries is well illustrated in the following figures.



The number of inquiries in data protection in 2019 is illustrated by the following figure:

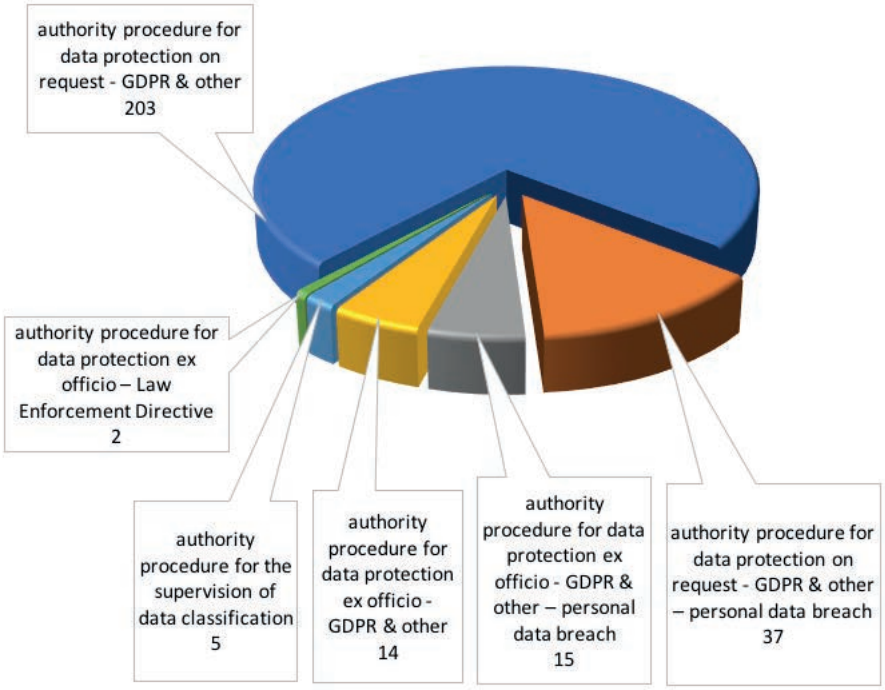
Inquiries in data protection as per case type



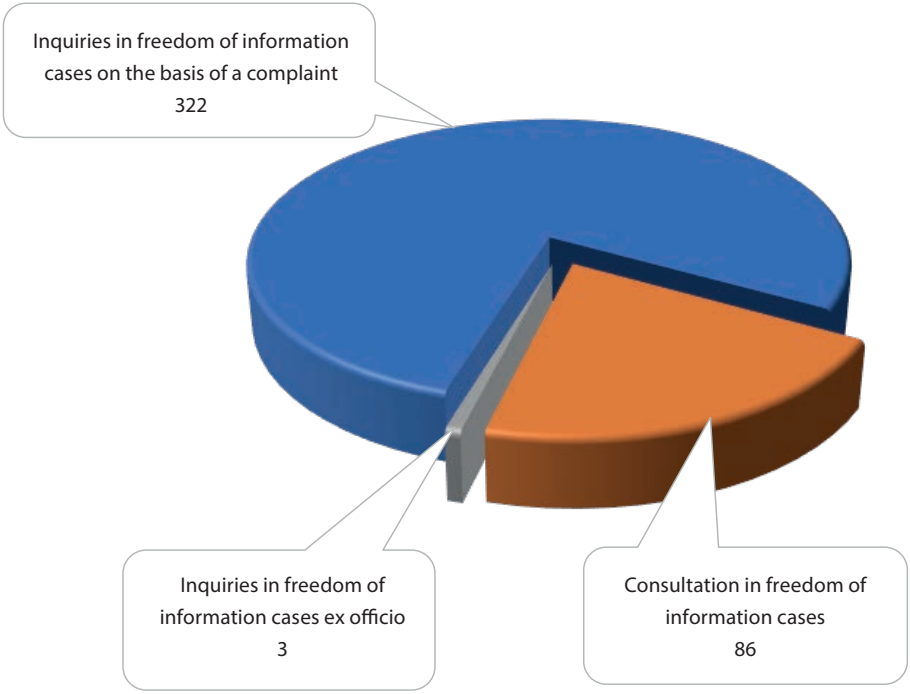
In 2019, the change in the procedural requirements will also show measurable results. The number of authority procedures initiated since the coming into effect of Act CL of 2016 on the Code of General Administrative Procedure (hereinafter: 'the Administrative Procedure Act') and the amendment of Act CXI I of 2011 on the right to informational self-determination and on the freedom of information (hereinafter: 'the Privacy Act') increased from 67 in 2018 to 276. With this increase in the number of cases, the workload of the administrators also multiplied

case type	Case number (db)
authority procedure for data protection on request - GDPR & other	203
authority procedure for data protection on request - GDPR & other – personal data breach	37
authority procedure for data protection ex officio - GDPR & other – personal data breach	15
authority procedure for data protection ex officio - GDPR & other	14
authority procedure for the supervision of data classification	5
authority procedure for data protection ex officio – Law Enforcement Directive	2
Total number of authority procedures:	276

Authority procedures as per case type



Freedom of information cases as per case types



In 2019, the telephone customer service of the Authority received 2933 calls, which is still an increase compared to the data of previous years. The number of interested parties requesting information and assistance from the Authority in order to protect their rights and interests as data subjects and to take effective action against the data controller has increased. The telephone customer service of the Authority also drew the attention of callers to the possibilities and limitations of exercising the data subject's rights ensured by the GDPR towards the data controller as well as the deadline for the data controller to respond. It also provided information on the legal remedies available to them in connection with the procedures of the Authority, how to lodge complaints and requests.

In a number of cases, property owners - or those living in condominiums or co-operative flats – requested information from the Authority of their legal options if their neighbor has installed a camera on his property to monitor their home, front door or stairwell. Unfortunately, in many cases, it is not clear whether security

cameras were indeed illegally installed, or whether their viewing angle was actually limited to their own property - for example, because it was properly masked, or perhaps the camera installed was a fake camera. In many cases, callers have already tried to initiate property protection proceedings with the relevant notary, but they were referred to the Authority.

The Authority frequently received calls that involved camera surveillance of employees. A common feature of the cases is that the data subjects have received no or insufficiently detailed information on the circumstances of the data processing. In addition, in many cases, data controllers inquired about how they could lawfully conduct camera surveillance.

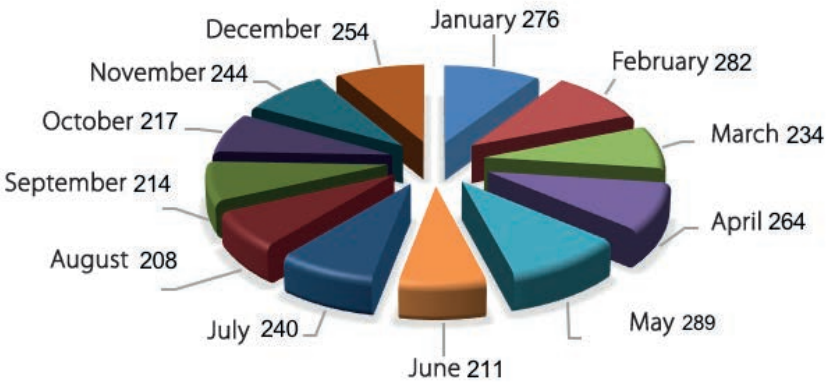
The European Data Protection Board's Guideline 3/2019 on camera data processing operations, which is currently only available in English, will hopefully help data controllers to comply in this area.

There were still a number of questions about the requirements to be met by a person or organization planning to launch a webshop, although the Authority made its guidance on data protection issues for privately operated websites already available in the summer of 2018 among its resolutions on data protection reform.[3]

Finally, many callers approached customer service with the problem of receiving massively harassing, mostly marketing emails, possibly text messages in large quantities, that they didn't ask to receive, nor have they ever signed up for it. In many cases, even if clicking on the Internet link at the bottom of the emails, it might not be possible to unsubscribe or there might be no unsubscribe link at all. The Authority also draws attention to the fact that, in addition to the rights of data subjects under the GDPR, the National Media and Infocommunications Authority has the task and competence to conduct supervisory proceedings related to electronic advertising in Hungarian or clearly intended for domestic recipients

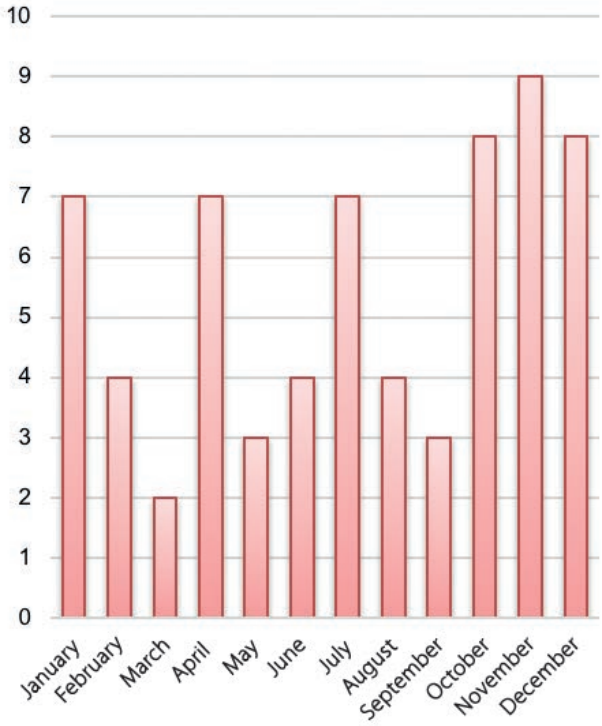
3 https://naih.hu/files/2017-02-17-webaruhaz-tajekoztato-NAIH-2017-1060-V.pdf

Telephone customer service in 2019 (number of calls)



In the first year after the GDPR becoming applicable, the Authority provided personal customer service 66 times, an increase of around 30% compared to 2018, where data subjects submitted complaints with regard to processing of personal data, or infringements of the right of access data of public interest, or data accessible on public interest grounds, or exercised their rights to access to documents on procedures.

Personal customer service in 2019 (cases)



In 2019, 2,400 new data controllers and data processors created accounts on the electronic data protection officer notification interface available on the Authority's website, and the Authority received more than hundred requests to delete the notified data controller and the data controller / data processing organization. Changes in the name (in the case of a legal entity) and contact details of the data protection officer may be initiated by data controllers and data processors by submitting a new notification through their account in the system, but deletion of previously recorded data is only possible upon written request.

I.2. Annual conference of data protection officers

In accordance with Section 25/N (1) of the Privacy Act the annual conference of data protection officers (DPOs) shall be convened by the president of the Authority. The conference is intended to maintain a regular professional relationship between the Authority and the DPOs, its goal is to develop a consistent legal practice with regard to the application of laws concerning the protection of personal data and access to data of public interest.

Thus, the law provides to maintain a professional relationship not with the data controller, but primarily with the DPO who has been communicated to the Authority - by the end of 2019 there were about 1,850 DPOs performing his / her duties at more than 4,200 organizations. Therefore, the possibility to participate in the conference is independent of the sector or legal relationship in which the DPO works, as he or she may have been appointed to several different organizations.

Given that, following the entry into effect of the GDPR, training in order to develop a consistent legal practice needs to be made available to a significantly larger number of participants and that DPO duties are not limited to the territory of Hungary, therefore this year the annual conference of DPOs was conducted electronically for the first time. By using e-learning solutions, the conference could also contribute to a higher level of utilization of the professional knowledge, as it can be reviewed several times, and its presentations can be used by officials even during their internal trainings.

In the spirit of professional cooperation, the Authority also provided an opportunity for data protection officers to shape the content of conference presentations. As part of this, in an online questionnaire in October 2019, the Authority assessed the needs and professional knowledge of DPOs, and their questions and issues of wider interest related to data protection and freedom of information

I.2.1. Results of the preliminary questionnaire survey

As of October 2019, we sent the conference invitation of the President of the Authority and the related questionnaire to the e-mail addresses of all 1797 DPOs who has been communicated to the Authority. As the respondents almost exclusively (97.7%) came to the site via the link available in the e-mail sent, it can be assumed that the questionnaire actually reached the data protection officers.

The survey yielded more than expected results, with 488 replies received, i.e. 27.15% of all notified DPOs took the opportunity provided in the Authority's invitation.

More than half of the voluntary respondents have been working with data protection and fulfilling the duties as data protection officer for 1-3 years. Nevertheless, almost 20% have been dealing on the field for only a few months, while 26% have been working with data protection for more than 3 years. 43% of the respondents also perform tasks related to freedom of information, so presumably they operate to a large extent in the public sector. However, less than 10% of the respondents are employed by an organization that carries out data processing activities (for criminal investigation, national security, national defense purposes) defined by the Privacy Act.

The results of the up-to-date knowledge of DPOs show that in the last year, 70% of officers have improved their data protection skills through one- or several-day training, while more than 20% (100 officers) have not participated in data protection training at all

Have you attended an organized training course on data protection in the last year?	Answers	Percentage
university training	80	16.39%
several-day training	182	37.3%
one-day training	156	31.97%
online training	40	8.2%
None of them	100	20.49%
Other...	11	2.25%

Three-quarters of the respondents to the questionnaire were also supported by their organization in expanding their data protection knowledge. They typically ensured their participation in organized trainings and were subscribed to professional content

Has your organization supported the expansion of your knowledge of data protection and data security?	Answers	Percentage
With reduction in working time	69	14.14%
With internal training	86	17.62%
With organized training	209	42.83%
With subscription to professional content	106	21.72%
None of them	126	25.82%
Other...	23	4.71%

With regard to their knowledge that they can acquire on their own, it should be noted that almost half of the respondents did not read the last year's annual report of the Authority, and the recent decisions, reports and announcements published on the naih.hu website after the GDPR became applicable, did not reach more than 100 DPOs. However, 78% of respondents visit the website of the Authority at least monthly.

How often do you visit the www.naih.hu website?	Answers	Percentage
Weekly or more often	195	39.96%
Monthly	185	37.91%
Less often	94	19.26%
Never	14	2.87%

Also, 62% of DPOs do not visit the website of the European Data Protection Board (EDPB), although guidelines on the use of the contractual legal basis under the GDPR in the context of the provision of online services, or on the processing of personal data through video devices were first made available there - as draft guidelines to promote a common understanding of European data protection laws, published for public opinion, are still only available on this interface. Furthermore, the site provides English summaries of recent decisions imposing a fine by the national supervisory authorities, which could also be a useful resource for the work of scientific researchers in the field of data protection.

How often do you visit the website of the European Data Protection Board?	Answer	Percentage
Weekly or more often	58	11.89%
Monthly	129	26.43%
Less often	214	43.85%
Never	87	17.83%

In connection with the proposals for the content of the Authority's renewable website, the vast majority of respondents would like to see a Q&A database concerning the SME sector and categorized official decisions that can be filtered by topic. Thus, the Authority will pay particular attention to related developments.

In connection with the activities of the DPOs, it was seen that the vast majority of them perform the advisory tasks to be provided to the data controller or data processor, as well as to the staff performing data processing under Article 39 of the GDPR, and their professional opinion is typically sought by the management of their organization. However, the majority has not carried out checks and audits regarding internal data protection compliance or has not documented such since its appointment, nor has it developed an action plan for these activities, which could improve the application of the accountability principle, the level of data protection awareness and transparency within the organization.

Since your designation as DPO at your organization have you...	Yes	No
delivered your opinion on drafts concerning internal rules and data processing?	446	42
been asked by the head/management of the organization for professional advice on issues related to data processing?	438	50
prepared an internal audit plan?	204	284
carried out a documented internal audit?	192	296

Based on the answers, it can also be seen that there may be shortcomings in many places in connection with the organization of awareness-raising trainings, while the tasks related to the exercise of the data subject rights and the needs for a data protection impact assessment have not yet arisen in many places.

Since your designation as DPO at your organization have you...	Yes	No
provided data protection awareness-raising training?	362	126
provided data security awareness-raising training?	279	209
been involved in preparing draft replies to requests exercising data subject rights?	277	211
carried out a data protection impact assessment?	220	268

A total of 173 professional questions of legal interpretation were received by the Authority which, in the opinion of the DPOs, may be of public interest. The questions largely concerned the new legal institutions of the GDPR, the changing legal bases and the way of exercising data subject rights, but the Authority also received questions in connection with the proceedings of the Authority, the scope of the Privacy Act and notification to the data protection register of the Authority, which terminated following 25 May 2018.

I.2.2. Electronic tutorials for the conference of data protection officers

Based on the results of the questionnaire survey and the average preparedness of DPOs, the Authority identified the topics of the conference and compiled instructional videos and written responses, providing guidance on the questions received.

On 23rd of December 2019, 10 instructional videos were published on a separate interface[4] created on the Authority's website, in which for more than two hours, the President, Vice-President and staff of the Authority presented the first experiences with the application of the GDPR. As according to the results of the sent-out survey the presentation of practical examples was considered useful by the DPOs, thus the speakers of the conference placed special emphasis on this when illustrating the most important changes.

4 https://naih.hu/dpo-konferencia-2019.html

Following the welcoming words, the President of the Authority was the first to present aspects of the imposition of fines in the Authority's proceedings in relation to two recent decisions, comparing them with the Article 29 Working Party's Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (WP253). After that, he described one of the most suggested topics in the survey, the aspects and requirements of data processing based on legitimate interests and balancing of interests.

Following the general presentation of the concept of personal data breach, the Vice-President of the Authority explained the tasks related to the handling of personal data breach by mentioning a number of practical examples and answering questions of interpretation based on the relevant guidance of the Article 29 Working Party. He then addressed in his third presentation the questions raised by DPOs in relation to the data protection impact assessment and the transfer of data to third countries.

The results of the preliminary survey conducted in connection with the conference and the tasks related to the appointment of the DPO, as well as the answers to questions related to the electronic DPO notification system available on the website of the Authority, were presented by the Head of the Certification and Social Relations Department.

The data protection expert of the Data Protection Department presented the procedures of the Authority and examined the identification, assessment and fulfilment of requests to exercise data subject rights, taking into account the experience of several authority proceedings for data protection concluded in 2019. He also answered questions received by the Authority regarding legal bases under the GDPR, referring to the case law of the Court of Justice of the European Union and the guidelines issued by the European Data Protection Board.

Finally, the Authority's project assistant answered some of the frequently asked questions received from small and medium-sized enterprises through the SME Hotline operated by the Authority under the European Union-funded STARII Project.

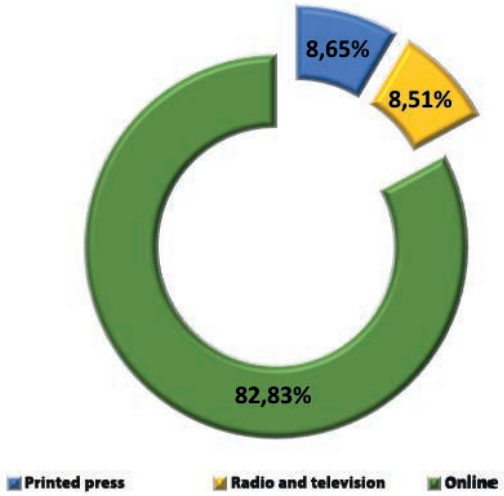
The videos can be watched on the website of the Authority for one year thanks to MTVA's Media Click streaming service, but the presentations will continue to be available for download from the website of the Authority.

In addition to the videos, the Authority published written answers to further 25 questions on data protection and 7 on freedom of information submitted by DPOs, which were not covered during the presentations.

I.3. Media Coverage of the National Authority for Data Protection and Freedom of Information

In the following, we summarize the media appearances of the Authority in 2019. There were 2,808 pieces of news in the media concerning the National Authority for Data Protection and Freedom of Information between 1st of January and 31rd of December 2019. It was in the Online media that the activity of the Authority was most often reported, running 2,326 news items (82,83%). The printed press published 243 articles on the NAIH (8,65%), while the electronic media did 239 (8,51%) articles.

A Media Coverage of the NAIH in 2019



Source: Observer Budapest Médiafigyelő Kft.

II. The Application of the General Data Protection Regulation

II.1. Data Protection Cases

The Authority responded to several data protection questions, consultation submissions, as well as conducted inquiries in data protection and authority procedures for data protection this year as well.

Among the decisions made in authority proceedings, the number of decisions that are also measured in court can be considered significant. The Authority closed a successful year in this regard. In 2019, there were five final court decisions on judicial review of the Authority's decision. The trial courts shared the Authority's position on the merits of the case each time. In four of the five closed cases, the Authority was successful: the court upheld the Authority's reasoning and upheld the decision (NAIH / 2019/167, NAIH / 2019/214, NAIH / 2019/2566, NAIH / 2018/6248), while in one case (NAIH / 2019/2074) the court instructed the Authority to initiate a new procedure with regard to the imposition of fines.

II.1.1. Data processing at workplace

1. *Changes in legal regulations*

Within the framework of the review of legislation due to the General Data Protection Regulation (hereinafter: 'the GDPR'), the "adaption" to the GDPR of several (sectoral) laws with data protection provisions were still in progress in 2019. The amendment of the provisions of Act I of 2012 on the Labour Code (hereinafter: Labour Code) concerning the processing of personal data was also part of this process.

According to the main changes effective from April 26, 2019, statements or data required by the employer from the employee shall basically be verified by presenting documents, thus as a general rule, prohibiting the employer from making copies of the documents.

As a further change, the Labour Code specifies the cases in which the employee's biometric data and criminal personal data can be processed. In essence, the Labour Code defines such interests and cases, in the event of which these data can be legally processed, if the requirement of necessity and proportionality

is met and the data processing of the controller is also based on an appropriate legal basis - mainly the legitimate interest. This may be the case, for example, where there is a risk of serious or massive, irreversible harm to the life, physical integrity or health of the employees or others, or if the employer safeguards toxic or hazardous chemical substances or biological material, or particularly considerable pecuniary value in accordance with Act C of 2012 on the Criminal Code. However, the major interests protected by law indicated in Section 11 (1) (b) of the Labour Code, as follows from the wording „in particular", are to be construed as examples only, and the Authority may also accept interests protected by other law if the necessity and proportionality of data processing is justified within a legitimate interest test.

A significant change in the scope of the control of employees is that after the amendment of the law, the employee shall be allowed to use information technology and computing equipment provided by the employer for the performance of work solely for the reasons within the framework of the employment relationship, unless there is an agreement to the contrary. As a general rule, therefore, an employee may not use the computing equipment provided for the performance of work for private purposes.

Violation of this rule may lead to labour law consequences, but the right of inspection - even if it is proven that the employee has used the computing device for private purposes –may only extend to the statement of the fact of private use, however, the employer cannot get to know any private data and information, only those related to the performance of work. This follows from the unchanged provision that employers shall be allowed to monitor the behavior of employees to the extent pertaining to the employment relationship. This also applies if, by agreement between the parties, the employee uses his or her own computing equipment for the performance of work under the employment relationship.

In addition, it should be emphasized that the rights relating to personality of employees, including the right to the protection of personal data, may be restricted if the restriction, such as data processing, is strictly necessary for reasons directly related to the intended purpose of the employment relationship and proportionate to the legitimate aim pursued.

The means and conditions for any restriction of rights relating to personality, furthermore the circumstances underlying its necessity and the proportionality, and the expected duration shall be communicated to the employees affected in writing in advance. As a result, and in accordance with the rules of the General

Data Protection Regulation, the employer shall provide information relating to the data processing and all its circumstances to the employee in an appropriate and transparent manner.

2. *Cases related to inspection of E-mail accounts*

Every year, the Authority receives a large number of complaints concerning data processing by employers. In 2019, two cases related to the inspection of e-mail accounts and one related to electronic monitoring should be highlighted, which were examined by the Authority in authority procedure for data protection.

In one case, the applicant objected that during his incapacity to work due to illness, his desk and computing access, equipment and e-mail account had been checked in his absence, the physical location of documents on his desk had been changed and photographs had been taken of all such inspected items, which, in his view resulted in unauthorized data processing and access. It is important that access to the e-mail account and computing equipment was provided, originally at the explicit request of the applicant, to ensure continuity of duties of the absent employee and not primarily to monitor him. Only due to deficiencies detected during the applicant's replacement was a full inspection carried out. (NAIH/2019/769.).

In another case, the applicant stated that, following the termination of his employment relationship with a hospital and without his permission, management had ordered the recovery of his actually canceled, deactivated hospital e-mail accounts because they were looking for a document. The applicant objected to that by this recovery they had access to his personal documents and data in the deactivated accounts, as he also handled his private correspondence there, since he was allowed to do so. (NAIH/2019/51.).

In case NAIH/2019/769 the Authority essentially investigated the inspection of the e-mail account and made important findings on the legal basis of the legitimate interest.

In its decision, the Authority stated that in the case of data processing for the purpose of the control of the employees, the legal basis for data processing may be the legitimate interest.

According to the facts of the case, the data processing was performed by the employer in the framework of the control of the employees, and the legitimate

interest in this control and in the personal data necessary for this control could be proved based on the legislation, the statements made during the proceedings and supporting documents. There was a risk of serious financial and additional legal consequences, the elimination or mitigation of which required the immediate action of the data controller. In this case, access to the e-mail account and computing equipment was not primarily provided for the purpose of control of the employee, but to ensure the continuity of duties of the absent employee. Only due to deficiencies detected during the applicant's replacement was a full inspection carried out in order to address the financial and other legal consequences, on an ad hoc basis.

In this case, based on all the circumstances of the case, the legitimate interest as legal basis could be justified even in the absence of a detailed legitimate interest test carried out in advance and in writing by the data controller. However, the Authority emphasizes that this does not affect the obligation of data controllers to assess the existence of the conditions necessary to justify the legal basis of legitimate interest in advance and continuously during data processing based on such legal basis, also in compliance with the fundamental requirement of accountability.

In addition, in both decisions, the Authority stated that, as a general rule, the presence of the employee should be ensured during the inspection of the e-mail account, in accordance with the principle of fair data processing.

The prior notification and personal presence of the employee - if this cannot be ensured, the presence of his / her proxy or representative - during the inspection, review of the e-mail account or search for a document is necessary, also because there may be different personal data of the employee and third parties in the mail system, which the employer is not entitled to process, beyond inspecting this nature of the personal data. If the employee – or the representative, proxy - is present during the review and inspection of the e-mail account or the search for a document, and can indicate before viewing the content of an e-mail account containing personal data that it contains private e-mails, this ensures that the employer does not violate this prohibition.

However, depending on the circumstances of the inspection of the e-mail account, there may be situations where the personal presence of the employee cannot be ensured for objective reasons. As an exception to the general rule, the Authority therefore also considers it acceptable in certain situations for an employee to be absent, such as in cases requiring immediate action, in the case

of an employee on sick leave or a former employee who no longer has an employment relationship with his employer. In this case too, however, the employee shall be informed of the planned employer measure and shall be given the opportunity to be represented by proxy or representative. If, despite these preventive measures - prior information and ensuring the presence of the employee or his / her proxy or representative - the employee is not reachable or does not appear in person or through the representative, the e-mail account may be accessed in his / her absence by an independent third party in order to take immediate measures. In such a case, however, every effort shall be made to record the circumstances of the inspection of the e-mail account in such a way that its exact course, the range of data learned, i.e. the data processing operations actually performed and their lawfulness can be verified. This also follows from the principle of accountability.

However, considering that in both cases, the controllers did not take any measures to ensure that the applicants had prior knowledge of the inspection of the e-mail accounts, the search of documents or their presence, the Authority found that the controllers had violated the principle of fair data processing.

The Authority also took into account in both cases that none of the data controllers had internal rules regarding the use and control of e-mail accounts. Closely related to this issue is the need to ensure compliance with the relevant regulations and data protection requirements, as this will ensure compliance with the appropriate technical and organizational measures under the General Data Protection Regulation. The regulation of data processing in an internal document and the recording of data processing operations is necessary, because it also includes the administration and documentation of all essential steps taken from the planning of data processing through their continuation to the realization of goals, and presupposes the ability to prove compliance with data protection requirements. In practice, this principle envisages, among other things, the establishment of rules and procedures for data controllers in accordance with the provisions of the General Data Protection Regulation. Appropriate technical and organizational measures also include the fulfilment of the data protection by design and by default, i.e the facilitation of the principles and data protection requirements by the data controller by incorporating guarantees.

In the opinion of the Authority, in the case of non-regular, ad hoc inspections and document searches, it is not expected that detailed internal rules will be prepared in advance for the specific individual case, however, with regard to the possibility of such ad hoc inspections it can be expected that the manner in which such

inspections will be carried out will be documented and regulated in advance, as during a given inspection who and how may have access to the computing equipment and e-mail accounts of the employee concerned, so that employees have clear, unambiguous information, including the possibility of ensuring their presence

3. *The principle of purpose limitation related to data processing at workplace*

The Authority received requests objecting to the data processing of the applicants' employer. According to the complaint, the employer distributed a list at the management meeting that included data on trade union membership of 51 employees. The list was generated by filtering the payroll data of the employees. During the authority procedure for data protection, the Authority found that the employer lawfully processed the data of the data subjects concerning the trade union membership in order to deduct the trade union membership fee from the employee's salary. However, this authorization does not mean that the data processed for the purpose of deduction could be used for other purposes. With regard to the principle of purpose limitation, the employer as a data controller is obliged to process the data he or she learns about employees in accordance with the relevant data protection rules and, above all, to ensure that within the work organization, only those who necessarily participate in the achievement of the given data processing purpose, have access to each data. In the opinion of the Authority, data on trade union membership can only be accessed by payroll accountants within the employer's organization, and the employer shall take appropriate organizational and technical measures to ensure that others, even the manager, do not have access to these data without a lawful purpose. On the other hand, the data may not be used for purposes other than that for which the consent has been obtained. The processing of personal data for a purpose other than for which they have been collected is only permitted if the processing is compatible with the initial purposes of the data processing. With regard to the purpose, the employer should have applied Article 6 (4) of the GDPR and ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected. In the opinion of the Authority, it was not compatible with the initial purposes set out above that the employer, aiming to use the data for other purpose, gave an instruction to query the trade union membership data from the database used for payroll and handled the data received in a list. The Authority also stated that the transfer and disclosure of the queried data to the management was unlawful as the data of the applicants regarding the trade union membership were disclosed to the participants of the management meeting, including the superior of the applicant, without a law-

ful authorization. The Authority imposed a data protection fine of HUF 3 million which was paid by the data controller and a judicial review of the decision was not initiated. (NAIH/2472/2019)

II.1.2. Certain important, interesting cases

The most typical subjects with which applications for authority procedures were filed include the following:

- data processing at workplace
- camera surveillance
- healthcare data processing
- data processing related to claim assignment
- data processing by debt collectors
- data processing by banks
- data processing by insurance companies
- right of access
- the rejection or omission of fulfilling data subject rights

1. *Hidden camera surveillance at workplace for the purpose of control of the employees*

Several submissions were filed with the Authority in which the applicants objected to the fact, that on numerous occasions, for control purposes, the agents of privately held corporation controlling the provision of services (hereinafter: BKK Zrt.) made on several tram lines hidden camera recordings of the employees of the privately held corporation providing transport services (hereinafter: BKV Zrt.) using a hand-held camera. In the recordings, the driver of the vehicle was fully recognizable and identifiable. According to the submissions, the recordings were made without the drivers' knowledge, they did not give their consent and they were not informed about the inspection in any way. According to the submissions, BKK Zrt. enforces penalty claims against BKV Zrt. based on the possible violations revealed during this inspection. If the inspection does not reveal an irregularity, the employee of BKV Zrt. will not be informed about the inspection in any form. If BKK Zrt. finds an infringement, BKV Zrt. applies a premium deduction to the employee based on this.

An inquiry has been initiated in the case. During the period under review, provisions of the Privacy Act were applicable. However, given that the data pro-

cessing was also continuous after the date of application of the General Data Protection Regulation, on the 25th of May 2018, the Authority examined the compliance of the data processing with both the Privacy Act and the General Data Protection Regulation.

During the clarification of the facts of the case, both companies referred to Article 14 (6) of the Capital General Assembly Decree 20/2012 (14 March) on the performance of traffic management tasks in Budapest (hereinafter: Designation Decree) as the legal basis for their data processing, according to which the transport organizer is obliged to regularly check the quantity and quality standard of the services ordered by it. On the basis of this legal provision, the transport organizer is also entitled to control the activities of the service providers in an open and hidden way, as well as through trial use. In the event of non-compliant behavior of the employee of the service provider, the transport organizer is entitled to initiate the employer's action specified in the public service contract with the service provider.

In the course of the inquiry, the Authority formed the position that if this inspection of the services provided by BKV Zrt. is performed by an inspector, and the use of hand-held cameras is necessary, the use of hand-held cameras might be acceptable, if
an appropriate legal basis for data processing, as well as guarantees and adequate information are ensured.

In the opinion of the Authority, this legal basis in the case of BKK Zrt. may be Article 6 (1) (e) of the General Data Protection Regulation, according to which the processing of personal data is necessary for the performance of a task carried out in the exercise of official authority vested.

However, it can be said about data processing necessary for the performance of a task carried out in the public interest and in the exercise of official authority vested as legal basis, that according to the Hungarian legal environment, primarily Article I (3) of The Fundamental Law of Hungary, and the practice of the Constitutional Court,
the State may restrict the fundamental rights of the data subject, such as the right to informational self-determination, to the degree necessary and proportionate for safeguarding a fundamental right or protecting a constitutional value, that is, in the public interest. The condition of the application of this legal basis is therefore that a law or EU norm regulates the data processing activity necessary for the performance of a task, carried out by the data controller in the public

interest. At the same time, however, such legal provisions often define only the data controller's public tasks, procedural scope and obligations but not the detailed rules for the related data processing operations. If the legislator, without taking into account the provisions of Section 5 (3) of the Privacy Act, has failed to set forth the detailed rules of such data processing, the data controller is obliged to carry out its data processing activity in accordance with general data protection rules, particularly principles and the necessity measure of legal basis and to demonstrate its lawfulness in compliance with the principle of accountability.

In its inquiry procedure, the Authority found that, in contrast of the above, Section 35 (1) - (2) of Act XLI of 2012 on Passenger Transport Services, applicable at the time of the procedure and still in force, contains only that the entity responsible for the service, i.e. the Municipality of Budapest, may at any time check or entrust its agent to check the fulfillment of the obligation of the transport service provider, i.e. BKV Zrt. The Designation Decree provides for in the same way, according to Section 14 (6) of which the transport organizer i.e. BKK Zrt. is obliged to regularly check the quantity and quality standard of the service ordered. BKK Zrt. is entitled to control the activities of the service providers in an open and hidden way, as well as through trial use.

However, in the opinion of the Authority, none of these legal provisions - as they do not comply with Section 5 (3) of the Privacy Act - provides a legal basis complying with the applicable Hungarian constitutional and legal requirements for BKK Zrt. to control the services provided by BKV Zrt. in such a way that the work of the employees of BKV Zrt. is monitored with a hidden technical device. In its inquiry procedure, the Authority found this inspection to be unlawful, inter alia, for these reasons.

In the opinion of the Authority, however, the purpose of data processing is lawful and, the data processing may be necessary and proportionate, it is necessary that the legislator establish the data processing rules by amending the legal environment in accordance with Section 5 (3) of the Privacy Act, in order that the conditions for the application of the legal basis pursuant to Article 6 (1) (e) of the General Data Protection Regulation are fully ensured.

As a result of the above, the Authority addressed a recommendation to the competent ministry and initiated the amendment of the legislation(s) falling within the scope of regulation to the extent necessary and sufficient to fulfill the indicated legislative obligation. (NAIH/2018/127, NAIH/2019/4556)

2. *Unlawful camera surveillances*

During 2019, the Authority conducted a number of authority procedures and inquiries in connection with unlawful camera surveillance.

In one of these cases, the clarification of the facts of the case revealed that the individual complained against did not monitor the activities of his neighbour and the persons present there, on his own, but by mandating a private investigation company. On the basis of the facts of data clarified during the procedure and the evidences attached, it was found that the camera was installed specifically for the purpose of monitoring the neighbour, and that the recordings were handled by the private investigation company. Considering, that the purpose of the monitoring was determined by the individual, while the company decided on its means, methods and handling of the recordings, which was performed on the basis of an agency contract, their joint controller status could be established. Although the parties complained against claimed that they had informed the monitored persons of their activities, this did not provide an appropriate legal basis for the surveillance and did not make it lawful.
In its agency contract, the company stated that it would perform its work “as described in the data protection act”, however, no legislation authorizes private investigators to carry out such monitoring. The Act on the protection of persons and property and the rules of private investigation states that a private investigator does not have official authority in the course of his or her activities and that a private investigator may make or use video and audio recordings only in compliance with personal data protection and privacy rights. The Authority therefore prohibited the continuation of further monitoring, ordered its termination and the erasure of the unlawfully made recordings, and imposed a data protection fine of HUF 800,000 on the company. (NAIH/2019/3633)

3. *Surveillance camera operated by a neighbor in a condominium*

In an area of common property where there are several houses, one of the residents complained that his neighbour had installed a camera whose setting angle was objectionable. The Authority initiated an inquiry into the case. The neighbour did not respond to the request of the Authority or did not reply to the questions asked, so the Authority initiated an authority procedure ex officio. The neighbour sent his replies to the initiated authority procedure, at the same time he also filed a complaint against his three other neighbours, so three more authority procedures were initiated in connection with the case. In one case, the Authority found

that the field of view of the camera operated by the neighbour included public space, common area and private area of others, and therefore the data processing was unlawful, however, the Authority did not find any violation of law during the inquiry into the other neighbours. (NAIH/2018/4761)

4. *Data processing of security cameras operated at the head office of a local self-government*

The applicant objected to the data processing of security cameras operated at the head office of a local self-government. He complained about the fact of monitoring the employees in the building, the lack of providing prior information about it, and the fact that , among others, information on the identity of the person responsible for data processing, the time interval of the recording, the period of data storage, the scope of the authority of the inspection staff and the normative order of recording is not provided. In its decision, which was also published on its website, the Authority found that the data controller had violated the applicant's rights under the GDPR by unlawfully processing his image without providing appropriate information. The Authority extended the authority procedure ex officio to the general data processing practice of the local government related to security cameras. In the framework of this, the Authority stated that legitimate interest under Article 6 (1) (f) of the GDPR as legal basis, as identified by the controller, could not be used to processing carried out by public authorities in the performance of their tasks, because of the exclusion rule specified in the GDPR. The appropriate legal basis for data processing related to the operation of a local government could be Article 6 (1) (e) of the GDPR.

However, the necessity and proportionality of the data processing are also necessary conditions for this, and appropriate prior information shall be provided to data subjects. In this specific case, it shall be taken into account, among other things, that there is also political activity in the territory of the local government, as well as the national minority self-government is located in the same building, so the use of cameras can only be justified by more significant reasons than usual. In its decision of October 2019, the Authority prohibited the continuation of camera data processing violating the provisions of the GDPR and imposed a data protection fine of HUF 5,000,000. (NAIH/2019/2076)

Based on the above it is clear that the number of cases related to video and audio recording is still significant. As indicated earlier, the European Data Protection Board has adopted Guidelines 3/2019 on processing of personal data through

video devices, which aims to promote common understanding of the law in this area in the future, and is at the same time an appropriate point of reference for data controllers when planning and carrying out their data processing operations.

5. *Recording of personal data in the Electronic Health Service Area (EHSA) (Elektronikus Egészségügyi Szolgáltatási Tér - EESZT)*

During 2019, several submissions were filed with the Authority in connection with the Electronic Health Service Area (EHSA). The submissions show a great deal of uncertainty on the part of data subjects in connection with the operation of the system. Several submissions for consultation or initiating an inquiry also included a request to prohibit the uploading of data to the EHSA and to erase data already recorded. In its replies, the Authority drew attention to the fact that the recording of personal data in the EESC is mandatory data processing, for which the General Data Protection Regulation, furthermore Act XLVII of 1997 on the protection and processing of medical and other related personal data (hereinafter: 'the Health Data Act') and EMMI Regulation 39/2016 (21 December) containing detailed rules relating to the EHSA as Member State legislation provide an appropriate legal basis. On this basis, the Authority rejected requests where data subjects applied to the Authority to prohibit or erase the recording of their personal data including health data in the EHSA. (NAIH/2019/6839, NAIH/2019/1852)

6. *Data protection risks of using DNA analysis services*

In early 2019, several newspaper articles addressed the growing number of advertisements for family tree research and ethnic origin testing offering DNA tests that could be ordered online and performed easily. In its statement , the Authority drew attention to the data protection risks that this may entail, in part, the transfer of its own genetic data to laboratories outside the European Union, and in part that the results may not only carry unique information about the person using the service

5 https://www.naih.hu/files/2019-03-23-genetikai-adatok.pdf

7. *Recordability of incoming calls and identification of phone numbers by psychological first aid hotline providers*

A psychological first aid hotline service provider requested the opinion of the Authority on the data protection issues of the construction of a new telecommunication system, the recordability of incoming calls and the identification of phone numbers. The Authority explained that, based on what was said by those in crisis situation during the call, the called party may have access to data concerning health, therefore its data processing shall comply with the stricter conditions specified for the processing of data concerning health. The data processing shall have an appropriate legal basis provided for by Article 6 of the GDPR and at the same time the condition set out in one of the points of Article 9 (2) shall apply. Article 9 (2) (a) allows for the processing of health data with the express consent of the data subject. As a general rule therefore, the consent of the data subject shall be obtained at the start of the call. Without consent, the call cannot be recorded and the conversation and assistance shall continue without voice recording. In the opinion of the Authority, Article 9 (2) (c) of the GDPR, which allows for the identification of a phone number and location, can only be applied to prevent an immediate danger to life or crisis. However, data processing based on this provision is only possible as long as the situation of the calling party justifies it or until assistance is organized or provided to him or her, in accordance with the principles set out in Article 5 of the GDPR. However, the Authority found no adequate legal basis for recording or tracking for quality assurance or educational purposes without the consent of the data subject. Such processing could be based on the legitimate interests of the controller from the legal bases set out in Article 6, but Article 9 of the GDPR does not provide for an exception to the general prohibition on the processing of health data in this respect. The protection of the health data of the calling parties and their interest that their condition cannot be disclosed to others in a way that can be identified without their consent, overrides the quality assurance and other interests of the service provider. (NAIH/2019/5042)

8. *Taking photographs in a health care institution*

In her request for opinion, the applicant questioned the lawfulness of the recent practice according to which prior consent of the head of the state and local government-maintained health institution is required for anyone to take photographs on the premises of the institution. On the same subject, the Commissioner for Fundamental Rights also requested the Authority to deliver its opinion. In its

opinion, the Authority emphasized that state and local government-maintained health care institutions perform a public task. The conditions, circumstances and material conditions existing in these institutions concern issues that may be of public interest, thus, the recordings made in such institutions without containing personal data are considered to be of public interest in accordance with the Privacy Act, i.e. making and publication of such recordings cannot be objected to in terms of freedom of information. If natural persons also appear on the recording, the rights relating to personality must be taken into account in the matter. As consent to data processing is part of the right to informational self-determination as a fundamental right, the photographing of persons present in the hospital (whether sick, relatives or employees) may, as a general rule, be based on their consent in accordance with the Civil Code and the GDPR. It should also be taken into account that the recording of images of patients in a health institution may involve the processing of special categories of personal data, as the photograph may indicate the person's state of health, or the place where the image was taken may contain such information (e.g. in an intensive care unit, even in the case of a picture taken in the waiting room corridor with the visible name of the unit etc.). In the opinion of the Authority, the right to information self-determination as a constitutional fundamental right cannot be restricted by the head of the institution. Thus, if the person in the picture has given his or her explicit consent to appearing in a recording, his or her self-determination cannot depend on the instruction of the head of the institution. It is the responsibility of the person who makes the image to ensure that no such person appears on the recording who has not given his or her consent to the recording or data processing of the image. In the opinion of the Authority, a general and total ban on the taking of images disproportionately restricts the fundamental rights of data subjects guaranteed by the Fundamental Law. The head of the institution can be considered to act appropriately in order to ensure the rights in accordance with Section 2 of the Health Data Act, if he or she provides information to the patients of the institution and other persons visiting the institution by placing information material in a visible manner, in several places, or in any other way that draws the attention of patients and relatives to the rules for taking pictures of other persons, the rights of the data subject and the obligations of the photographer. (NAIH/2019/2741, NAIH/2019/3406)

9. *Providing copy of documentation in connection with hospital care*

One applicant had an accident in 2015 that resulted in him receiving hospital care. In 2016, he submitted a complaint in connection with the hospital care, on

the basis of which an investigation procedure was initiated in the hospital concerned, and a procedure was also initiated at ÁNTSZ (National Public Health and Medical Officer Service) based on the Complaints Act. In 2019, the applicant requested the hospital several times to send certified copies of the documents issued in connection with the investigation procedure, and the investigation conducted by ÁNTSZ. The hospital set determined a reimbursement fee for sending the requested documents, given that the applicant had already received the requested documents when he left the hospital. The applicant paid the reimbursement fee. The hospital sent the copies of the requested document to the applicant 84 days after his request was submitted.
The Authority found that the hospital had violated Article 13 (3) of the GDPR by failing to provide information on action taken on the request within one month of receipt of the request, as well as Article 15 (3) of the GDPR by failing to provide the first copy free of charge, and determined a reimbursement fee. The applicant's request for a copy submitted after the GDPR became applicable shall be regarded as a first request for access, therefore no costs can be charged. The Authority rejected the request to receive copies in certified form, since Article 15 (3) and the principle of accuracy under Article 5 (1) (d) of the General Data Protection Regulation do not imply an obligation for the data controller to certify the actual content of the copy by means of an authentication. Pursuant to Article 58 (2) (d) of the General Data Protection Regulation, the Authority ex officio instructed the hospital to bring its internal reimbursement fee rules in compliance with the provisions of the General Data Protection Regulation. (NAIH/2019/5112)

10. *Access to the healthcare documentation of a deceased person*

The processing of personal data concerning the circumstances of the deceased person's death and the cause of death and the personal data contained in the healthcare documentation shall be subject to the rules laid down in legally binding European Union act or legislation on the processing of health data and personal data contained in the healthcare documentation. From 25 May 2018, the GDPR provides for the main rules of personal data processing. However, according to recital 27, the GDPR does not apply to the personal data of deceased persons, and therefore Member States may provide for rules regarding the processing of such data. In Hungary, using the opportunity provided by the GDPR in connection with the processing of the personal data of deceased persons, the provisions of the Privacy Act, which entered into force on 26 July 2018, provide for the exercise of the rights relating to personal data after the death of the data subject. However, without a statement made in the life of the data subject,

this only allows the close relatives of the deceased data subject to terminate or rectify the unlawful processing. Based on other legal regulations, however, it is possible to exercise additional data access rights, e.g. Act XLVII of 1997 on the Protection and Processing of Medical and Other Related Personal Data ('Health Data Act') and Act CLIV of 1997 on Health ('Health Act') provide for health care documentations and the access to health data. (NAIH/2019/5831)

11. *Personal data processing beyond retention period*

The applicant became a customer of the data processing bank due to a loan contract. At the time of termination of the contract, there was a disagreement between the bank and the applicant on the amount of the settled and remaining debt. The bank assigned its claim to a winding-up institution. Following the correspondence, the winding-up institution initiated a payment order procedure against the applicant, which became a lawsuit due to a statement of opposition. In the litigation, the winding-up institution did not possess the bank documents supporting the claim (current account statement, balance statement), they were submitted by the bank. According to the court of first instance, the claim lapsed, and the judgment was upheld by the court of second instance. After receiving the final and binding judgment delivered in the second instance, the applicant requested information on which of his data considered as bank secrets are processed by the bank, and which of his other personal data they process, as well as requested information on the duration of the data processing. The Authority found that in addition to the data processed on the appropriate legal basis, the bank also processed data of the applicant in accordance with the provisions of the Act C of 2000 on Accounting (hereinafter: 'the Accounting Act') requiring the fulfillment of the obligation to retain documents, but the specified period of retention has already passed. Such data include the applicant's marital status, telephone number, name and telephone number of his / her employer, e-mail address and data related to his / her closed bank account. In the absence of a valid contract, the controller could not prove the existence of any of the legal bases set out in Article 6 (1) (a) to (f) of the GDPR regarding the personal data processed beyond the required retention period, therefore the Authority ordered their erasure and imposed a data protection fine of HUF 2,000,000,. (NAIH/2019/2113)

12. *Information on the identity of the controller*

In a claims management case, the data subject submitted several requests to two different data controllers, who, jointly process the data subject requests. There was no indication in the reply letter sent to the data subject that the responding controller had responded to the data subject's request, which was sent to another controller. The letter did not provide the data subject with any information regarding the fact that the data controller whom the request was originally addressed to forwarded the data subject's request to the data controller from whom he eventually received a reply. The Authority did not accept the argument of the data controller, who responded to the data subject according to which they complied with the transparency requirement, also by the fact that the letters sent to the data subject always indicated that the data subject's request was addressed to its intermediary approved by the MNB (Hungarian Central Bank). In the opinion of the Authority, however, no conclusions may be drawn from this statement, as to the quality of being data controllers or processors. The Authority also couldn't accept the argument of the controller, according to which the data subject should have been aware of the circumstances of the data processing, because the „communication with the data subject was continuous" regarding the fact that the claim had been managed for more than nine years. Given the fact that the respondent controller who sent the response did not provide the data subject with adequate prior information on the identity of the controller entitled to deal with requests for erasure, and the response letter also did not indicate to the data subject that the controller's response was a data controller action following a request submitted to another controller, the Authority found that the responding controller violated the principle of transparency. (NAIH/2019/4424)

13. *Information on the processing of the personal data of the data subject in case of claims management*

A winding-up institution did not provide information within one month of receiving the request, and then, only after becoming aware of the authority procedure, provided incomplete information on the processing of the data subject's personal data. The information did not include exactly what personal data concerning the data subject were processed in connection with the fulfillment of the legal obligation under the Accounting Act, Act CCXXXVII of 2013 on Credit Institution and Financial Enterprises and Government Decree 42/2015 (March 12) on the protection of the IT system of financial institutions, insurance and reinsurance companies, as well as investment companies and commodity exchange service

providers. This made it impossible for the data subject to see how the personal data concerning him or her were processed, thereby violating the principle of transparency under Article 5 (1) (a) of the GDPR. In view of the fact that the subsequent information was also incomplete, the Authority ordered the winding-up institution to provide a response in accordance with Article 15 (1) (a) - (h) of the GDPR and imposed a fine of HUF 300,000. (NAIH/2019/4424)

14. *Data processing practices of a financial enterprise related to investment services*

The Authority examined the general data processing practices of a financial enterprise in relation to investment services. The two main points in the examination of the processing of personal data in the aptitude tests conducted by the enterprise were the legal basis (Article 6 GDPR) and the information (Article 13 GDPR). Under the Investment Enterprises Act, financial enterprises are only required to complete an aptitude test with their clients when using certain investment services (investment advisory service, portfolio management). The examined financial enterprise has always completed the aptitude test with its clients when entering into a contract with them, under which they have become eligible to use a portfolio management or investment advisory service. The financial enterprise did not examine whether its clients eligible to use the investment service and portfolio management actually intended to use these services, or whether they chose this type of contract only because of other benefits arising from the contract. The financial enterprise processed the personal data of its clients who do not use investment services and portfolio management based on their legitimate interests, but did not justify the priority of its own legitimate interests over the rights and freedoms of the data subjects in the interest balance test. He informed his clients about the processing of personal data collected in the new investor (MiFID) questionnaires in several different documents, some with different content. None of the documents included that, in certain cases, the financial enterprise would process the personal data of its clients provided in the aptitude test based on its legitimate interest, thus making it impossible to exercise the right to object. When imposing the fine, the Authority weighted the following circumstances: this was not the first time that the financial enterprise violated the provisions of the GDPR, and a warning would not have been a proportionate and dissuasive sanction. It was assessed as an aggravating circumstance that the infringement persisted during the period under investigation and that both infringements affected a large number of data subjects.
Inappropriate information indirectly impeded the exercise of the data subject right to object, and the lack of transparency of the information is to be consid-

ered as a serious violation, as the financial enterprise had to provide information to data subjects on specific professional issues that the average data subject could not access from other sources. It was an attenuating circumstance that the financial enterprise stated that one of the purposes of its data processing on the basis of its legitimate interest and its legitimate interest in data processing was to ensure greater protection of investors. (NAIH/2019/3107)

15. *Transfer of personal data by transfer of a claim*

Applicants objected to that after taking a bank loan from a financial institution, the outstanding claim was purchased by a company and the applicants 'personal data was also transferred to the data controller upon transfer of the claim. In the opinion of the applicants, the company processed their personal data unlawfully as it did not have a license to claims management. The applicants turned to the Hungarian Central Bank (MNB), which initiated a market surveillance procedure and stated in its decision, that the company was engaged in receivables purchase financing activities without the permission of the MNB. According to the applicants, during the proceedings of the MNB, it was established that the company also had unlawful access to their personal data. The company has become the owner of the claims against the applicants under the assignment agreement and processes their personal data for the purpose of enforcing the claims and in order to enforce the debtors to perform. This data processing purpose alone is considered lawful. However, in view of the fact that the MNB found in the market surveillance procedure that the company carried out the receivables purchase activity without permission, and prohibit the company from carrying out this activity, the Authority is of the opinion that the data processing related to this unlawful activity and its purpose also needs to be considered as unlawful. The Authority upheld the part of the request concerning the finding of unlawful data processing and found that the winding-up institution processed the personal data of the applicants in the course of its unauthorized receivables purchase activities on an inappropriate legal basis, and for unlawful data processing purposes. The Authority established that the data processing of the company was unlawful. It ordered the restriction of the processing of the personal data concerning the applicants, as well as prohibited the data controller from using them for the purpose of claims management, and imposed a data protection fine of HUF 1,000,000 as an additional sanction. (NAIH/2019/1598)

16. *Data processing practice of the Hungarian National Fishing Association (MOHOSZ) during the fishing card application process*

The Authority received several complaints in which the complainants objected to the data processing of the Hungarian National Fishing Association (hereinafter: MOHOSZ) regarding the practice of requesting a photocopy of the tax card during the fishing card application process, both online and in person. An inquiry has been launched into the case. MOHOSZ referred to data processing necessary for the performance of the contract, the consent of the data subject and the legitimate interest of MOHOSZ as the legal basis of the data processing, and its privacy policy also referred to the accounting legislation regarding the data on the invoice. In order to decide on the lawfulness of the data processing, in addition to the legal basis, the purpose for which MOHOSZ requested the copies of the documents had to be examined, as well as the adequacy of this data processing to achieve the given purpose. The data processing purposes indicated by MOHOSZ: customer identification, checking the accuracy of personal data, risk analysis.

The data in the copy of the tax card is also considered personal data. In the opinion of the Authority, MOHOSZ has no statutory obligation to handle the tax identification number, either for personal identification purposes or for billing purposes. The tax identification number is not a mandatory content element of an invoice to be issued to a citizen as a certificate. In the inquiry, the Authority established that MOHOSZ does not have a legal authorization to handle the tax identification number, therefore pursuant to Section 7 of Act XX of 1996 on the methods of identification and using of identification codes which replace the personal identification mark (hereinafter: the 'Identification Act'), the legal basis for its processing can only be the consent of the data subject, if the data processing has a lawful purpose. In the opinion of the Authority, the consent as indicated in the privacy policy is not an appropriate legal basis for data processing, because one of the conceptual elements of a valid consent that it shall be freely given, which only takes place if the data subject freely, free from influence decides to make a legal declaration authorizing data processing. In addition, pursuant to the Identification Act the citizen cannot be disadvantaged due to the granting, refusal or revocation of the consent, however, the fact that the client is unable to register in the absence of the consent obviously qualifies as an influence or disadvantage.

MOHOSZ referred to data processing necessary for the performance of the contract and also its legitimate interest as the "possible" legal basis for the process-

ing of the tax identification number. However, the use of these "possible" legal bases is contrary to what is provided for in the Identification Act, as identification codes, including the tax identification number of natural persons, may be used only on the basis of the authorization of law or, in the absence thereof, the prior written consent of the person concerned or the consent given in the administrative order. Concerning the reference to the legitimate interest of the data controller, the Authority drew MOHOSZ's attention to the fact that the fundamental rights of the data subject have priority in this case, the mere fact that they intend to prevent possible abuse is not sufficient to use the tax identification number as a universal identifier. Thus, MOHOSZ shall not use the tax identification number for registration purposes and must delete the collected tax identification number data. (NAIH/2019/3620)

17. *Disclosure of personal data revealing ethnic origin*

In an inquiry which started in 2018, but ended in 2019 an individual objected to the fact that the online version of a foundation's yearbook listed in the name list the fact, that he had received a scholarship available for ethnic students in higher education. The complainant said he did not consent to the disclosure of the special data revealing his ethnic origin, when he signed the scholarship agreement. In the absence of the data controller's cooperation, the Authority assessed the complaint on the basis of the attached documents. The Authority established that the processing started under Act LXIII of 1992 on Personal Data Protection and the Publicity of Data of Public Interest, however during the preparation for the application of the GDPR, according to recital 171 of the GDPR, the data processing already under way on the date of application of the Regulation should have been brought into conformity with the Regulation. As the data processing continued in 2019, the rules of the GDPR apply to the disclosure of ethnic origin as sensitive data, and in addition to the legal basis set out in Article 6 of the GDPR, the data processing shall also comply with the restriction under Article 9, which is in line with the lawful purpose of the processing. In the opinion of the Authority, monitoring the transparent operation of the Foundation can be carried out and ensured without disclosing the sensitive data, if the list of scholarship recipients is otherwise available on paper and made available to the interested party on request. Disclosure of non-personally identifiable public information, such as how many people have received scholarship and how much they have received, is sufficient for anyone to control, while indicating that the details can be viewed in the places provided, especially if they do not have an appropriate legal basis for disclosure of data. The fact that the processing is limited to the data content necessary to

achieve the purpose, on a lawful legal basis, and in accordance with the principle of purpose limitation and data minimization pursuant to Article 5 (1) of the GDPR, in the absence of a reply, has not been demonstrated by the controller. Nor has it been demonstrated why it is currently necessary to make sensitive data available to anyone in order to achieve transparency as a data processing purpose. If, according to the original documents, the complainant had also given his consent to the disclosure but withdrew it in the exercise of his right under the GDPR, the controller would still have had to review the lawfulness of the processing under GDPR rules and consider that, despite the withdrawn consent, on what legal basis, in accordance with Article 6 and in accordance with Article 9, data processing for the purpose of controllability and transparency as a data processing purpose may be based. Accordingly, the Authority found that the foundation had no legal basis for the public disclosure of the complainant's name and ethnic origin. Upon receipt of the Authority's reply, the complainant informed the Authority that he had contacted Google with a reference to the reply and requested the removal of the disclosed data, which Google complied with, so that the data on the complainant's ethnic origin would no longer appear as a hit if entered in the search engine. (NAIH/1101/2019)

18. *Disputing the accuracy of personal data processed*

A complainant received an email from a service provider addressed to another customer of the service provider. The problem was that the two people were called the same and their email addresses were similar. The complainant reported the problem to the service provider, but the service provider stated that he had contacted his customer, but his customer confirmed that the e-mail address attached to his name was correct, so the service provider could not delete the e-mail address and continued to send emails to the complainant. After lengthy consultation, they were able to agree with the client to attach a different email address to his name, so the issue was resolved. The reason for this complaint is that Gmail does not differentiate between email addresses including a „dot" and without a „dot". As a result, it was possible that (also) the complainant registered with the e-mail address x.y@gmail.com received notification of the completion of the invoice sent to the e-mail address of the customer registered with the e-mail address xy@gmail.com. The service provider has informed the Authority that in the future it will regularly check the email addresses of its subscribers' Gmail accounts where the difference is only a „dot" and contact them to avoid further problems. The Authority drew attention to the fact that in the future, if the accuracy of personal data is contested, the service provider should act in

accordance with Article 18 (1) (a) of the GDPR, which requires the controller to restrict the processing if its accuracy is contested. The Authority drew the attention of the controller to the development of practice in accordance with Article 32 (1) of the GDPR. Such practice could be, for example, if somebody want to register a Gmail email address where only one „dot" is different from an existing Gmail email address, it shouldn't be allowed to be registered. (NAIH/2019/776)

19. *Language requirements of a privacy policy*

A British company, a company not active according to the British company register, which therefore would not be able to carry out economic activities, so it would also not be able to provide services to Hungary. The owner resides in the Czech Republic and the complainant lives in Hungary. As an example, we would cite two paragraphs from the privacy policy of the complained company with the remark that according to the Fundamental Law, Hungary protects the Hungarian language. The interesting thing about the case is the language-degrading policy itself. Quote:
"Everyone at our company consider the use of personal data very importantly and meaningfully and accordingly it should treat. Please you read carefully how we protect personall information of you. Should any of them bee unaware, please lett us know. " […] "We only use profiled and automated processing in our marketing campaign for the purpose of inventing our targeted products and services — we want to offer a table that is relevant to them and not burdened with redundancy. We do not use profiled (automated) or automated processing with automated decisions that would have legally consequences for you or significcantly affect you." The lesson of the case is that language imperfections sometimes hinder or slow down efficient administration, and at the same time do not meet the requirements set out in GDPR related to the transparency of data processing. (NAIH/2020/83)

20. *Election-related data processing*

In 2019, the Authority received several complaints about the practice of collecting large numbers of personal data from voters in addition to collecting election-related recommendations. The data were collected mostly for the purpose of building a database of sympathizers, as well as in connection with certain signatures and civil initiatives - both expressly and explicitly in support of a specific goal.

In this regard, the Authority drew attention in its recommendation issued in April 2019 on election-related data processing to the fact that data collection can only take place for a well-defined, lawful purpose in any case. The purpose shall be indicated in accordance with the requirement of fair data processing and shall not be misleading. In its recommendation, the Authority specifically mentioned that data collection which takes place at the same time as the collection of recommendations, but for a different purpose (such as building a database of sympathizers), is considered as an independent data processing for a purpose other than the nomination of the candidate, of which the data subjects shall therefore be informed by indicating this data processing purpose. In this respect, the Authority explained that if a citizen provided his or her data only for the purpose of a political initiative (such as a local or national petition), this data should be erased as soon as the processing has achieved its purpose and even if the purpose of the processing has failed. However, in most cases, in addition to the initiative, the data subject may also provide his / her personal data (in particular his / her name, e-mail address, telephone number) for later contact. The use of the contact details thus provided for contact purposes, if provided by the data subject without any time limit, is lawful as long as the data subject does not initiate the erasure of his or her personal data with the data controller.

In its application for authority procedure for data protection received by post on 17 September 2019, the applicant (who was the chairman of the board of directors of municipally owned companies at the time of application) stated that municipal representative of Budapest VIII. district (who became deputy mayor after the October 2019 municipal elections) published a photo of the applicant in a post on its official (i.e. not private) Facebook page, to the taking and publication of which the applicant did not give his consent. The applicant stated that at the moment the photograph was taken, he immediately drew the data controller's attention on the spot not to use his image and not to publish it on any social site because he was not willing to give his consent. His minor daughter who was present at the conversation, was also pictured. Although her face was obscured, but since it was written in the post that she could also be seen in the picture, she became easily identifiable. The applicant further stated that he had tried to contact the data controller in writing in order to remove the post, but the data controller did not comply with its request.

Following receipt and assessment of the statements required to clarify the facts of the case, the Authority adopted a decision on the matter on 4 March 2020 stating that:

– The name of the applicant was considered to be data accessible on public interest grounds at the time of taking and publishing the image, however, his image cannot be considered data accessible on public interest grounds pursuant to Section 26 (2) of the Privacy Act, considering that his appearance is not relevant to performing public duties.
– The photograph was not taken when the election announcement was destroyed, but after it, thus it does not show the alleged violation, but only the fact that the applicant crosses a designated pedestrian crossing with an unrecognizable piece of paper in his hand. The photograph therefore shows, on the one hand, a moment in the applicant's private or family life which cannot be considered a public appearance and has no connection with the performance of public duties and the exercise of fundamental rights to ensure free discussion of public affairs, and on the other hand the photograph does not at all prove that what is written in the post corresponds to reality. The consequence of this is that the consent of the applicant would have been necessary for the taking and publication of the photograph. The right to the freedom of expression, the purity of the elections and the balanced information of the voters indicated by the data controller cannot be accepted as a valid legal basis.
– The image published in the post does not have a separate value of additional information contributing to the discussion of public affairs, a text entry without the image would have been sufficient to inform the public.
– Neither the taking of a photograph nor its publication is compatible with the purpose set out by the data controller, namely the recording and disclosure of an offense. On the basis of the statements and documents obtained during the procedure, it could not be established that the interest in taking and publishing the image had priority over the applicant's interests and data protection rights, or that the data processing would have been necessary for the performance of the duties in a task carried out in the public interest or in the exercise of official authority vested in the data controller.
– The data controller did not provide any response or information to the request of the applicant in the framework of the exercise of the data subject rights in the manner and within the time period specified in Article 12 (3) - (4) of the General Data Protection Regulation. The data controller's statement that he did not respond to the applicant's request because he considered it part of the campaign cannot be accepted.
– The image remained available on the data controller's Facebook page for several months after the October 2019 municipal elections, despite the

fact that the applicant has not held the position of chairman of the board of directors of municipally owned companies since November 2019.

In its decision, the Authority obliged the data controller to remove the post, and imposed ex-officio a data protection fine of HUF 100,000 on him, because the data processing without the appropriate legal basis and purpose significantly affected the applicant's privacy. In addition, a violation of law with regard to the exercise of the data subject's right has taken place, the data controller has infringed several articles of the General Data Protection Regulation [Article 5 (1) (a) to (c), Article 6 (1), Article 12 (1) to (5), Article 15 (1), Article 17 (1)] and the violation was caused by the intentional behavior of the data controller. [NAIH/2020/32 (NAIH/2019/6885)]

21. *Information in case of data processing related to collecting signatures*

In a further procedure initiated to examine the lawfulness of data processing related to the collection of signatures, the Authority explained that appropriate information is a conceptual element central to the application of the data subject's consent as a legal basis, which is closely linked to the implementation of all conceptual elements of the consent, such as freely given, specific and unambiguous. This is necessary in order for data subjects to have appropriate information on exactly what they consent to, to know the details of the data processing and to exercise their right to withdraw their consent. In connection with the provision of appropriate information, the General Data Protection Regulation also sets out substantive and formal requirements for data controllers. (NAIH/2019/5062)

22. *Processing of the personal data of the applicant in case of electronic administration*

The Authority has received several submissions concerning electronic administration (such as ePaper submissions) in which all personal data used to identify the submitting representative (managing director, lawyer etc.) form part of the submitted application, and will be attached to the file and forwarded to each party in a given case (for example, to the other party in a lawsuit). This data processing is mandatory by law, and National Infocommunications Service Company Limited by Shares (NISZ) only performs the role of data processor according to the law, it cannot determine the conditions of data processing. Therefore, in 2019, the Authority initiated the amendment of Government Decree 451/2016

(December 19) on the detailed rules of electronic administration at the Ministry of Interior, in order to comply with the requirements of necessity and proportionality of the GDPR. Under a new provision proposed by the Ministry of Interior on the initiative of the Authority and commented on by the Authority, the personal identification data of the applicant may only be processed to the extent necessary for his / her identification until the end of the identification. This legislative amendment is still in progress

23. *Obligations of the data controller in case of an official request*

In the course of its administrative procedure, a data controller has filed a request with another data controller in order to request information on the final and binding decisions taken by the requested data controller in the previous two years in connection with an ongoing case. The requested authority sent a copy of its decisions in the case, which also contained the personal data of a person not involved in the case pending before the requesting authority.

Fulfilling an official request constitutes mandatory data processing under Article 6 (1) (e) of the General Data Protection Regulation. During the fulfilment of the request, the provisions of the Administrative Procedure Act and the rules of the General Data Protection Decree shall also be complied with. Accordingly, the requested data controller, merely by complying with the official request, is not exempted from the obligation to comply with the principles of purpose limitation and data minimization of the General Data Protection Regulation during the transfer. In the context of complying with the request, the requesting authority is in a position to determine the scope of the data necessary to establish the facts in its own case, including the scope of personal data, so it is primarily its responsibility to decide, within those legal limits, whether the request is also necessary regarding personal data. However, this does not mean that any official request should necessarily and automatically be interpreted by the requested person as covering any range of personal data indiscriminately. The requested controller shall, where appropriate, carry out the assessment and take the necessary measures (e.g. anonymization in the final / binding decision sent). (NAIH/2019/13)

24. *Unlimited retrieval of vehicle data based on license plate number*

In his submission the Commissioner for Fundamental Rights obliged to that, as a result of an amendment to the law, an unlimited retrieval of vehicle data, including personal data, became possible on the basis of the license plate number, which, according to him, could lead to misuse. In its response, the Authority pointed out that

in the Preamble of Act LXXXIV of 1999 on the Road Traffic Register the legislator indicated that, taking into account the protection of personal data, the law exhaustively determines the scope of data that can be registered, the data sources of the register, the duration of data processing, the scope and limits of data provision,

the scope of those entitled to request data and the data protection rules. The Authority also pointed out that the amendment to the legislation extended the already existing possibility of data request by electronic retrieval. As the amendment does not allow for misuse but, on the contrary, it serves the public, direct and free of charge electronic verification of data on motor vehicles involved in road transport and the submission did not have any further data protection relevance, no inquiry has been launched. (NAIH/2019/1424)

25. *Archiving of personal data contained in library documents in the public interest and their processing for scientific and historical research purposes*

In a submission, the Authority was requested to deliver its opinion on archiving of personal data contained in library documents in the public interest, and on their processing for scientific and historical research purposes. The storage, preservation and digitization of personal data contained in library documents that are part of the collection of libraries, is considered data processing. In this regard, however, it is worth noting that the GDPR does not apply to the personal data of deceased persons. In the opinion of the Authority, one of the possible purposes of data processing in the context of library activities is archiving in the public interest. The GDPR should also apply to data processing for archiving purposes, as explicitly referred to in Recital 158. The digitization and disclosure of documents containing personal data is also considered to be data processing under the GDPR, so it is an essential condition for its lawfulness to have an appropriate legal basis in addition to its lawful purpose. In the opinion of the Authority, the legal basis for the processing of libraries in the performance of their statutory tasks could be Article 6 (1) (e) of the GDPR, as such processing is necessary for the performance of a task carried out in the public interest. Pursuant to the first par-

agraph of Article 89 of the GDPR, the processing of personal data for archiving purposes in the public interest, scientific and historical research purposes shall be carried out with appropriate safeguards protecting the rights and freedoms of the data subject. This therefore means that the data controller shall design the data processing in such a way, that they comply with the provisions of the GDPR. The GDPR only allows the Member State legislator to provide derogations from the GDPR's rules on the exercise of data subject rights if the purpose of the data processing is archiving in the public interest, and even the GDPR itself contains such exceptions. According to Article 17 (3) of the GDPR, the obligation for the controller to erasure shall not apply if the processing is necessary for the performance of a task carried out in the public interest, or for archiving purposes in the public interest in so far as the exercise of the data subject's right to erasure is likely to render impossible or seriously impair the achievement of the objectives of that data processing. If the legal basis for the processing is Article 6 (1) (e) of the GDPR, the data subject also has the right to object. If the data subject objects to the processing, such as the publication of a digitized newspaper article containing his or her personal data, the controller shall no longer process the personal data unless the controller compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject. This consideration must be carried out on a case-by-case basis by the controller, taking into account the interests and rights of the data subject exercising the right to object. However, libraries cannot modify the content of digitized library documents in such cases either, as their task is to take care of the collection, which goes hand in hand with preserving the integrity of the documents. (NAIH/2019/1342)

26. *Posting the names of persons being in arrears in the stairwell*

Posting the names of persons being in arrears in the stairwell is a recurring problem. According to Act CXXXIII of 2003 on Condominiums (hereinafter: 'the Condominiums Act'), the general meeting shall decide on the adoption of the annual accounts. It is therefore necessary for the general meeting to be able to get acquainted with the data contained in the accounts when submitting or approving the annual accounts, such as the requirement to contribute to the common costs and the extent of their fulfillment by indicating the names of the co-owners. There is therefore no legal obstacle for co-owners to know the identity of persons who are in arrears in the payment of common costs. The way to find out can be, for example, by a closed prospectus thrown into the mailbox, an inspection of the books, or a closed general meeting (held only with the participation of the co-

owners) explaining the names of the co-owners being in arrears and the amount of the arrears. Data on the arrears of a natural person for common costs are data that can be disclosed to the co-owners, which however, maintain the quality of personal data, so the principle of purpose limitation of the General Data Protection Regulation must be enforced when processing and using personal data relating to common costs. In accordance with the principle of purpose limitation, the condominium representative and the co-owners shall respect the individual's rights relating to personality with regard to the data, which come to their knowledge in connection with the operation of the joint property, and shall use such data for the initial purpose. Thus, providing information may be lawful if it is necessary to know the budget of the condominium and does not allow an unauthorized person other than the co-owners to know the common cost accounting containing the personal data. For the reasons detailed above, making the names of persons being in arrears available in a stairwell or other public place violates data protection rules, as the disclosed personal data can be learnt by persons other than the co-owners. (NAIH/2019/2223)

27. *Right to information of the parent not exercising parental custody*

A parent who does not have parental custody and is separated from his child is unable to track the child's academic performance because the other parent has not provided the information needed to use the electronic diary. In the opinion of the Authority, the child's academic progress shall be considered as substantial matter affecting the future of the child in accordance with the provisions of the Civil Code. A parent without parental custody has the opportunity to request information about the child's academic progress from the school, the teacher and the other parent. In the opinion of the Authority, a parent who does not exercise parental custody is only entitled to know the information necessary to decide in substantial matters. However, the Authority is not entitled to assess the extent of the content of the information on which the decision in substantial matters under the Civil Code is based. Considering the legal uncertainty is caused by the fact that different institutions have different interpretations of which data they are entitled to disclose in the context of information, and whether they are obliged to verify the exercise of parental custody, the Authority has asked the Commissioner for Fundamental Rights to examine this issue. (NAIH/2019/2202)

II.1.3. Cross-border cases

The Authority cooperates with data protection authorities in other Member States of the European Union under the GDPR. In 2019, the Authority was involved in hundreds of cross-border data processing cases as concerned authority, which accounts for about one third of all cross-border cases, and there were cross-border data processing cases in which the NAIH acted as the lead supervisory authority. These cases are briefly described below.

1. A complaint about the free version of the antivirus of a security software company was filed with the Dutch Data Protection Authority on 25 May 2018. According to the complainant, the privacy settings in the free version were disabled and could not be changed, which, according to the complainant, violated the data subject rights under the GDPR. The Czech DPA as the supervisory authority of the main establishment of the controller acted as the lead supervisory authority pursuant to Article 56 of the GDPR, and the data protection authorities of all EU Member States were involved in the procedure as authorities concerned. The Authority expressed a relevant and reasoned objection to the first draft decision of March 2019, as the subject matter of the procedure and the legal consequences were not properly indicated. Subsequently, the Czech DPA extended the justification for the draft and indicated that it would set out the legal consequences separately in a second decision under its procedural law. Thus, the Authority adopted the new draft decision in August 2019.

Under the GDPR, all data that can be linked to a natural person, even indirectly, is personal data, including the dynamic IP address and the unique number assigned by the company to a particular end-user device and installation. It was also found that the controller had violated Article 24 (1) of the GDPR, i.e. failed to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that the processing of personal data is performed in accordance with the GDPR. (NAIH/2019/1257)

2. One complainant turned to the Authority as he had provided his personal data years ago when buying a television from a large electronics company because the data controller had given him an additional 1 year warranty in exchange for registration. Since the extended warranty had already expired, he requested the erasure of his personal data. On the website operated for the exercise of the data subject rights, the data controller has, inter alia, made it necessary to upload a scanned version of an identity document in order to accept the data subject's request, both in the case of erasure and in the exercise of other rights. Therefore,

the Authority initiated the procedure of the Information Commissioner's Office (ICO) of the United Kingdom acting as lead supervisory authority under the GDPR, and participated in the procedure as a concerned authority. According to the ICO's draft decision, the controller reviewed its procedures and decided to change its practice regarding data subject requests.

Based on the above, the ICO sent its draft decision to the Authority stating that no further action was required. The Authority made minor comments which did not constitute an objection and proposed clarifications to the draft decision. (NAIH/2019/331)

3. The complainant complained to the Authority that he had applied for a job at a Hungarian branch of an international bank, but, as no agreement had been reached, he asked the controller to erase his personal data from all his systems. According to the data controller's reply in English, the complainant's request was not fulfilled, as personal data of candidates are kept for two years from the last job application submitted, in accordance with their internal rules. The Authority initiated an inquiry into the case and sent a request for clarification to the controller. Based on statements of the bank and the privacy policy available on its website, the main establishment of the data controller is in London, therefore the Authority has initiated the procedure of ICO being the lead supervisory authority under the GDPR. The Authority participates in the procedure as concerned supervisory authority. (NAIH/2019/2542)

II.2. Personal Data Breaches

In its previous annual report, the Authority provided general information on the notification and handling of personal data breaches, as well as the most common types of data breaches and the measures for their prevention and remediation. This year, the Authority has decided to provide a brief summary of some typical and interesting cases from last year, with the intention of drawing the attention of data controllers to key aspects of dealing with personal data breaches in order to prevent the mistakes and deficiencies described in the cases.

1. In the case of personal data breach in a primary school, the Authority found, based on the facts of the case revealed, that from December 2018 till February 2019, a list containing the name, class and other more sensitive personal data of children attending school (i.e. whether the child is disadvantaged or multiply disadvantaged, has special educational needs or receives regular child protection benefits) was publicly available on the controller's website. The document was prepared for internal use, and it could only have been accessed by the teaching staff after providing a username and password.

The Authority became aware of the personal data breach on the basis of a submission and the controller did so no later than on receipt of the decision of the Authority. However, the controller did not identify the case as a personal data breach and nor did it fulfill its obligations under the relevant provisions of Articles 33-34 of the General Data Protection Regulation: it did not carry out an analysis of the risks of the personal data breach, did not notify the personal data breach to the Authority, nor did it invoke the exception to the obligation to notify. In addition, it has not complied with its obligation to document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken

In its decision, the Authority found that the examined personal data breach was considered to be high risk, as unauthorized access and disclosure of the personal data concerned could result in social disadvantage due to their nature, consequently the data controller should have to communicate the personal data breach to the data subjects, without undue delay in accordance with Article 34 of the Data Protection Regulation. Although the controller notified the parents and guardians of the data subjects about the case, it did so more than four months after becoming aware of it, and not with the content required by the Regulation. It was also assessed as a risk-increasing factor that the data controller could not determine the cause of the personal data breach. The Authority also stated on

the basis of the data controller's statement that it did not create a separate regulation regarding the permissions of the interface available after login.

However, in assessing the personal data breach, the Authority considered the following as mitigating factors:
a) in the course of the proceedings, the Authority has not become aware of any information indicating that the persons concerned have suffered any damage by the infringement;
b)) it can be inferred from the facts of the case established that the infringement was not intentional, but it was caused by the data controller's negligence;
c) the controller has infringed the rules on the processing of personal data for the first time;
d) the controller has removed the published list from its website after becoming aware of it, thereby remedying the risks of the personal data breach.

Based on the above, the Authority found in its decision that a warning was not a proportionate and dissuasive sanction for the infringements detected during the procedure, thus a fine of a symbolic amount was imposed. (NAIH/2019/2238)

2. An employee of a child welfare body mistakenly mailed 9 documents containing personal data to a social institution with a similar function but in a different area of competence, thus violating the confidentiality of the data. The personal data breach involved the following personal data of 18 persons (including minors): identification data, contact data, data relating to criminal history, crime, punishment or other action taken, social identity data and other data handled by the data controller in connection with child protection procedures.

Five days after mailing to the wrong address, the wrong addressee reported the case to the data controller, and the mails returned to him another eight days later. In the opinion of the data controller, the wrong delivery became certain only then, so he considered this date as becoming aware of the personal data breach. The personal data breach was notified to the Authority more than two weeks later even from that date. The controller justified the late notification on the grounds that the returned mail had not been forwarded to his senior official, as an event organized by the controller had been held in the meantime, which was part of the statutory task of the controller; and also the wrong addressee itself is a body performing similar tasks, only having other competencies. In his own risk analysis, the data controller also took into account that although the scope of the data is significant, it could only be accessed by a few, at most two persons, who are obliged to maintain confidentiality. As a result of the analysis, the data control-

ler concluded that the personal data breach was of medium risk, and in order to remedy it, it introduced double addressing controls and took measures to maintain emergency data protection training. However, it did not consider it necessary to communicate the personal data breach to the data subjects.

Based on the facts of the case established, the Authority found that the data controller had taken appropriate remedial actions, however, the personal data breach was not notified to the Authority within the deadline set by the GDPR. In the opinion of the Authority, the controller already became aware of the personal data breach when the wrong addressee informed him of the wrong addressing. Thus, 24 days passed after the data controller's having become aware of the personal data breach and notifying it (16 days even if the date indicated in the data controller's statement is taken into account).
In its decision, the Authority obliged the controller to take the necessary measures to ensure that a possible future personal data breach is notified within the deadline set by the Regulation. The Authority did not accept the controller's justification for the delay: the timely notification of the incident should not be precluded by the fact that the controller has other obligations or the lack of accurate information, as the Regulation allows to provide information regarding the personal data breach in phases. The Authority also emphasized that if having become aware of a personal data breach, the superior at the appropriate management level should be notified immediately so that the personal data breach can be addressed and notified if necessary.

Furthermore, the Authority took into account that the controller was also late to take measures to address the personal data breach, including in particular to make the risk analysis. In the absence of taking measures to address the personal data breach, the actual risks of the personal data breach to the rights and freedoms of individuals cannot be adequately assessed, which in itself is a risk.

As a mitigating circumstance, the Authority considered that
a) when the department involved in the personal data breach reported the case to the DPO of the controller, he / she immediately started to fulfill the obligations related to the personal data breach;
b)) the incident is the result of the negligence on the part of an organizational unit, so the breach does not originate from a systemic problem with the data controller, nor is there any suspicion of intent in connection with the breach;

c) the controller has notified the personal data breach to the Authority, however, not without undue delay, and it also follows from its other actions taken following the personal data breach that it is generally aware of its obligations in the event of a personal data breach.

Based on the above, the Authority found it necessary to impose a fine. (NAIH/2019/3854)

3. In many cases, personal data breaches originate in the lack of security measures or inadequate security measures, so it is crucial that personal data breaches are, where possible prevented by appropriate technical and organizational measures. Adequate security of personal data must also be ensured by data controllers during paper-based data processing.

A personal data breach occurred with the disappearance of outpatient records from a specialist clinic of a healthcare institution. The personal data breach likely occurred in such a way that a member of the cleaning staff mistakenly considered the file containing outpatient sheets, which the staff of the institution forgot on the floor of the office, to be waste. The documents contained the personal data of about 70 data subjects, including health data. Of the elements of the concept of a personal data breach, only the loss of the data occurred, however, the information indicating unauthorized access to or disclosure of the data did not come to the knowledge of the data controller. In order to address the personal data breach, the data controller took measures to establish good documentation storage practices, to make lockers used for storing documents containing personal data lockable and to comply with the rules of office waste storage.

The personal data breach was notified to the Authority only when it was established that the search for the lost documents did not lead to a result, so the data controller exceeded the deadline for notification several times. The Authority also found in its decision that the personal data breach was not communicated to the data subjects without undue delay and that the content of the information was inadequate. When determining the sanction applied, the Authority also took into account that the personal data breach poses a higher risk due to the nature of the personal data processed as well as the data subjects, as unauthorized access to them may have significant consequences for data subjects. On this basis, the Authority considered it necessary to impose a fine in the case. (NAIH/2019/5743)

4. The hospital notifying the personal data breach sent a postal mail containing the laboratory findings of up to 10 pregnant patients to a nurse's network, but the mail was returned to the data controller by the Hungarian Post damaged, without content, and packed in a plastic bag.

The data controller sent the postal mail as an unregistered item. Documents and laboratory findings containing personal data in the postal mail were lost and destroyed, i.e. the case resulted in the accidental destruction of the data. The findings included the patient's name, date of birth, mother's name, home address, social security number, and the results of the laboratory test. The lost personal data were also available from other sources thus the availability of the data was not permanently damaged.

At the time of the personal data breach, the data controller kept a record book of the delivery of all postal items, but at the time of the incident he did not have such a detailed register from which he could determine exactly which findings of the data subjects the lost mail contained. The data controller was not able to inform the data subjects as the consultation with the recipient did not lead to a result. In order to avoid similar personal data breach in the future, the data controller provided in Director's Instruction that if a finding needs to be delivered by post, it should be sent by registered letter or with acknowledgement of receipt, moreover a register has been introduced in which, in the case of postal mails containing findings, the data subjects of the findings will be indicated. During the audit, the Authority found that, based on the circumstances revealed, there were no indications that the confidentiality of personal data had been compromised or that the availability had been permanently compromised. The data controller communicated the personal data breach to the addressee thus it has fulfilled its obligations under Articles 33-34 of the GDPR.

Regarding the security of data processing under Article 32 of the Regulation, the Authority is of the opinion that the transfer of documents containing personal data, including health data, of the data subjects in a fully identifiable way, may pose a higher risk which justifies stricter action by the controller. When defining data security measures, the controller should have taken these higher risks into account and defined them in such a way as to guarantee that unauthorized persons will not have access to, lost or destroyed personal data. In the case of postal delivery, the data controller must use one of the services of the Hungarian Post that is suitable for this purpose, for example, sending by registered mail, in which case the Hungarian Post will deliver to the addressee or other authorized recipient.

Therefore, in the opinion of the Authority, the data processing measures at the time of the personal data breach did not guarantee data security in proportion to the risks, and the Authority therefore found that the controller did not comply with the requirements of Article 32 of the Regulation. (NAIH/2019/7998)

5. According to the personal data breach notification of the Budapest Police Headquarters, on January 11, 2019, one of his employees lost a flash drive with 4 GB of storage space used by him for data storage during the performance of his duties. The data carrier contained the full list of BRFK's nominated personnel and an electronic copy of the entire personnel file regarding the change of law enforcement service relationship. The data carrier and the files on it were not provided with any access protection, and the employee copied the documents to a data carrier not for service but for private use, in order to present them later on the management meeting to the executives exercising the employer's rights. The documents on the data carrier contained the following personal data of 1733 data subjects: birth name, date of birth, mother's name, social security number, position, scope of activities. The employee of the data controller did not apply any security measures on the data carrier in connection with the stored data, thus violating the ORFK instruction 18/2018 (V.31) on the IT Security Regulations of the data controller. The data controller stated that it hadn't received any information regarding the discovery of the flash drive or the misuse of the data, nor was he aware of any information indicating unauthorized access to the data. The data controller suggested that the data carrier was destroyed due to the weather conditions prevailing at the time of its loss, so that no further security incident beyond the loss of the data was likely to occur.

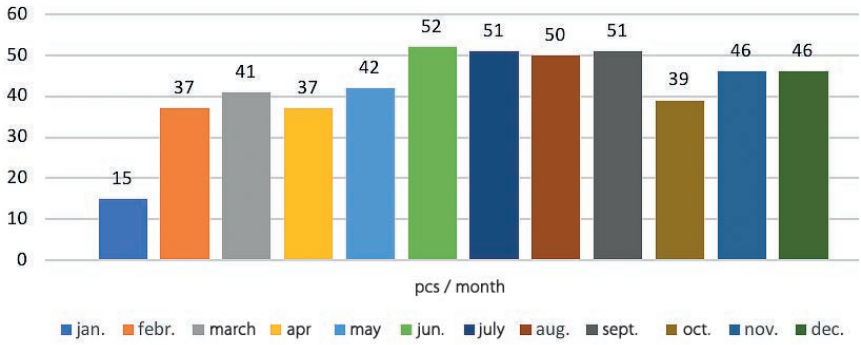
The Authority agreed with the data controller on the classification of the incident as fundamentally risky, since the data stored on the flash drive included data that was not publicly available or not accessible on public interest grounds. The Authority emphasized that of the elements of the concept of personal data breach, only data loss occurred in the present case, but that there was a risk of further breach of confidentiality as the data carrier and the data stored on it were not protected by any technical measures against unauthorized access. The personal data breach was not notified within the deadline set by Article 33 (1) of the Regulation. The controller stated that the loss of the flash drive probably took place on the 11th of January 2019, and on that day the employee also briefly informed his superior. Therefore, in the opinion of the Authority this date was considered to be the date when the controller became aware of the personal data breach. In the opinion of the Authority, for the purposes of assessing the time of

becoming aware of the personal data breach, it is sufficient for a substantive administrator / superior to become aware of the occurrence of the data breach at the controller who did not cause the data breach himself, and who has all the opportunities and means to notify the relevant decision-makers.

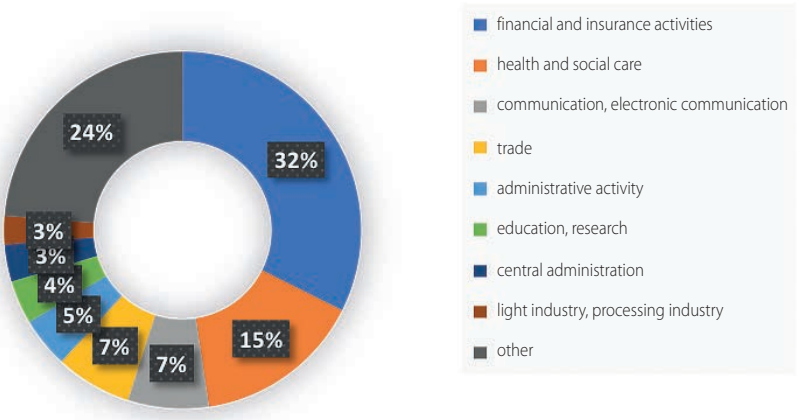
The data controller justified the late notification of the personal data breach by carrying out a full command investigation of the case and by submitting a request for resolution of the ORFK. The personal data breach was finally notified on the 25th of February 2019, on the basis of which a total of 45 days passed between having become aware of the personal data breach and the notification, which means that the notification deadline required by the Regulation as a general rule has been exceeded fifteen times. The Authority did not accept the data controller's reasons for exceeding the deadline because, in his opinion, practically all the facts and circumstances necessary for the risk assessment of the personal data breach had been available since the probable loss of the flash drive and the date of having become aware of it. Nor can the absence of accurate information be an obstacle to notify a personal data breach in time, as Article 33 (4) of the Regulation allows the information to be provided in phases. Furthermore, the data protection officer of the data controller was notified on the 28th of January 2019, well above 72 hours after having becoming aware of the personal data breach, which is an unacceptable practice according to the Authority. The Authority also found that the data controller did not comply with the provisions of its own internal instructions regarding risk assessment and notification of personal data breach.

Based on the above, the Authority imposed a data protection fine of HUF 5 million and ordered the publication of its final decision including identification data of the data controller. (NAIH/2019/2471)

Monthly distribution of a total of 506 personal data breaches notified in 2019



Distribution of personal data breach notifications as per sectors 2019



II.3. Procedures reviewed by Court

We present the most interesting cases of which judicial review was currently in progress at the time of writing this report.

1. Data processing related to admission to festivals

The Authority examined the data processing of the "Sziget" festival and similar events related to admission in a data protection authority procedure (NAIH/2018/6248; NAIH/2019/55). In its decision of May 2019, the Authority found that the data processing at these events was not based on an appropriate legal basis and failed to meet the principle of purpose limitation, and that the data subjects did not receive appropriate preliminary information about the processing of their personal data.

On the account of the data processing conducted after the 25th of May 2018, the Authority imposed a data protection fine of HUF 30 million, and ordered the data controller to align its data processing practice in the course of admissions with the provisions of the General Data Protection Regulation.

The company organizing the festivals initiated a judicial review of the Authority's decision because, in its opinion, the Authority unlawfully initiated the authority procedure and did not clarify the facts of the case properly, therefore, the decision of the Authority is unlawful.

The Budapest-Capital Regional Court of Appeal upheld the decision accepting the Authority's argument. The data controller appealed this ruling at the Curia, the proceedings of which are still underway.

2. Judicial assessment of the legal basis relating to claim assignment

Debt collection companies often claim before the Authority that the legal basis for the processing of debtors' personal data is a contractual legal basis under Article 6 (1) (b) GDPR, as claims which were subsequently acquired by assignment arose from a contract. The Authority found that the legal basis under Article 6 (1) (b) GDPR, with the exception of certain steps prior to entering into a contract, can only be applied if the processing is necessary for the performance of the contract. Thus, this legal basis cannot be extended to data processing which are necessary to remedy the situation resulting from the non-performance of the contract by the person concerned, and to take steps arising from the normal ob-

ligation of cooperation of the contracting parties. The performance of the contract may also include the steps, when the data controller who concluded the contract with the data subject, i.e. is the other party to the contract, calls upon the data subject to perform in the event of a delay in the performance. However, a contractual legal basis under Article 6 (1) (b) of the GDPR can no longer apply if the controller assigns his claim against the data subject to a debt collection company due to non-performance (i.e. seeks to resolve the problem outside the contract). Thus, there is no longer a contractual relationship between the debt management company and the debtor. The legal basis for the transfer of data in the context of a claim assignment can thus only be different, typically the legitimate interest of the assignee in enforcing the claim for his own part.

According to the reasoning attached to the Civil Code, the assignment of claims takes place on the same logic as the transfer of ownership, so the claim assignment is in fact nothing more than the transfer of ownership of the claim. By claim assignment, the claim is separated from the original legal relationship from which it arises, and the assignee replaces the assignor only in respect of the claim and not in respect of the fundamental legal relationship. Since by the assignment the claim separates from the fundamental legal relationship and the assignee becomes the holder of the claim, the assertion of the claim by the assignee, and the related data processing are no longer performed for the performance of the contract from which the claim originally originated, as in that case the claim acquired through the assignment should be enforced by the assignee not for its own benefit, but for the benefit of the assignor. By the claim assignment, if it takes place for consideration, the assignor's claim against the debtor is fully or partially reimbursed, depending on the purchase price. The assignee acts in his own interest and for his own benefit in order to recover the claim, since by claim assignment he becomes the holder of the claim and the enforcement of the claim, the enforcement of the debtors to perform, and the processing of the data for that purpose serves his legitimate interest and not the performance of the underlying contract. As the claim has become independent of the contract after the claim assignment, the legal basis for personal data acquired by claim assignment at the same time as the claim cannot be a contractual legal basis within the meaning of Article 6 (1) (b) of the GDPR.

This position of the Authority was confirmed by the Budapest-Capital Regional Court of Appeal in its judgment. However, this does not necessarily mean that there is no legal basis for the processing of debtors' personal data by debt collection companies. If the personal data of debtors - natural person identification data and data relating to the claim - have been obtained in the framework of their

receivables purchase activity permitted by law, then the existence of a legitimate interest in enforcing legally acquired claims and processing the above-mentioned data necessary for this purpose, can in principle be established based on the legal regulation. (NAIH/2019/2566)

3. Personal data breach case in court

In its decision NAIH/2019/2668/2 of 21 March 2019, the Authority found that a political party as data controller in respect of a personal data breach involving a database containing personal data of more than 6000 data subjects had not complied with its obligation to notify and document the personal data breach, and to communicate it to the data subjects as provided for in Article 33-34 of the GDPR.
Therefore, the Authority imposed a data protection fine of HUF 11,000,000 on the party.

Based on a notification related to the personal data breach submitted in August 2018, the Authority first initiated an inquiry and later an authority procedure for data protection. According to the notification, there was an entry on a hacker forum that drew attention to an IT security (so-called SQLi) vulnerability on the party's website http://web.dkp.hu. Exploiting the vulnerability, the attacker who wrote the entry managed to access a database that contained a lot of personal information about party members and sympathizers (name, email address, username, function in the party, weakly encrypted password). The attacker published the database on the forum and, according to him, drew the attention of the data controller to it. However, the data controller did not notify the personal data breach to the Authority and did not communicate it to the data subjects.

During the authority procedure, the party took the view that, as the stored data had not been updated for years, they were out of date and that a personal data breach involving the disclosure of such a database should not be notified to the supervisory authority or communicated to the data subjects. In its decision, the Authority argued for the high risk to the rights of the data subjects, as sensitive conclusions can be drawn from the data regarding political opinion and party affiliation even if they have not been updated for years. In addition, the use of weak password encryption (MD5 algorithm) can pose an increased threat to the privacy of the data subjects. The Authority therefore considered the provisions of the GDPR on the handling of personal data breaches to be applicable in the above case.

The party initiated a judicial review of the decision with the Budapest-Capital Administrative and Labor Court. In its action, the party argued that since the vulnerability that caused the personal data breach already existed before the GDPR became applicable on the 25th of May 2018 (from April 2018), the provisions of the Regulation on the handling of personal data breaches should not apply to it. It also disputed the legitimacy of the amount of the fine, for its proportionality and disregard for the party's sources of revenue. The NAIH requested that the action be dismissed.

In its judgment at first instance, the Court shared the Authority's view that the personal data breach should be subject to the rules of the GDPR on the handling of personal data breaches, as the security breach persisted after the EU Regulation became applicable and also the data controller party became aware of it then. However, as regards the reassessment of the criteria for the amount of the fine, the court of first instance ordered a new procedure before the Authority. Both the applicant and the Authority appealed against the non-final judgment at first instance to the Curia as a court of second instance. The second instance proceeding is still ongoing in early 2020.

4. Review of the Authority's decision on infringement of the right to the protection of criminal personal data by the Curia

A journalist made a note in an archive on the request form "[…], his partner […] - 1960" regarding learning of two judgments, in which the archive stated that "It can only be issued with his supporters or in an anonymized copy." The archives provided the researcher with ten anonymized pages from the judgment of the court of first instance, and three from the judgment of the court of second instance. Subsequently, articles appeared in several media outlets that the data subject had been convicted of a crime in the 1960s.

In its decision, the Authority found that the archives had unlawfully granted access to the judgments and therefore imposed a data protection fine of HUF 3 million. The Authority also called upon the archives to establish rules of procedure to ensure compliance with Section 24 (1) and (2) (a) of Act LXVI of 1995 on Public Documents, Public Archives and the Protection of Private Archival Material (hereinafter: Archives Act).

In the reasoning of its decision, the Authority explained that the archives did not comply with the requirements of Section 24 (2) (a) of the Archives Act because they did not recognize that the judgment constituted criminal personal data in

its entirety, as it contained information that could be linked to a criminal offense committed by convicted persons. The researcher identified specific natural persons on the data request form, based on which the archives should have recognized that the judgments could be linked to the designated persons despite any anonymization, thus anonymisation pursuant to Section 24 (2) (a) of the Archive Act would not have been applicable. (NAIH/2016/2504/27 /H)

The archives initiated a review of the decision because, in its view, they had correctly applied the relevant legislation, as the judgments were given before the 2nd of May 1990, were not subject to a research ban, so anonymously they had to make the judgments available to the researcher and they did not have the opportunity to refuse it under Section 25 (b) of the Archive Act. The subjective element should not play a role in determining the quality of personal data, and the classification of data should not depend on whether or not the person is able to link it to a specific person.

By its judgment, the court of first instance set aside the decision of the Authority. According to the court of first instance, it follows from the interpretation of the Authority that the archives could decide, in the light of the information available to the researcher, whether or not a link can be established between the particular judgment and the data subject, that is, whether the anonymised record can be provided. However, examining such subjective content of consciousness would make it impossible to assess research requests and anonymisation itself. In the opinion of the court of first instance, the concept of personal data cannot depend on the content of consciousness, i.e. no distinction can be made when assessing a research application according to what information the researcher has and what he or she indicates on the application form. In the given case, the indication of the name of one of the data subjects, due to its frequency, is not suitable for identifying a specific natural person, as a result of which the Authority unjustifiably claimed that the connection between the data subject, and the judgments provided in anonymised copies could be re-established in one step, and that the archive should have recognised this. The Authority interpreted the concepts of personal data and criminal personal data in such an extensive manner, and classified the entire judgment only considering the given request of the given researcher, i.e. depending on subjective consciousness, as criminal personal data, which interpretation does not comply with the provisions of the Privacy Act. According to the court of first instance, the applicability of the anonymisation set out in Section 24 (2) (a) of the Archive Act shall be interpreted from the point of view of the research, i.e. the research may be carried out with an anonymised

copy if it does not infringe the text. (Budapest-Capital Administrative and Labour Court 13.K.32.793/2016/15)

The Authority filed a review application against the judgment of the court of first instance because it considered that the court of first instance erred in stating that the concept of personal data could not depend on the content of the consciousness, the information available to the researcher and the name of the data subject is not suitable for identifying a specific natural person. In the opinion of the Authority and according to Article 29 Data Protection Working Party Opinion 4/2007 on the concept of personal data, the quality of personal data does not require that everyone be able to identify the person, but that it is sufficient if a group is able to identify it, i.e. the subjective content of consciousness must be taken into account. The request form contained the remark "[…], his partner […] - 1960", so it can be deducted from this itself that this was suitable for identification, since it was not merely a common personal name indicated, but a combination of two persons' names and a year. The Authority does not expect an archive to examine the researcher's subjective content of consciousness in all cases. The essence of the Authority's finding is, that if the data request form contains enough data to identify a natural person, even if some data is obscured or deleted in the document provided on the basis of it, the remaining provided information can be contacted with the person indicated on the data request form despite the obscuration, and therefore anonymisation pursuant to the Archive Act is not possible in this case. This finding did not require a detailed examination of the extract provided to the researcher, as it cannot be ruled out that no data or findings were included on the thirteen pages. Thus, it is not what the researcher knew about what matters, but whether the content of the data request form allows specific individuals to be identified.

The archives filed a cross-application for review against the judgment of the court of first instance and a counter-application for review against the Authority's review application. According to the cross-application for review, the Authority did not fulfill its fact-finding obligation by failing to examine whether the extracts from the judgments constituted personal data.

In the opinion of the Curia, both the review application and the cross-application for review were thorough. The Curia had to take a position on the question of principle whether the search for criminal convictions containing the criminal personal data of still-living natural persons could be carried out with an anonymized copy before the expiry of the protection period pursuant to Section 24 (2) (a) of

the Archive Act, in the event that the researcher requests the judgments by indicating the names of the convicts and the year in which the crime was committed.

During the protection period, the archives decide whether the research can be authorized under an exception rule on the basis of the information provided by the researcher (researcher's data sheet, data request form) and the legal requirements for the searchability of the archival material to be researched or whether there is a statutory reason for refusing to comply with the request.

Contrary to the position of the court of first instance, the data and information contained in the search request are relevant to the assessment of the research request, as if the data subject can be identified on the basis of them, no matter how professionally and carefully anonymized the judgments are made available to the researcher by the archives, the researcher can relate the content of the material to be researched - containing personal data - in one step to the natural person indicated in the application. This is contrary to the legislative purpose of creating the possibility of research with an anonymized copy, so in such a case the research pursuant to Section 24 (2) (a) of the Archive Act is conceptually excluded and consequently cannot be authorized.

The court of first instance was right to find that the common name of the person concerned was not in itself sufficient to identify the data subject. However, the request form contained not only the name of the data subject, but also a combination of the names of two convicts in a criminal case and a year. The Curia, in accordance with the Authority's decision, found that this information was already sufficient for identification, as the additional information attached to the name made the data subject distinguishable from other persons of the same name, thereby becoming identifiable.

The Authority did not expect the archivist to examine the researcher's content of consciousness, but to recognize, on the basis of the data contained in the research request, that if the research request contains sufficient data to identify a natural person, research with an anonymized copy shall not be permitted in the archive material containing personal data during the term of protection.

The Curia shared the Authority's opinion that the content of the anonymized copy provided to the researcher by the archives was irrelevant to the legal issue to be judged, as there was no legal possibility to allow research with an anonymized copy in the given case. However, what the archives forwarded to the researcher is of major importance in establishing the infringement, as an infringement can

only be established in relation to the anonymized copy actually provided to the researcher. The Authority therefore failed to fulfill its obligation to clarify the facts of the case in this respect.

During the review procedure, the Curia found that the court of first instance had misinterpreted the substantive rules, as a result of which it had also erred in concluding that there had been no infringement, and had erred in disregarding the Authority's failure to clarify the facts. The Curia therefore shared the Authority's position on the merits of the case and ordered a new procedure for further clarification of the facts

III. Procedures Related to Data Processing for Criminal Investigation, National Defence, and National Security Purpose

III.1. Procedures Related to Data Processing under the Privacy Act

On the basis of current and extrapolated trends in technical development, such as the drastic reduction in the cost of image surveillance systems and image storage, the development of big data analysis capabilities, the spread of biometric data processing and the use of artificial intelligence, and the emergence of robotic systems for mobile surveillance (e.g. drones, robotic vehicles), as well as of available information on known developments and plans, it can be assumed that in the future public bodies will be able to monitor the behavior of data subjects and to collect personal data in more and more places and in an increasingly sophisticated way through automated IT systems.

As in previous years, in 2019 the focus of the Authority was on large IT systems that contain data in connection with many data subjects, operate on a national scale and usually with the participation of several data processing bodies. These were the "Dragonfly" project in an intermediate phase of implementation mentioned in the previous annual report, or a pilot project launched to pre-test innovative services and solutions for smart cities. Several of the data processing that came into focus in 2019 have a "dual purpose," i.e. in addition to their primary purpose, they also have a lesser-known secondary, law enforcement, or national security purpose.

III.1.1. The VÉDA-System

The VEDA system is operated by the police. Its primary purpose is to provide technical support for police monitoring of compliance with road traffic rules. The continuously operating image recorders of the system are located above and along the country's roads. Based on the camera images, the license plates and other unique characteristics of the vehicles, as well as violations of road traffic rules are detected automatically. The data, including data on vehicles for which no traffic offense has been identified, are stored for thirty days.

In the opinion of the Authority, the traffic police control carried out with the VÉDA system has a legitimate data processing purpose, the achievement of which is in the public interest. Based on the available data, the VÉDA system has been

operated by the police within the legal framework of the road safety measures. However, doubts arise, whether the application of the nationwide automated data collection system complied with the rules, therefore, in order to clarify the situation, the Authority requested further information from the State Secretary for Administration of the Ministry of Interior.

The legal problem at issue highlighted that examining the VÉDA system with regard to fundamental information rights of citizens, it can be stated that its data protection impact profile differs in several respects from the police measures (hereinafter referred to as “classical police measures”) provided for by Act XXXIV of 1994 on the Police (hereinafter: Police Act). In particular, the following differences should be highlighted

1. Instrumental inspections can also take place during classic police measures (e.g. breathalyser, speed cameras), however, technical inspections with the VÉDA system are exceptional in terms of the lack of personal involvement of the police at the inspection site and at the time of the inspection. There is no personal contact between the person being inspected and the police officer conducting the inspection, so it is possible that the data subject does not even become aware of the inspection and there is no way to exercise „in situ” his or her rights to information, access and judicial redress.

2. The inspection process is automated and human knowledge and decision making is carried out by the police only in relation to inspections that the technical system has assessed as potential offenses. The question is to what extent a measurement of an automated system can be considered a “police measure” in such circumstances in which the data collected by the machine is retained, but since they do not indicate a traffic offense, they are not subject to human evaluation. If such cases are to be considered a police measure, for example, who is the police officer in charge and what is the location of the measure?

3. In the VÉDA system, data collection takes place continuously, in several locations in parallel. Automated data processing requires only minimal human supervision, so unlike classical police measures, the need for live labour does not create a bottleneck in the process of data collection and data use that would set a natural limit to increasing the number of control sites, i.e. extending police surveillance of citizens.

4. While classic police measures can be linked to a specific location, the VEDA system is centralized: data collected from many locations are stored and used centrally, so there are technical possibilities to link the collected data with each other and with data from other sources. The operation of the VÉDA system presumably creates a nationwide, constantly accumulating data mass suitable for "big data" analysis, from which, for example, a movement profile and a traffic habit profile assigned to a vehicle or a person can be created.

In the case of VÉDA, the lawful purpose of surveillance is not disputed, but in the opinion of the Authority, it is necessary to clarify how to find a balance between the interests of road safety related to surveillance and the protection of personal data and the right to privacy enshrined in the Fundamental Law. The nature and content of the legal regulation of monitoring systems is crucial, as the legal regulation can determine the framework for the application of the technology.
VÉDA and similar systems realise mandatory data processing, therefore the application of the rules on the right to information, access and the right to lodge a complaint of the data subject is not sufficient to prevent excessive data collection. Sectoral rules on data processing should set out specific guarantees for the protection of personal data.

In its reply, the Ministry of Interior expressed its openness to continue data protection consultations related to the VÉDA system and, if necessary, to correct the legal regulations. The consultation on this subject is still ongoing at the time of writing.

III.1.2. Biometric application of the National Directorate-General for Aliens Policing to facilitate portrait comparison

The Authority examined the IT system of the National Directorate-General of Aliens Policing (hereinafter: OIF) on the basis of a notification. According to the information received from the Director General of the OIF, the application operated by the OIF does facial recognition and face image comparison only on static images, i.e. not on motion pictures or camera image streams. The OIF shall process facial data in accordance with the sectoral laws applicable to its activities and shall use facial data recorded in the course of the procedures within its competence for the purpose of personal identification. The face images are also compared with face images from the warrant register and with face images of wanted persons published in the public interest by Interpol, Europol and the FBI, i.e. publicly available, on the websites of these bodies, in order to filter out

unknown or false identities or wanted persons. The operation of the OIF system is semi-automatic, so it does not actually perform personal identification, but shows results that are most similar to the face to be compared. Based on the displayed results, the administrator takes the necessary action against the person who cannot identify himself / herself, the choice of which is facilitated by the result of the face image comparison.

The Authority found that the persons involved in the OIF procedures are aware of the recording and use of facial images, i.e. the data collection is not covert. With regard to the procedures within the competence of the OIF, it can be expected that some of the foreigners concerned do not have identity documents and may have a counter-interest in establishing their true identity, therefore semi-automatic machine support for identification and identity verification is justified. In the course of the investigation, the Authority did not receive any information indicating that the OIF had set up a continuously operating, automated monitoring infrastructure over a large geographical area. The face image comparison assisted by a mechanical system, as well as the use of data for official purposes, requires human labour. The need for living labour creates a bottleneck in the process of data use that precludes mass, stockpiling biometric data collection. The Authority closed the investigation into the case, but at the same time initiated the preparation of a legislative amendment with the State Secretary for Administration of the Ministry of Interior that explicitly refers to warrant data published by foreign law enforcement agencies among the OIF data sources.

III.1.3. Data content of the RK sheet issued during identity check by the police

In connection with a citizen's complaint to the Office of the Commissioner for Fundamental Rights concerning a series of police identity checks, the Deputy Commissioner, who protects the rights of nationalities living in Hungary, requested the opinion of the Authority on certain provisions of the Police Act and the Police Service Regulation related to identity check. Pursuant to the Police Act, the data of the person whose identity being checked shall be recorded if it is necessary for further actions, procedure or other circumstances justify it. The data shall be recorded on the so-called RK sheet. However, for each identity check, the Service Regulations provide for verification of the data of the individual and the document presented in the Schengen Information System, the warrant registration system and, where applicable, in the personal data and address register or the document register. It is necessary to document the queries from the

database, therefore according to the current practice, an RK form is filled in for each identity check, i.e. the data of the document concerned and presented are recorded even if it is not necessary for further action or procedure.

In its reply, the Authority recalled that personal data shall be processed only for clearly specified and lawful purposes, in order to exercise certain rights and fulfill obligations pursuant to the Privacy Act. The purpose of processing shall be met in all stages of processing; data shall be collected and processed fairly and lawfully. Only personal data that is essential and suitable for achieving the purpose of processing may be processed. Personal data may be processed only to the extent and for the period of time necessary to achieve its purpose. Section 25/F of the Privacy Act provides for the keeping of an electronic logbook in the case of automated data processing systems. According to the Police Act, the head of the receiving police body is responsible for the lawfulness of the data collection and use of data by the police. The fact of the data transfer must be documented at both the transferring and the receiving body. On this basis, the Authority stated the followings:

The Service Regulation provides for the mandatory processing of personal data at the legal source level of ministerial decree by requiring the person whose identity being checked and the document presented by him or her to be verified by querying the background register. Pursuant to Section 5 (1) (a) of the Privacy Act, the mandatory processing of personal data shall be ordered in an Act or, based on the authorization of an Act, within the limits set forth therein and for data other than sensitive or criminal personal data, in a local government decree for purposes in the public interest. Pursuant to Section 5 (3) of the Privacy Act, for mandatory data processing, the type of data, the purpose and conditions of data processing, the access of such data, the controller and the duration of the processing or the regular examination of its necessity shall by specified by the Act or local government decree ordering mandatory processing. Pursuant to the cited legal provisions, a decree of the Minister of Interior may not prescribe mandatory data processing. However, it should also be taken into consideration that the rules of the Police Act referred to above provide a legal framework for data processing by the police, including data processing during police measures and access to background records. As explained in the relevant decisions of the Constitutional Court, the requirement, that the issues to be regulated need to be ordered in an Act, is not in any connection with fundamental rights. The legal source level of decrees is also sufficient to regulate indirect and distant relations with fundamental rights. Therefore, from the point of view of the legal source lev-

el, it is acceptable to prescribe the mandatory register queries during the identity check in the Service Regulation. At the same time, the Authority finds it problematic that the Service Regulation prescribes the queries of background records relevant to law enforcement, even in the case of identity checks where the identity check is not for law enforcement purposes. In such cases, such verification of the data is not in line with the lawful purpose of the police measure.

If queries made during the identity check are necessary, they shall be documented. Police data controller bodies and police staff performing data processing tasks are responsible for the lawfulness of their data processing. A precondition of the data controller's subsequent accountability is the proper documentation of the data processing, including records queries. Documentation of data processing is also a requirement for enforcing the right to access of the persons affected by the query. Thus, it is necessary to document the query of personal data, but neither the Privacy Act nor the Police Act provides for this to be done by completing the RK sheet. The requirements for documenting data processing are set out in the rules of the Privacy Act related to electronic logbook (Privacy Act Section 25 / F. (1)), the content of the right to access of the data subject (Privacy Act Section 17) and in Section 84 (4) of the Police Act. In view of this, the Authority considered it reasonable to revise the point in the Service Regulation which makes full background checks mandatory for identity checks for other purposes than law enforcement in order to avoid stockpiling data collection. In addition, the Authority called for the implementation of IT support for the documentation of the identity checks, which would benefit both citizens and the police officers by speeding up administrative tasks.

III.1.4. Monitoring of the correspondence of detainees

Based on a citizen's complaint, the Authority examined the data processing practices of the Sátoraljaújhely Strict-and Medium Regime Prison (hereinafter: the prison) regarding the handling of letters, according to which the letters received by the detainees shall be photocopied by the prison and only the photocopies shall be handed over to the detainees. The original of the letters shall be kept closed and, if the detainee requests so, handed over to a relative designated by him at the time of the reception of visitors. Otherwise, the original letter shall be handed over to the detainee on leaving the prison or on release. According to information received from the prison, it was necessary to design such mail handling because it had been found on several occasions in the past that the letters

to the convicts were soaked in intoxicating or narcotic substances, which the detainees consumed torn into pieces or rolled into cigarettes.

The Authority accepted the explanation that the photocopying and the temporary keeping of the original letters serve to maintain the order of detention and to protect the health of convicts, but pointed out that the copying of letters and the separate storage of original letters entail the mandatory processing of personal data, which should be in line with the legal requirements for mandatory data processing. According to the Privacy Act, the order of mandatory data processing falls within the scope of legislation. In our case, Act CCXL of 2013 on the enforcement of penalties, measures, certain compulsory measures and administrative confinement (hereinafter: Penalty Enforcement Act) contains the sectoral rules. Section 9 (1) of the Penalty Enforcement Act provides for the restriction of the exercise of the rights of convicts. Section 174 of the Penalty Enforcement Act contains the rules of correspondence and its limitations. The detailed rules are laid down in Decree of the Minister of Justice 16/2014 (19 December) (hereinafter: IM Decree). These sources of law do not contain rules on the copying of detainees' letters and the handling of originals, therefore, the Authority, in its opinion sent to the State Secretary for Administration of the Ministry of Justice, considered it necessary to regulate the above-described letter handling practice prior to the arrival of drug-soaked mail items in the prison, as well as the regulation of the appropriate documentation of data processing at the level of a decree, which shall exclusively relate to letters that can be opened and verified on the basis of the Penalty Enforcement Act. The record shall contain at least the unique identifier of the letter, the addressee, the date of subsequent delivery and the identity of the recipient of the letter. If the letter is handed over to a relative at the detainee's request, the detainee's statement to that effect should also be kept. In view of the data quality requirement, the Authority also recommended that copies of letters to be handed over to detainees shall be made in clearly legible quality. (NAIH/2019/5469)

III.2. Procedures Related to Personal Data Breach in connection with Data Processing under the Privacy Act

III.2.1. Specific Features of Procedures Related to Personal Data Breach in connection with Data Processing for Criminal Investigation, National Defence, and National Security Purposes

As the GDPR became applicable, the rules of the Privacy Act were supplemented by provisions which interpret the concept of personal data breach in connection with data processing for criminal investigation, national defense and national security falling within the material scope of the Act, as well as define the rules for the handling of a personal data breach and the related tasks of the Authority. The national legislation transposes the rules of the Data Protection Directive for Police and Criminal Justice Authorities (hereinafter: Police Directive)[6] . Although the relevant normative material of the law is parallel to the GDPR rules on personal data breaches in terms of the purpose of the regulation and the basic legal institutions, due to the differences in details, it is appropriate to discuss the Authority's procedures related to personal data breach in connection with data processing for criminal investigation, national defense and national security. With regard to the specific features of the national regulations and the specificities arising from the nature of the data processing under the Privacy Act, the following should be highlighted:

1. The obligation to transpose the rules of the Police Directive related to personal data breaches only applies to data processing for criminal investigation purposes. However, in the interest of consistent data protection regulations, the Hungarian legislature, taking into account the obligation of the state to protect fundamental rights provided for in Article I (1) of the Fundamental Law, decided to extend the scope of the rules related to personal data breaches to all personal data processing under the Privacy Act. At the same time, the regulation reflects on the secret service nature of the activities of the national security services and the high priority of enforcing the national security interest, therefore, in the case of data processing for national security purposes, if required by the national security interest, the law allows the data controller to postpone informing the data subject and notifying the Authority to the date after such interest of the national security have ceased.

6 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

[The Privacy Act also allows, in connection with personal data breaches related to data processing for criminal investigation and defense purposes, an Act to exclude, restrict or delay the provision of information to the data subject under the conditions and for the reasons set out in Section 16 (3). However, this does not affect the controller's obligation to notify the Authority.]

2. According to Article 31 (4) of the Police Directive, if the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so. The Privacy Act transposed this into Hungarian law in such a way that it does not authorize the Authority to order the data controller to provide the data subject with information, but to establish on the basis of the notification of the personal data breach that the communication of the personal data breach to the data subject is required due to its high risk. However, this leads to essentially the same result as provided for in Article 31 (4) of the Police Directive. Since if the Authority communicates the aforementioned finding to the controller, it is obliged to communicate the personal data breach to the data subject in accordance with 25/K § (4) of the Privacy Act.

3. The nature of data processing for criminal investigation, national defense and national security purposes differs in many respects from the data processing, typically by economic operators, for which the GDPR sets out a data protection framework. The former data processing is typically mandatory data processing performed by state bodies, in which case the relevant Hungarian sectoral laws define all the essential elements of data processing, including, for example, the data retention framework, possible routes of data transfer and the rights of data subjects or the conditions for restricting the rights of data subjects. These circumstances should also be taken into account when considering the risks of personal data breaches. In the case of data processing falling within this scope, a personal data breach may infringe not only the rights and interests of the data subject, but also the performance of a public task, constituting an overriding public interest, which requires the processing of personal data. Compared to personal data breaches under the GDPR, it may even be mentioned that while in the case of data processed by a company, it is a realistic possibility for unauthorized persons to try to obtain personal data processed by the company, such as a customer database, for direct marketing purposes or for using it to obtain other economic benefits, in the case of data processing for criminal investigation, national defense or national security purposes, such a risk is minimal and therefore deserves much less attention when considering the risks of a personal data breach.

III.2.2. AExperiences of the Authority regarding Procedures Related to Personal Data Breach in connection with Data Processing for Criminal Investigation, National Defence, and National Security Purposes

Regarding the nearly two dozen personal data breaches related to data processing under the Privacy Act, which the Authority investigated in 2019, the following can be established:

1. Data controllers

Most notifications were received from police forces. In our opinion, this can be explained by three reasons:
1. The police is a large organisation present throughout the country, and the processing of personal data plays a major role in the performance of its tasks.
2. A significant proportion of police data processing is „fieldwork", such as police measures or house searches etc. Experience with the notifications has shown that there is an increased risk of data carrier loss or other similar personal data breaches at external locations.
3. Police officers carry out their duties in a disciplined manner and have strong control mechanisms within the police organisation, so personal data breaches do not remain latent but are handled in accordance with the relevant legislation, including notifying to the Authority.

In terms of their territorial distribution, several notifications related to police authorities were received from Budapest, but personal data breaches were also notified by data controllers in other counties.

2. Causes of personal data breaches

The personal data breaches examined were typically negligent acts within the organisation that did not constitute bad faith. In most cases, the incidents were caused by losing data carriers accidentally (for example, the data carrier was dropped from a holder attached to clothing while the police chased the offender) or by negligence. There have also been cases where personal and criminal personal data have been transferred through negligence during administration and case management, to third parties who are not entitled to access.

In one case, one of the police bodies reported an act of bad faith within the organisation. In this context, the data controller also reported the criminal offence to the authorities and the prosecutor's office ordered an investigation into the criminal suspicion of abuse of office. In this case, the person causing the personal data breach abused his right to access personal data and criminal personal data processed in connection with a criminal proceeding (including the personal data of the suspect). In addition to unlawful access, the suspicion of unlawful use and transfer of data to third parties has arisen, and this is being clarified in the framework of an investigation ordered by the prosecutor's office.

3. Scope of data concerned in personal data breaches

It can be stated that, in most of the cases, the personal data of the data subjects (name, natural person identification data, identification data of person identification documents, sometimes copies thereof), address data, as well as personal criminal data relating to criminal proceedings in connection with personal data breaches at police bodies (personal data in the historical facts of the case, or data expressing the procedural position of the person involved in the criminal proceeding, possibly data referring to police measures against the data subject) are described as data concerned in the notified personal data breaches.

4. Time of notifying the personal data breach

In connection with personal data breaches related to data processing under the Privacy Act, which were notified last year, it can be stated that the data controllers mostly fulfilled their obligation to notify within the deadline, i.e. within 72 hours after having become aware of the personal data breach. In one case, the notification was made about a day late. There was also a case where the data controller did not correctly interpret the time of having become aware of the personal data breach. In this context, it should be emphasized that the time of having become aware of the personal data breach does not mean the time when the personal data breach was communicated to the Data Protection Officer (hereinafter: DPO) within the controller's organisation, i.e. when he or she became aware of the personal data breach. This only coincides with the time when the data controller became aware of the personal data breach if the personal data breach was detected by the DPO himself. In its decision relating to a personal data breach, the Authority explained that the relevant factor for assessing the time of having become aware of the personal data breach is that such an admin-

istrator or superior of the controller becomes aware of the occurrence of a personal data breach who did not cause it and who had the opportunity and means to notify it to the relevant decision-makers or officer. From then on, the controller has 72 hours to notify the personal data breach to the Authority.

5. Measures taken to address the personal data breach

In the Authority's experience, among the measures taken to address the personal data breach, data controllers place great emphasis on holding the person in the data controller's personnel responsible for the personal data breach to account. From the data controller's point of view, of course, personal data breach shall also entail this. However, from a data protection point of view, measures to mitigate the possible adverse consequences of a personal data breach and other measures (such as to prevent future personal data breaches) are relevant. With regard to the personnel of the data controller, such a measure may be education and awareness-raising describing the avoidance of personal data breaches, the rapid recognition of personal data breaches that have occurred and the taking of appropriate measures. It should be noted that these measures are also commonly used by data controllers.

In connection with personal data breaches, the Authority also examines what measures and tools were provided prior to the personal data breach to prevent and avoid possible data breaches, as well as whether the data controller has identified a deficiency in its operation and work processes that allows the personal data breach to occur. If so, have been any measures taken to remedy them? There was a case where the data controller reviewed the procedure affected by the personal data breach due to the personal data breach that occurred, as a result of which the rules of working procedure were changed immediately. In this case, the Authority found that the data processing body had adequately modified its procedure from a data protection point of view through building data protection measures into the working procedure. The rules and measures concerning the process of document management, control during mailing, preservation of data carriers and review of the information stored on them came to the fore, considering that the notified personal data breaches have largely taken place in relation to losing the data carriers or leaving them in a specific place, and sending them to an unauthorized person.

III.3. Hungarian Supervision of the Schengen Information System

III.3.1. The Schengen Information System

The Schengen Information System (SIS II) the largest IT system in Europe, intended to handle the risk arising from the elimination of internal borders and the tighter control of external borders, mainly through efficient data sharing.

The IT system set up at EU level consists of three parts: a central system, national systems and a communication infrastructure. The central part of SIS II is operated by EU-LISA Agency, while the national parts are operated by each Member State. In Hungary, this task is performed by the Deputy State Secretariat for the Management of Records of the Ministry of Interior - as a national N.SIS II Office. Additional information related to the alerts entered in the system is handled by the SIRENE Bureau at the National Police Headquarters.

The SIS contains tens of millions of alerts (warrants of caption). At the local level, all police officers and other law enforcement authorities and officials who require the data to perform their law enforcement and criminal investigation duties have immediate and direct access to the system. The SIRENE bureaux primarily exchange data relevant to criminal cooperation and coordinate cross-border operations. In the course of this activity, they shall provide supplementary information on alerts and coordinate appropriate actions connected to alerts issued in SIS II.

The SIS II system operates on the basis of strict data protection rules, compliance with which is regularly monitored by the European Data Protection Supervisor and the supervisory authorities of the Member States, the NAIH in Hungary. Access to the data shall also be limited, they shall be accessible only to the extent necessary and proportionate, for the purposes set out in the EU Regulation and national law, by national law enforcement, border control, customs, judicial, visa and vehicle registration authorities.

In accordance with EU and Hungarian data protection law, everyone has the right to be informed on request of the data processed in the SIS II, to request the rectification of data which have been entered inaccurately, to request the erasure of data which have been unlawfully processed or to apply to a court or a supervisory authority in order to protect personal data rights. Data subjects shall have the right to apply to a competent authority under the national law of any Schengen Member State or to bring an action before a court. The lawfulness of

the data entered in the system shall be examined in accordance with the national law of the Member State to which the request is submitted.

The relevant Hungarian national law is Act CLXXXI of 2012 on the Exchange of Information Framework of the Second Generation Schengen Information System, as well as the Amendment of Certain Policing Acts and thereby the Hungarian Simplification Programme (SIS II Act). According to the SIS II Act, if anyone wishes to be informed whether his / her data are in SIS II or if he / she requests the rectification or erasure of data in SIS II, he / she can submit his / her request to any government office, police station or Hungarian embassy by filling in the specified form. Requests are examined in the first instance by the SIRENE Bureau, which may refuse the requested information in the interests of national security, the prevention or prosecution of criminal offenses, the security of the enforcement of penalties and the protection of the rights of others. The SIRENE bureau shall inform the applicant of the fact of refusing to provide information, the legal basis and the remedies available to him / her.

III.3.2. Schengen monitoring and evaluation mechanism

Council Regulation (EU) No 1053/2013 regulates the evaluation and monitoring mechanism to verify the application of the Schengen acquis. The purpose of the evaluation mechanism is to monitor the application of the Schengen acquis in the fields of data protection, external borders, police cooperation, return, the Schengen Information System and visa policy in the Member States of the Schengen area. The Member States and the Commission shall be jointly responsible for implementation of the evaluation mechanism, but the Commission shall have an overall coordination role in relation to establishing annual and multiannual evaluation programs, drafting questionnaire and setting schedules of visits, conducting visits and drafting evaluation reports and recommendations. Evaluations may consist of questionnaires and on-site visits which may be announced or unannounced. Announced on-site visits shall be always preceded by the completion of a questionnaire.

1. Multiannual evaluation programme

A multiannual evaluation programme covering a period of five years shall be established by the Commission, not later than six months before the beginning of the following five-year period. Each Member State shall be evaluated during

each five-year period covered by the multiannual evaluation programme. The multiannual evaluation programme shall list the order of Member States to be evaluated each year.

2. On-site visits and questionnaire

The teams responsible for on-site visits shall consist of experts designated by Member States and of Commission representatives. The maximum number of Member States' experts participating in an announced on-site visit shall be eight and the maximum number of Commission representatives shall be two. The leading experts of an on-site team shall be a Commission representative and an expert from a Member State. The Commission may invite Frontex, Europol, or the European Data Protection Supervisor (EDPS) to designate a representative to take part as an observer in an on-site visit. The Commission shall establish a standard questionnaire in close cooperation with the Member States which shall cover the relevant legislation, commonly agreed recommendations and best practices, in particular as stated in the Schengen catalogues, and the organisational and technical means available for the implementation of the Schengen acquis and available statistical data on each field of the evaluation. By 1 July each year, the Commission shall send the standard questionnaire to those Member States which are to be evaluated in the following year. The Member States shall provide the Commission with their replies to the questionnaire within eight weeks of communication of the questionnaire.

3. Evaluation reports and recommendations

An evaluation report shall be drawn up by the on-site team following each evaluation which shall be based on the findings of the on-site visit and the questionnaire, as appropriate. In case of on-site visits, the evaluation report shall be drawn up by the on-site team during the visit. One of the following assessments shall be given to each finding in the evaluation report: 1) the evaluated Member State is compliant with the regulations, 2) the evaluated Member State is compliant with the regulations but improvement is necessary, 3) the evaluated Member State is non-compliant with the regulations. The Commission shall communicate the draft evaluation report to the evaluated Member State within six weeks of the on-site visit and the evaluated Member State shall provide its comments on the draft evaluation report within two weeks of its receipt. The Commission shall, after consulting the other Member States, adopt the evaluation report, which it shall transmit to the European Parliament.

Evaluation experts shall draft recommendations for remedial action aimed at addressing any deficiencies identified during the evaluation. Within three months of adoption of the recommendations, the evaluated Member State shall provide the Commission and the Council with an action plan to remedy any deficiencies identified in the evaluation report. Depending on the seriousness of the deficiencies identified and the measures taken to remedy them, the Commission may schedule announced on-site revisits to verify implementation of the action plan.

4. Participation of Hungarian experts in the Schengen evaluations

The Member States and the Commission are jointly responsible for implementing the evaluation and monitoring mechanism, which in practice means that the teams responsible for on-site visits are composed of experts nominated by the Member States and representatives of the Commission. Member States are therefore obliged to play an active role in appointing an expert to the evaluation teams. Accordingly, the Authority's staff also participate as experts in Schengen evaluations concerning data protection. In 2019, a staff member of the Authority participated in the Schengen evaluation concerning data protection of the Czech Republic.

5. Schengen evaluation of Hungary concerning data protection

The Schengen evaluation of Hungary took place in the autumn of 2019, at the end of the evaluation program of the Schengen Monitoring and Evaluation Mechanism for the period 2014-2019. In the context of a data protection on-site visit between October 7-11 2019, the Authority as the competent national data protection authority responsible for supervising the proper implementation of EU and national data protection legislation, in particular those related to SIS II and visa policies, was visited by a representative of the Commission and data protection experts appointed by the Member States The staff of the Authority presented the relevant national regulations, gave a presentation on the organization of the Authority, detailing its legal, budgetary and other guarantees ensuring the independence of the Authority. The Authority's supervisory activities and the results of data protection inspections carried out at bodies with access to the Schengen Information System and the Visa Information System were explained too. They also described the exercise of data subject rights, case statistics on submissions to the Authority, information materials on the Authority's website and customer service points, and international cooperation with Member State counterparts.

As the next part of the on-site program, the delegation visited the N.SIS II Office in the Deputy State Secretariat for the Management of Records of the Ministry of Interior as the body responsible for the operation of the national part of SIS II. The activities of the Office were presented by the staff of the Office, followed by presentations by colleagues representing external companies responsible for operation and development. Finally, the delegation also visited the server room hosting the NS.CP server and national interface. The visit then continued at the SIRENE Bureau as the competent authority responsible for the management of SIS II and its use for law enforcement purposes. In Teve Street, the DPO of the National Police Headquarters gave a presentation, and then the head of the SIRENE Bureau presented the operation of the organization, its tasks and the legal background of their activities. The delegation visited Activity Management Center of the Budapest Police Headquarters and made a short visit to the Police Headquarters of District XIII. The program continued at the Ministry of Foreign Affairs and Trade, and at the National Directorate-General for Aliens Policing as authorities with access to the Visa Information System and competent in the field of visa procedures. After a presentation by the Consular Service of the Ministry of Foreign Affairs and Trade, furthermore a presentation by the DPO, the organizational unit operating the Consular Information System and the developers, the on-site team also visited the central server room of the Ministry of Foreign Affairs. Finally, the delegation visited the National Directorate-General for Aliens Policing, where the architecture, operation and development of the national visa information system were presented. There was talk about the related tasks of the IT Department, compliance with the data security regulations and immigration procedures related to visa matters.

A member of staff from the Schengen Cooperation Unit of the Directorate-General presented their tasks in relation to data processing in the context of the Schengen Information System, their cooperation with partner authorities and the SIRENE Bureau, furthermore the way in which data subjects exercised their rights and the handling of requests and statistics. At the end of the program, a final joint consultation was held with members of the on-site team and representatives of all relevant bodies, where the remaining issues were clarified and the members of the Authority thanked everyone for their helpful cooperation during the visit. The Commission staff member and the team of experts shall draw up a draft evaluation report following the on-site visit and communicate it to the Authority of the evaluated Member State. The bodies involved in the evaluation shall provide their comments on the draft evaluation report. The Schengen evaluation of Hungary concerning data protection, i.e. the summary of the findings of the on-site visit and the finalization of the draft report, is still ongoing.

6. Changes due to the review of the evaluation and monitoring mechanism

The Commission has summarized the experience of recent Schengen evaluations (November 2014 - December 2019) and has revised and modified the standard questionnaire used for evaluations in the light of the experiences. The adoption of the new Schengen evaluation questionnaire was preceded by a consultation process in which Schengen Member States were able to comment on the new questionnaire. The amendments aim to speed up the evaluation process and make the practical implementation smoother, both in terms of on-site visits and follow-up. The Commission has also collected the most common errors and shortcomings over the last five years, as well as good practice as an example. The so-called SIS Supervision Coordination Group, which coordinates the data protection supervision of the Schengen Information System, shall draw up a list of good practices identified to help Member States which are to be evaluated in order to prepare successfully.

III.4. Participation in the Joint Supervisory Activity of Data Protection Authorities

III.4.1. Borders, Travel and Law Enforcement Expert Subgroup – BTLE

Earlier this year, the BTLE Expert Subgroup received a mandate to prepare guidelines on Article 47 of the Police Directive, which work is still ongoing. Furthermore, the BTLE developed methods for evaluation of large-scale IT systems in the area of freedom, security and justice. In December 2019, the Coordinated Supervision Committee (CSC) held its inaugural meeting in Brussels. The tasks of the CSC include the exchange of information, the conduct of inspections and investigations, the discussion of application and interpretation issues related to Regulation (EC) No 1725/2018, the resolution of problems related to the data subject rights as well as the development of other harmonized solutions. In April 2019, the expert subgroup was approached by the LIBE Committee requesting the opinion of the European Data Protection Board (EDPB) on legislative changes[7] related to the European Union's information systems. In its reply, the EDPB reiterated its previous concerns about the new system, i.e. the interconnection of the various information systems. In addition to the above, the expert group discussed and prepared specific parts of the report written by the EDPB on the Third Annual Review of the Privacy Shield Convention, concerning data processing for national security and criminal investigation purposes. In this context, the expert group discussed the rules of procedure of the EU Centralised Body (EUCB). The Privacy Shield agreement provides, as an important element of the Ombudsperson mechanism, that complaints from EU citizens shall be submitted to the Ombudsman by the EUCB which acts as the contact point. In addition to the planned tasks of the expert group, the issue of the processing of Passenger Name Record (PNR) data following the withdrawal of the United Kingdom from the European Union (Brexit) also arose. Some Member State authorities have reported that they have been approached by individual air carriers requesting their opinion on what will be the legal procedure for the transfer of PNR data (and thus the processing of PNR data in general) for

7 Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011

the United Kingdom after Brexit. The expert group found it useful to issue a joint opinion, however, this will only be possible once the open legal issues related to Brexit have been concluded.

III.4.2. Schengen Information System II Supervision Coordination Group (SIS II SCG)

The coordination monitoring team (Supervision Coordination Group) established under Regulation (EC) No 1987/2006 of the European Parliament and of the Council on the establishment, operation and use of the second generation Schengen Information System (SIS II), which entered into force on 9 April 2013, continued its activities in 2019 too.

The coordination group prepared a questionnaire related to the conditions for issuing alerts under Article 24[8] of the SIS II Regulation, in order to assess the differences between procedures of the Member States. The coordination group also aimed to examine the issuing of alerts on persons and objects for the purpose of discreet checks or specific checks pursuant to Article 36 of the SIS II. The SIS II SCG discussed and adopted its work plan for the next period (2019-2021), which includes, in addition to the above, the monitoring of the work of external service providers contracted with the N.SIS Offices of each Member State, typically performing technical and operational tasks, in order to comply with data protection rules. The SIS II SCG shall review its report on the exercise of the right of access, available on its website, in line with legislative changes, and will examine the procedures of the Member States to answer the requests for access, in particular to verify the identity of the applicant. The work plan also includes a discussion on the use of facial recognition systems and a collection of the most common recommendations received by different Member States in relation to Schengen evaluation, in order to effectively prepare for future evaluations.

The DPO of eu-LISA, the operator of the Schengen Information System, informed the SIS II SCG that eu-LISA had updated the transliteration standards centrally, making it easier for the system to deal with problems with different writings.

8 Regulation (EU) 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II); Article 24: Conditions for issuing alerts on refusal of entry or stayl

The inaugural meeting of the Coordinated Supervision Committee was held in Brussels on 3rd December 2019. The basic purpose of setting up the committee is to allow the working groups responsible for the coordinated supervision of large-scale IT systems in the area of freedom, security and justice to adapt their work schedules flexibly. Article 62 of Regulation (EC) No 1725/2018 (GDPR) provides for the coordinated actions by supervisory authorities. The first system to implement such coordinated supervision under the aegis of the EDPB is the IMI system, followed by Eurojust (2019). The transformation (SIS II, VIS, Eurodac) and the establishment (EES, ETIAS, ECRIS-TCN) of other coordinated control teams is ongoing.

In 2019, the Authority received 25 requests regarding the processing of personal data stored in SIS II. Most of these requests were questions related to the exercise of data subject rights (request for information, erasure), in which cases the Authority provided the complainant with general information on the right and procedure for contacting the SIRENE Bureau and on the means of redress.

III.4.3. The Visa Information Supervision Coordination Group (VIS SCG)

The aim of the Visa Information System is to support the implementation of the common EU visa policy, consular cooperation, and consultation between central visa authorities. The Visa Information System is used at the consulates of the Schengen Area where visas are issued and at external border crossing points, where border guards check the identity of persons with biometric visas. The aim of VIS is to ensure the identifiability of persons not fulfilling the conditions of entry and stay in the area of the Member States. The VIS is accessible by law enforcement authorities, asylum authorities, and the Europol.

During 2019, the Visa Information System Supervision Coordination Group conducted a survey on the data protection training of the staff of authorities with access to the Visa Information System. The VIS SCG finalized its activity report for the previous period (2017-2018) and prepared its work plan for the next period (2019-2021). The VIS SCG decided to develop a joint supervision plan, based on the method used for supervision of the SIS II, including a questionnaire on the data security of the Visa Information System assessing compliance with the

9 Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II); Article 36: Objectives and conditions for issuing alerts

minimum requirements. In the working plan, the group also identified tasks that could be added to the draft, such as conducting coordinated on-site visits at consulates, self-monitoring under Article 35 of the VIS Regulation , monitoring advance data deletion (under Article 25) or the procedure under Article 31 .

In 2019, the Authority received 3 requests relating to the Visa Information System, which were answered within the framework of providing general information, and the Authority did not initiate a review procedure in any case.

III.4.4. The Eurodac Supervision Coordination Group (Eurodac SCG)

REGULATION (EU) No 603/2013 established the Eurodac system, enabling the countries applying the Dublin Regulation to establish by the comparison of fingerprints in the Eurodac System which Member State is oblige to carry out the asylum procedure. For the purposes of protecting personal data, the Member States sending data to the Eurodac shall ensure that the taking of fingerprints and the operations related to the processing, transfer, storage, and erasure of data are lawful. Data processing by the Eurodac is supervised by the European Data Protection Commissioner in cooperation with the national supervisory authorities (Eurodac SCG).

The Eurodac Supervision Coordination Group finalized its report on the exercise of data subjects' rights, which can be found on the Eurodac SCG website. The Eurodac SCG, together with the European Union Agency for Fundamental Rights (FRA), prepared a material to inform data subjects. The information leaflet is a brochure written in understandable language illustrated with icons with the aim of providing data subjects with adequate information about the processing of their fingerprints and their rights. Emphasis is placed on the communication with children and icons indicate what information needs to be provided orally and / or in writing before taking the fingerprints. The Eurodac SCG prepared its work plan for the next period (2019-2021), which includes a jointly developed inspection method to be used by Member States for national control activities, a survey of law enforcement agencies with access to the system (including Europol) and the examination of false alarms.

10 Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation)

11 VIS Regulation Article 31: Communication of data to third countries or international organisations

III.4.5. Customs Information System Supervision Coordination Group and the Europol Cooperation Board

In 2019, representatives of the Authority continued to attend the meetings in Brussels. As in previous years, the future of FIU.net and its relationship with SIENA continued to be a key topic in the discussions. Furthermore, the group also addressed the transfer of personal data concerning minor suspects and the changes in the relevant legal situation regarding data processed by Europol after the UK's exit from the EU.

IV. Freedom of Information (FOI)

IV.1. Introduction

In 2019, the Freedom of Information Department had a total of 663 pending cases, of which 489 were initiated that year and 174 were cases carried over from the previous year. The number of authority proceedings for data protection initiated in 2019 was 11 (cases where there was a conflict or collision between the two information rights), and the number of consultation cases was 116.

In addition, the Department had 17 cases of delivering opinion on legislation. In this regard, it should be noted that Section 38 (4) (a) of the Privacy Act explicitly authorizes the Authority to give its opinion with respect to draft laws concerning data of public interest and to data accessible on public interest ground, which is in line with Section 7 (b) of Act CXXXI of 2010 on public participation in developing legislation. The latter Act aims to ensure widespread knowledge of the law as data of public interest as well as to promote social participation in the legislation.

Based on complaints received by the Authority in 2019, the interests of the citizens continue to be extremely diverse: it focuses on subjects among others like real estate acquisition statistics of foreigners to state aid for sports and sport events to the salaries of municipal notaries. In response to these, in the autumn of 2019, the NAIH also issued two detailed guides of great significance on the operation of the bodies of local governments and on public procurement data[12] . The Authority is convinced that the thematic professional guidelines will effectively contribute to the clear solution and uniform application of issues important for the public and for those applying the law.

12 https://naih.hu/freedom-of-information-in-hungary.html

IV.2. International outlook

As it was stated at the International FOI Symposium in Potsdam, held annually by the Brandenburg Information Commissioner[13] , everyone should be aware that transparency is a multiplier for efficiency and opposing state intentions have a counterproductive effect.

In 2019, NAIH was one of the first to be accredited by the International Conference of Information Commissioners (ICIC)[14] , which is the only international network of worldwide FOI supervisory bodies. The Authority has participated in the work of the ICIC Governance Group since its establishment.

In March 2019, participants from more than 50 countries convened in Johannesburg at the 11th International Conference of Information Commissioners (ICIC)[15]. The conference was chaired by Adv. Pansy Tlakula, Chairperson of the Information Regulator of South Africa (an independent body supervising the enforcement of the two information rights), nominated by the parliament for five years in 2016 and appointed by the President. Ms Pansy Tlakula served as Chairperson of the South African Commission on Human Rights from 1995 to 2002 and was a member of the African Commission on Human and Peoples' Rights. From 2010-12, she held the mandates of Special Rapporteur on the African Model Law on Access to Information, which has since been used as a model legislation of 23 African countries.

At the conference, weighty consideration was given to the needs of vulnerable social groups. The final statement of the conference also emphasizes that it is vital for vulnerable groups not only to have access to information of public interest, but society must also be informed of their special situation and needs. Emphasis was placed on presenting different models for the status of the supervisory body - independent or joint legal protection with data protection, independence criteria, separate law or common legal norm, etc. The other main issue concerned the interaction between data protection and freedom of information. African Information Commissioners have repeatedly emphasized that the right of access to information that functions as Community law clearly takes precedence over the right to the protection of personal data as an individual right in Africa. At the

13 https://www.lda.brandenburg.de/cms/detail.php/bb1.c.648047.de?highlight=Symposium
14 https://www.informationcommissioners.org/hungary
15 https://www.informationcommissioners.org/icic-2019/programme

same time, the growing nature of the interaction is undeniable, for example in the field of electoral procedures, the publicity of public databases or public officials.

Another important event of international importance is the continuation of the Case Handling Workshop placing practical topics on the agenda, which was held for the first time in Budapest last year. In 2019, the event was hosted by the Gibraltar Supervisory Authority[16] and focused on the issue of the conflicts between competing legal regimes in freedom of information matters, government contracts with businesses or transparency in the work of emergency hotline services.

IV.3. Important decisions of the Constitutional Court

In 2019, the Constitutional Court adopted several major decisions on FOI, which are of particular significance in the interpretation of law by the Authority.

Decision of the Constitutional Court 3190/2019. (VII. 16.) on publicity of the Paks II. nuclear power plant impact studies

Taking also into account the Authority's resolution NAIH/2017/2365/2/T, the Constitutional Court rejected the constitutional complaint against the decision of the Szekszard Regional Court on the refusal to disclose data of public interest.

The complainant requested all impact studies related to the expansion of the Paks Nuclear Power Plant to be made available by the nuclear power plant developing company MVM Paks II. Atomerőmű Fejlesztő Zrt. The data request was rejected with reference to the possible restriction of the right to access data underlying a decision. The court found this argument to be well-grounded. According to the Constitutional Court, what constitutes a decision in terms of freedom of information is a question of interpretation of an intergovernmental agreement promulgated by law. The legal interpretation of the court, including the scope of environmental data, complies with the provisions of the Fundamental Law, as in a series of negotiations concerning investments of national security and national strategic importance, such as the expansion of the Paks Nuclear Power Plant,

16 https://www.gra.gi/data-protection/press-releases/freedom-of-information-workshop

the protection of the Hungarian negotiator and the Hungarian state may make it necessary to restrict the right to access data of public interest

Decision of the Constitutional Court 3147/2019. (VI. 26.) on the obligation of confidentiality of the „data subject" of data accessible on public interest grounds concerning the use of public funds

A serial actor concluded an assignment contract with a film production company on playing the main character of a movie series financed by the Media Services and Support Trust Fund (MTVA). The actor has also undertaken in the contract – under the obligation of penalty payment – to handle the assignment fee as a business secret. When the production company had called off the assignment contract concluded with the actor, he disclosed the amount of the assignment fee in a press product on the internet. The production company sued the actor for the payment of the penalty. The courts of first and second instances had obliged the petitioner to pay the penalty and the Curia approved the final judgement. The Constitutional Court did not take a position on whether the disputed data (e.g. the information on the amount of the assignment fee included in the contract and subject to the obligation of confidentiality) qualifies as a data of public interest or data accessible on public interest grounds, as it is the duty of the courts to assess this in case of legal dispute. However, the Constitutional Court pointed out that organisations managing public funds shall not deny access to data accessible on public interest merely with reference to a contractual confidentiality clause.

Decision of the Constitutional Court 3069/2019. (IV. 10.) and Decision of the Constitutional Court 3070/2019. (IV. 10.): in the case of publicity of data related to the opinions and resolutions obtained in the context of preparing the uniformity decision of the Curia, the examination of the content of the data, on which the decision is based, is obligatory

In the underlying case of the constitutional complaint the petitioner asked the court – after the rejection of its request for the disclosure of data of public interest – to bind the Curia to disclose the data related to the opinions obtained in the context of preparing the relevant uniformity decision of civil law.

The Constitutional Court has found the following:
The decisions of public servants are prepared freely, informally and free from public pressure. Thus, the requirement of publicity applies only to the final outcome rather than the intermediary working materials. The legal interpretation that considers the totality of the requested documents – irrespectively to their content – as data that serve the purpose of supporting the decision-making, this way preventing access to the documents, allows for the unjustifiably broad – therefore unnecessary – restriction of the right to access data of public interest. In the case under review, the Constitutional Court established that, as the court had had no information about the identity of the persons who had provided external opinion and about the content of the opinions, it had decided in the case without actually examining the material justification of restricting publicity. This way the court placed the totality of the requested documents under the restriction of publicity without paying attention to their content. A judicial decision that allows for the restriction of fundamental rights to an extent wider than necessary is incompatible with the Fundamental Laws.

Decision of the Constitutional Court 13/2019. (IV. 8.): interpretation of the definition of data of public interest, the limits of the obligation to produce data of public interest

The petitioner requested(in the framework of a scientific research) data disclosure in the public interest, the Curia to disclose the list and certain data (case numbers, date of submitting the statement of claim, the names of the litigating parties in the case of legal entities) of civil litigations pending for at least seven years. However, the Curia stated that it was unable to provide the requested list of data as it did not have a record on the dates of submitting the statement of claim.

The Constitutional Court pointed out: request for data – not exercised in an abusive manner - should not be refused by referring to the extra work implying time or cost needed for making the requested data accessible. Nevertheless, a differentiation should be made concerning the case when the request for data is not aimed at disclosing data retrievable with additional work, but for inducing the controller to obtain new data or create data of another quantity, statistics or statements from the data it processes otherwise. The openness of the operation of the judiciary as a separate branch of power, does not differ fundamentally from that of other organizations financed from public funds. The duty of the Curia is to develop the uniformity of the case law of the courts and, primarily, to decide

about extraordinary legal remedies. The date of submission of the statement of claim and the connected duration of the procedure reaching or extending over seven years - although it is deductible from the court files - is not considered as data created in connection with the Curia's activity or the performance of its public duties. Furthermore, the Curia has no monopoly over the information requested to be disclosed as the court of first instance, in accordance with its duties specified in the procedural Acts, necessarily contributes to all essential points of the civil procedure, including the registration of the date of submitting the statement of claim. By taking into consideration all circumstances, the Constitutional Court rejected the petitioner's constitutional complaint.

Decision of the Constitutional Court 29/2019. (XI. 4.): criticism of a person performing public duties (notary) in social media - the question of proving reality

In multiple cases in 2011, a citizen criticised the notary of the municipality on the message board belonging to his own account of an Internet social media portal. Furthermore, at a local public hearing, he stated before the public that the victim notary had denounced him twice and he had made a false testimony at the police.

In the action brought by the notary for the enforcement of personality rights, the Curia maintained the force of the judgements of the courts of first and second instances stating that the petitioner was guilty of the offence of libel and the continuous offence of defamation. According to the reasoning of the Curia, what was said is relevant only in relation to the accused and the aggrieved party, and not in the context of the public life of the city, so it certainly cannot be regarded as information of public interest, and their presentation at a public hearing was not justified by a legitimate private interest.

On the basis of the complaint submitted by the petitioner, the Constitutional Court annulled the Curia's approving ruling maintaining the force of the judgements of the courts of first and second instances, stating that the court made its decision in accordance with the relevant constitutional criteria, but the constitutional conclusions drawn from it are incorrect. When interpreting the limits of freedom of expression, especially its restriction by criminal law, the Constitutional Court has set a stricter standard than "offence to the sense of honour". According to the interpretation that further develops the previous practice on the basis of the Fundamental Law, in the debate of public affairs, criticism or value judgment affecting the exerciser of public power or a public figure cannot, as a general rule,

be the basis for legal liability. In this context, only those communications go beyond the constitutional limit of freedom of expression that offend human dignity, i.e. the content of dignity that legally captures the essence of human nature. Furthermore, the reasoning of the judgment against which complaint was submitted, did not set out the reasons why the statement of facts in question was 'relevant only in relation to the accused and the aggrieved party, and not in the context of the public life of the city'.

After the decision, the Curia repeated the review procedure and again it maintained the force of the final decision. Against this decision, the petitioner filed a second constitutional complaint with the Constitutional Court, according to which there is no obstacle for the court to reaching a different conclusion from the challenged decision as a result of balancing between freedom of expression and the protection of reputation. The expressions used by the petitioner had been protected by the freedom of expression, because the criticism had not violated the essential core of the human dignity of the affected public figure. However, by maintaining the force of judicial decisions that criminalised the protected expression of opinion of the petitioner, the Curia violated the petitioner's right under Article IX (1) of the Fundamental Law. In connection with the reference to false testimony, the Constitutional Court considered the challenged judicial decision unconstitutional because it did not state why the statement of facts relating to the aggrieved party fell outside the scope of debate of public affairs. In the debate of public affairs, the accused must be given an opportunity to prove the truthfulness of its statement considered as defamation. This cannot be substituted, if in the course of a review procedure (when the subsequent taking of new evidence is not possible), the Curia concludes that the statement of the accused has already been established to be untrue.It is one of the guarantees of the freedom of expression that the courts examine, also in the framework of the basic procedure, the truthfulness of the statements made by the accused person, and this person may enforce his or her procedural rights in a formal way. The Constitutional Court therefore annulled the decision again and, in view of the importance of the constitutional issue, ordered that the decision be published in the Hungarian Gazette.

IV.4. Rules of the Reimbursement of Costs Regarding Data Requests – Recent developments

In the autumn of 2019, the Constitutional Court dealt with the reimbursement of costs related to the disclosure of data of public interest in two decisions:

Decision of the Constitutional Court on the examination of the posterior norm control against Section 4 (4) of the Government Decree 301/2016. (IX. 30.) on the amount of the cost reimbursement chargeable for performing a request for data of public interest (Case Nr.: II/1808/2016.sz.)

The provision challenged by 58 members of parliament (MP) regulates the amount of the cost reimbursement chargeable for performing a request for data of public interest. According to the petitioner MPs, the challenged provision does not take into account the average wage costs of the staff members engaged in the relevant activity, and the hourly rate of HUF 4,400 is exaggerated, therefore, the provision is in breach of the right to access data of public interest, as it requires payment in consideration of exercising a fundamental right. The Constitutional Court first pointed out that it is not obligatory to charge a cost reimbursement for the labour input used in the course of performing the request for data of public interest, and even if it is indeed charged, neither the Privacy Act, nor the Government Decree specify in advance the exact amount chargeable for using the workforce, as it actually depends on the real labour costs.

Therefore, the Constitutional Court states that the provision, which only specifies the maximum amount of the labour charge per working hours connected to performing the data request is not contrary to the provision of the Fundamental Act. Actually, the challenged provision is not a limitation on the freedom of information, as in a certain sense, – by introducing the upper limit – it facilitates access to data of public interest and data accessible on public interest grounds, since in the case of annulling the provision, the position of the parties requesting data would become less advantageous than the present one. With regard to the above, the Constitutional Court rejected the petition of the MPs for posterior norm control.

Decision of the Constitutional Court relating to the constitutional complaint against the judgement No. Pfv.IV.22.218/2017/4 of the Curia (reimbursement of costs for performing a request for data of public interest) (Case Nr.: IV/1013/2019.)

The petition essentially contained criticism of the judicial interpretation and application of law in connection with the reimbursement of expenses related to paper-based data disclosure by post. The petitioner requesting the data considered the postage fee of HUF 680, determined on the basis of the Government Decree, to be infringing. First, the petitioners applied to the NAIH, and then, after the NAIH did not established an infringement, an action was brought before the court to modify the reimbursement of costs related to the disclosure of data of public interest. They argued that, under the relevant legislation, postage cost can only be charged for sending a copy of the document containing the requested information, but not for a simple reply letter without a copy. They also questioned that they would be required to reimburse postage costs for two letters. The courts found that the reimbursement was made in accordance with the provisions of the Privacy Act and the Government Decree, as the paper in the postal envelope containing the reply shall be considered as a data media. The amount of the reimbursement is also not unlawful, as double postage cost was charged for mailing to the two applicants. The petitioner then filed a constitutional complaint with the Constitutional Court, which found that the mere fact that the petitioner considered the reasoning of the otherwise justified court judgment to be incorrect, was not a constitutional issue. Pursuant to the Government Decree, the cost of workforce may not exceed HUF 4,400. This amount was calculated on the basis of the gross hourly earnings of the civil servants employed full-time at central budget bodies, as provided by the Central Statistical Office during the preparation of legislation, by rounding it up (the exact amount was HUF 4353.4). The legal provision has been adjusted to this amount because many types of bodies, different in terms of their legal status and operational framework, are obliged to fulfill requests for data in the public interest, and the employees of these bodies are also subject to different laws on legal status. Nevertheless, according to the presumption of the legislator, data requests are typically fulfilled by central state administration bodies, therefore it is justified to take the average earnings of persons employed here as civil servants as a basis.

In 2019, the NAIH received 32 complaints by citizens objecting to the legal basis of charging reimbursement of costs or disputing the amounts charged. The Ministry of Finance, the Hungarian Central Bank, the Public Procurement and Supply Directorate, local governments, government offices, as well as companies owned by state or local government, and public institutions were among

the data controllers. The amounts determined showed a great variety; sums of a few 10 thousands of forints were most usual, but there were charges running up to several hundred thousands, and in some striking cases even million forints (Pécs Sport Nonprofit Zrt .: HUF 4,841,000; Hungarian Army Health Center: HUF 3,805,000, National Police Headquarters: HUF 2,966,575). The highest cost reimbursement, nearly HUF 9 million, was determined by the Hungarian Tennis Association.

Significant proportion of the cases closed resulted in the data controller fulfilling data requests without charging fees or reducing the fees based on miscalculation and returning the fees that had been paid. This was the result of our inquiries of e.g. the Hungarian Central Bank, the Public Procurement and Supply Directorate, the FEV IX. Ferencváros Asset Management and City Development Inc., and the Érd District Office of the Pest County Government Office.

At the same however, it is true that several inquiries commenced last year were still unclosed at the time of drafting the report, as the positions did not come nearer even after several exchanges of correspondence. In one such case, the Ministry of Finance established a reimbursement fee of HUF 33,033 for 17 working hours related to the fulfillment of the data request, and a reimbursement fee of HUF 36,510 for 19 working hours. In both cases, the Authority found that the fulfilment of the data request cannot be considered to be a disproportionate use of the workforce for an organization of this size. (NAIH/2019/944, NAIH/2019/982).

Fulfilling a data request necessarily involves certain amount workforce allocation – this is an institutional concomitant of the fundamental right to access data of public interest. However, organs performing public duties shall be prepared to receive requests for access to data of public interest, or data accessible on public interest grounds related to any of their activities. The Authority came to a similar conclusion in the case of the fee of HUF 176,000 determined by the NIF Hungarian National Infrastructure Development Company. Due to the disagreement of the data controller, the inquiry ended with the publication of the findings. (NAIH/2019/507).

In court (remedy) proceedings, the burden of proof for the justification of the amount of the fee, shall lie with the controller, therefore, it is important to have a detailed, accurate calculation and documented costs. The court may modify the amount charged for fulfilling the request for access to the data of public interest, or may order the organ performing public duties to commence a new procedure to determine the amount of the fee payable.

The right of access to data of public interest is not an unrestricted fundamental right, however, it enjoys privileged constitutional protection as one of the conditions for and part of the exercise of the right to freedom of expression.
Accordingly, laws restricting freedom of information must always be interpreted strictly. In a concrete case of a complainant, and in accordance with Section 4 (3) of the Decree, the Authority found that the amount of the social contribution tax to be paid by the employer could not be charged to the data requester, therefore ordered the data controller to repay it. The municipality concerned complied with the order. (NAIH/2019/5705)

Freedom of information as a fundamental right requires transparency served by sufficiently detailed information on the reimbursement of costs relating to the fulfilment of data requests, in which the public service bodies are obliged to indicate all the reasons and cost elements that were taken into account when determining the fee. Appropriate information contributes greatly to the data requester's true understanding of why and what reimbursement he or she must pay in order to obtain access to the data he or she wishes to know.

The amount of workforce cost should be calculated based on the actual work processes. The Authority has repeatedly drawn the attention of data controllers to give an explanation what work processes are required by fulfilling the data request. In one case, the ORFK informed the data requester that headcount and decommissioning data, covering the entire professional police staff, were handled by the police based on the data of January 1 of each year. Thus, in order to compile a statement containing data broken down by body and on a monthly basis, it would be necessary to carry out a national data collection involving all relevant police bodies exercising the employer's rights. Accordingly, the ORFK precisely indicated the circumstance due to which the fulfillment of the data request would have involved a disproportionate use of the workforce necessary for the performance of the core activity of the body performing public duties. (NAIH/2019/4306). In such cases, it is also worth for data requesters to consider whether it is appropriate to maintain the request for data of public interest in an unchanged form. Data requesters may at any time, after consulting the controller, decide to change the form or manner in which they wish to receive data of public interest, of course in such a way that the data request achieves its purpose, thereby significantly reducing or even eliminating the cost of the data request.

In another case, an organ performing public duties provided for significant reimbursement (HUF 355,600) for the sole reason that „the involvement of a DPO

(Data Protection Officer) is necessary for the data protection control of contracts". In this regard, the Authority drew the data controller's attention to the fact that the mere fact that certain personal data in the contracts have to be anonymised and that this task is controlled by the DPO, does not justify the claim for reimbursement (NAIH / 2019/5915).

In cost-reimbursement cases, it is also important to emphasize that when determining the reimbursement of less than HUF 5,000, the fulfilling of the data request cannot be made subject to prior payment of a specified fee, and the first 4 working hours cannot be charged in advance [Government Decree Section 3 (1)]. It often causes uncertainty that it is not clearly indicated in the cost calculation if the said 4 working hours have already been deducted.

IV.5. Important court decisions

I. Market operators that establish a financial or business relationship with a person or organisation belonging to one of the sub-systems of the public finances, shall expect wider publicity.
II. If the request meets the minimum requirements for the specific identification of the requested data, the request shall be dealt with on the merits. Furthermore, if necessary, as a sort of active obligation, the requesting party shall be called on to clarify the request. (Court of Appeal of Pécs Pf.III.20.036/2019/4.*)*

If the data controller cannot prove in a lawsuit for access to data of public interest a decision-making process in which the data to be disclosed is used, it cannot effectively refer to the decision-underlying nature of the data, or to the fact that the disclosure of the data would jeopardize the lawful functioning of the organ performing public duties, or would jeopardise the performance of its duties without any undue external influence. Restrictions on publicity cannot be based on the possibility of an opinion being delivered at an uncertain date in the future. (Metropolitan Court of Appeal 32.Pf.20.913/2018/4-II.)

When fulfilling requests for data of public interest, bodies performing public duties shall, as a general rule, make the requested data available to citizens free of charge in the normal course of day-to-day operations. Fulfilling the data request necessarily involves a certain amount of workforce - this is an institutional concomitant of the fundamental right to access data of public interest. Only the cost of workforce exceeding four working hours may be charged to the data

requester, if the fulfilment of the data request would involve a disproportionate use of the workforce necessary for the performance of the activities of the body performing public duties. The assessment of this shall be made in each case by careful consideration of all the circumstances. (Metropolitan Court of Appeal 8.Pf.20.420/2019/5.)

I. Personal and special data disclosed during court proceedings do not share the legal fate of data of public interest or data accessible on public interest grounds. II. The publicity of the hearing in the litigation procedure is not the same as publicity of the litigation documents. Interested parties may appear at the hearing and observe the oral procedure, but this right does not include access to documents. Documents in litigation procedure, including the minutes of hearings, may not be disclosed because of the personal data they contain, even if the procedural act of which they were made, has otherwise taken place in public. (BDT2005. 1277., Court of Appeal of Győr Pf.I.20.238/2016/7., Metropolitan Court of Appeal 17.Pf.21.336/2017/7., Court of Appeal of Szeged Pf.I.21.182/2017/14.)

On the interpretation of Section 27 (3a)[17] of the Privacy Act:
'The court of second instance shared the view of the judgment at first-instance regarding that the defendant, as a person outside the public finances, manages its own assets, risks and responsibilities when concluding material supply contracts, in order to fulfil a business agreement with a person belonging to the subsystems of the public finances. However, in the view of the Court of Appeal, it is not relevant that this created a new obligation. On the other hand, the Court of Appeal emphasizes that the link between the data, obtained in the context of the legal relationship between the defendant and its suppliers relating to the type, quantity, source and cost of all raw materials built-in in an EU-funded investment, and the public funds as a source, is too remote and indirect for the defendant to provide information about its details as data accessible on public interest grounds in accordance with the rules of Section 27 (3a) of the Privacy Act. On the basis of a grammatical interpretation of this section, the court of second instance also states that it is the person establishing a financial or business rela-

17 Section 27. § (3a) of the Privacy Act: A natural person, legal person or organisation having no legal personality that establishes a financial or business relationship with a person belonging to one of the sub-systems of the public finances shall, upon request, provide information to anyone with respect to data that is public on public interest grounds based on paragraph (3) and that is in connection with such a relationship. The obligation to provide information can be fulfilled by disclosing the data accessible on public interest grounds, or by indicating the public source that contains the data disclosed earlier in an electronic form

tionship with a person belonging to the sub-system of the public finances, who is obliged to provide data, namely with regard to the data accessible on public interest grounds relating to the legal relationship between the two of them. The contracts between the defendant and its subcontractors are not related to the sub-systems of public finances, thus the obligation to disclose data pursuant to Section 27 (3a) of the Privacy Act cannot be interpreted for them.'
Judgement Nr. 8.Pf.20.031/2019/5. of the Metropolitan Court of Appeal

IV.6. Data of persons in the public service accessible on public interest grounds

In the 2018 annual report of the NAIH, we devoted a separate subchapter to the publicity of data of employees accessible on public interest grounds, and the publicity of certain types of data in various categories of employment relations.

In 2019, one of the important developments in this area is that Act CXXV of 2018 on Government Administration (hereinafter: Government Administration Act or Kit.) entered into force on 1 January 2019, which created a separate law for the legal relationship of public service officials (government officials, state officials).

Act CXCIX of 2011 on Public Service Officials (hereinafter: Kttv.) lists which data are considered to be data accessible on public interest grounds (the name, citizenship, the name of the public administration organ employer, the beginning of public service relationship, classification data, position, date of appointment to lead position, granting of title, and remuneration).

However, neither the Government Administration Act nor Act CVII of 2019 on special status bodies and the status of their employees (hereinafter: Küt.), applicable only from 1 May 2020, contains a provision analogous to this.

As a result, the situation has arisen that different rules of publicity may be applied to employees of public administration bodies subject to different laws (Kttv., Kit., Küt.). Thus, while in respect of an employee in the public service subject to the Kttv, the data listed above, including the remuneration, are accessible on public interest grounds, but these data in the case of an employee holding a similar position but subject to the Kit. or Küt., no longer qualify as data accessible on public interest grounds pursuant to the Kit. and Küt.

On the one hand, this may, without a justifiable constitutional reason, lead to the discrimination of employees subject to the Kit., Küt. or Kttv., who, in the opinion of the Authority, belong to a homogeneous group, and to the violation of the requirement of equal treatment. On the other hand, it also results in a situation that violates the legal certainty in the application of law, with regard to Section 26 (2) of the Privacy Act.

Pursuant to Section 26 (2) of the Privacy Act, the name of the person acting within the functions and powers of the organ performing public duties, as well as his functions and duties, executive mandate, and his other personal data relevant to performing public duties, shall qualify as data accessible on public interest grounds.

On the basis of the consistent practice of the Authority related to this provision, the data on relating to remuneration is considered to be data accessible on public interest grounds in the case of an employee acting within the functions of the organ performing public duties. Having regard to the provisions of the Privacy Act, there is no reason to deviate from this practice, even after the Kit. and Küt. entered into force.

At the same time, for the sake of legal certainty, it should be avoided that in the absence of a specific provision requiring publicity among the types of data specified by law, the scope of interpretation of the term 'data relevant to performing public duties', as specified in Section 26 (2) of the Privacy Act, is referred by the regulation to the scope of the abstract legal interpretation of the data controller body performing public duties, requiring individual consideration.

The Authority's experience also confirms the difficulties of legal interpretation arising from this legal situation. In connection with a specific notification in 2019, the Authority took the position that the remuneration and bonus of the head of the government office, as well as of the head and deputies of the district office subject to Kit. are data accessible on public interest grounds, given that they are clearly related to the function of persons performing public duties. However, other social benefits are no longer considered data accessible on public interest grounds. In relation to them, instead of providing personal data, only aggregated data shall be provided in a non-identifiable manner.

In line with the domestic law enforcement practice and the previous decisions of the Constitutional Court, as well as with its resolution NAIH/2015/7163/2/V, the position of the Authority is unchanged regarding that the scope of data, specified in Section 179 of the Kttv., in relation to employees subject to the Kit. and Küt. shall be accessible on public interest grounds.

On the basis of the above, the Authority addressed a recommendation to the Ministry of Justice to prepare the necessary amendments to create a clear legal situation.

IV.7. Local public affairs – openness of the operation of the bodies of local governments

2019 was a year of local elections and the increased interest of the constituent citizens in the transparency of local government operations became noticeable already in the previous period. Furthermore, the new representatives and mayors also raised issues and asked questions in many cases. A full[18] as well as an abridged version[19] of the NAIH guide on the openness of the operation of the bodies of local governments is available on our website, and this professional compilation reached all local governments through the Local Government Newsletter edited by the Ministry of Interior. The guide highlights the enforcement of the data principle rather than the document principle, furthermore, it details the conditions of closed sessions, the right of the municipal representatives to access data, the publicity of welfare cases, accessible information on municipal rental housing and provides guidance on mandatory publication of data and anonymisation.

The guide emphasizes that the local government representative does not have independent tasks and powers. Thus, his or her work primarily involves participating in the preparation, organization and monitoring of decisions on certain matters falling within the decision-making competence of the body of representatives and its committees. In the performance of his duties, the representative may access the necessary amount of data only during the discharge of the public task, in accordance with the principle of necessity and proportionality of the data processing. This also applies to the protocol of closed sessions held before the term of office of the representative, as well as to access to the data of the welfare records kept by the municipal notary. Thus, the representative may only have access to the relevant documents in a specific case to the extent necessary for the discharge of his tasks. (NAIH/2019/8161).

18 https://naih.hu/files/NAIH-guide-on-the-openness-of-then-operation-of-the-bodies-of-local-governments2019.pdf

19 https://naih.hu/files/ShortNAIHGuide-on-then-openness-of-the-operation-of-the-bodies-of-local-governments.pdf

With regard to the protected data obtained in connection with their duties, the representatives and committee members may not provide information to third parties, they may not forward the data to them or allow them to inspect them.

When implementing data security, the main goal is to prevent the transfer of data to unauthorized persons. This can also be achieved if an internal, closed electronic mail circle is provided for the local government representative or committee member, thus preventing the document from being sent or forwarded to an "external" e-mail address. (NAIH/2019/8337.)

From the viewpoint of data protection, the correct procedure is when the submissions produced for the closed session are returned by the participants of the session after the decision of merit is made. It is expected of the person chairing the session to warn the participants of the session to handle the information on the case confidentially and their related obligation of confidentiality.

The submissions to and the protocol of the closed session shall not be subject to the obligation of publication, only the anonymised decisions of the closed session or the decision itself must be published. The Authority is consistent in its view that a request for access to data of the closed session cannot be rejected without examination on the merit, on the sole ground that the matter was discussed or decided in closed session and therefore cannot be disclosed.

Whether a session of the body of representatives is open or closed will determine the accessibility of the submissions and the decisions made there, as well as the protocol of it. The submissions and statements made at open sessions and the events taking place there qualify as data of public interest (or public data accessible on grounds of public interest), hence as a major rule the relevant data and information (submission, decisions, voting ratios) can be accessed freely by anyone without limitation and they can be disseminated. At the same time, it may happen that the documents of the open session include data subject to restriction on access.
In such a case all the protected data must be rendered illegible in all of the documents concerned. The obligation to protect the data holds despite and besides publication.

In the case of disposal over municipal assets and in the cases listed under Section 46(2) c) of the Local Government Act[20] –if an open session would infringe upon the business interests of the local government or another stakeholder, the body of representatives may order a closed session –exercising its power to weigh the matter. In line with the Fundamental Law, Section 7 of the National Assets Act[21] declares that the fundamental purpose of the national assets is to ensure the discharge of public tasks.

In the context of the possibility of discussing submissions related to municipal assets in closed session, the Authority underlines the importance of ensuring a wide range of publicity and if possible, not to order a closed session.

Resolving the conflict between trade secrets and the freedom of information, Section 27(3) of the Privacy Act, in case of the use of public funds, qualifies the "quasi" trade secrets as data accessible on public interest grounds. In this case, if the discloser expressly marks the parts concerning the trade secret and explains in detail the reasons for protection of the trade secret, the local government, as its contracting party, may not disclose it.

Section 46 of the Local Government Act provides for the openness of the sessions of the body of representatives and the conditions of holding closed sessions. Section 2 of the Local Government Act declares the openness of the sessions of the body of representatives as a principle, which is confirmed by the legislator in Section 46 (1) of the Local Government Act. In addition, each body of representatives must determine separately, in its own operating rules, how to ensure publicity, which binds the local government in disclosing the data. Participation in an open session of the body of representatives can take several forms: most often in person, but more and more local governments use live coverage of the sessions of the body of representatives e.g. on the local / local government television or radio channel or on the Internet (on the website of the local government, or social media), as a way of ensuring publicity. Pursuant to Section 26 (2) of the Privacy Act, personal data accessible on public interest grounds included in these recordings may be disseminated in compliance with the principle of purpose limitation. (NAIH/2019/7890, NAIH/2019/8077, NAIH/2019/8173, NAIH/2019/8256, NAIH/2019/8337).

20 Local Government Act: Act CLXXXIX of 2011 on the Local Governments of Hungary
21 National Assets Act: Act CXCVI of 2011 on the National Assets of Hungary

IV.8. Publicity of Public Procurement Data

Public procurement procedures are initiated by organisations managing public funds or certain undertakings outside the competitive sector (such as energy or water suppliers, public transportation companies, postal service providers) to procure services, goods or works above a certain value limit. Ensuring transparency and the public's ability to control the efficient use of public funds is one of the key principles of the public procurement procedure. The Authority is of the firm view that, both the acts of the contracting authority and the documents submitted by tenderers in public procurement procedures fundamentally contain data of public interest and data accessible on public interest grounds. Publicity and transparency can be ensured through mandatory publication, inspecting documents and the fulfilment of requests for data of public interest.

The phases of the public procurement procedure:

I. Preparatory phase: planning public procurement procedures, annual public procurement plan, drafting the rules of public procurement
II. Launching the public procurement procedure -invitation to tender
III. Supplementary informations
IV. Preliminary dispute resolution, inspecting documents
V. Opening of the tenders received
VI. Bid evaluation (summary of tender evaluation)
VII. Request to make up for deficiencies
VIII. Notification of the tenderers on the results of the procedure (eventually legal remedy procedure, inspection of documents)
IX. Conclusion of the contract with the winning tenderer, performance

The decisive point in terms of freedom of information is the decision on the selection of the winning tenderer and the conclusion of the contract. From then on, the data of the public procurement procedure can no longer be qualified as data supporting decision-making.
The law explicitly specifies to whom, when and what data shall be published in the electronic public procurement system (EKR) and on the website of the Public Procurement Authority. Thus, the public procurement plan, the names of the contracting parties, the concluded contracts and any amendments to the contract, as well as the data relating to the performance of the contract shall be published. These data are published at the Internet site https://ekr.gov.hu/portal/¬kezdolap.

The rules of general administrative procedure apply to the public procurement procedure and the legal remedy procedure of the Public Procurement Arbitration Board, based on which tenderers and other clients may, in justified cases, exercise their right to inspect documents (subject to restrictions). In the consistently held opinion of the Authority[22], the right to access data of public interest, as a constitutional right, is broader than the right to inspect documents of which has an administrative procedural nature. The fact itself that the data requested to be accessed are used in a public procurement procedure or are generated in the course does not deprive them of their character as data of public interest, moreover precisely in this way these data will become data of public interest. In the case of procurement procedures closed by a decision, as a general rule, the documents shall be accessible (including, for example, the full winning tender, with the exception of trade secrets, or the data of not winning tenders that are necessary for comparison).

Following the conclusion of a defense and security procurement procedure, in addition to the general rules of the Privacy Act, the special provisions of the separate law must be applied to the accessibility of the data of defense procurements. In the interests of ensuring the transparency of managing public funds, trade secrets do not necessarily constitute a barrier to accessibility in this area, but the law provides a limited opportunity to qualify protected knowledge (such as technological processes, know-how, business strategies, etc.) that is important for management efficiency, as secrets. The rightful financial, economic or market interest of economic operators may override the public interest linked to accessing the data, but this must always be decided on an individual basis, after careful consideration.

IV.9. Data underlying a decision

According to the resolution of NAIH (NAIH/2019/1824), the data controller lawfully refused to fulfil the request to access data of public interest when a complainant asked the Hungarian National Police Headquarters what police movements had taken place due to the demonstrations since 12th December 2018. The data requester asked, on a daily basis, from which towns police officers were assigned to Budapest, how many police officers were assigned, broken down by

22 See NAIH Report 2018, page 113

towns. Furthermore, the data requester asked how many police officers in total participated in the law enforcement operations and what “rank” they had.

Two previous judgments of the Metropolitan Court shall be taken into consideration in this case:
- ‘The specific headcount data of each police unit, the size and type of technical equipment available, and the knowledge of the names used in police radio broadcasting contain facts and circumstances that may indeed be suitable for preparing a subsequent decision.’ Furthermore ‘the aggregate statement of assets, the statement of the costs of the additional tasks incurred in connection with the mass demonstration, […] the event log shall contain data, the knowledge of which may be suitable for jeopardising the lawful functioning of the organ performing its tasks and competences without any undue external influence. (19.P24/882/2009/14)
- ‘In the case of data relating to the exact headcount of units involved in the operation, different police call numbers and the description of the technical means associated with each unit, a reference to these data as decision-preparing data is justified’. Furthermore, in other similar cases, an indication of the stuff number of the police securing the facility and event, as well as what technical means can be attached to the units may indeed be suitable to facilitate the preparation of a decision or to ensure lawful functioning and performance of the tasks and competences of the organ without any undue external influence. (19.P.24.246/2010/9)

In another case, a civil society organisation contacted the Ministry of Human Resources (EMMI) and requested to receive the ministerial response given to the recommendation of the Commissioner for Fundamental Rights in his inquiry into homelessness in particularly dangerous weather conditions („Red Code”). According to EMMI, this ministerial response letter is not considered to be of public interest and therefore, it shall not be subject of a request for data of public interest. In the course of the investigation, EMMI also claimed that the document contained data underlying a decision and, as the data requester requested the full document to be made accessible, it was not possible to fulfil the data request.

In a further request to substantiate the quality of the decision-preparing data, the EMMI explained that, in their view, according to Act CXI of 2011 on the Commissioner for Fundamental Rights, the response of the investigated authority to the Ombudsman’s recommendations is not considered to be data of public interest until the Commissioner for Fundamental Rights provides information on the cessation of the fundamental rights violation revealed in his report. Prior to this, we can only talk about intermediate working materials, which in this case

are related to the material of a draft legislation still in preparatory stage related to homelessness care. Therefore, knowing the position of the Ministry would endanger the free expression of the standpoint of the preparers of the draft legislation during the preparatory work of subsequent decisions.

In its resolution, the Authority referred to the fact that the Commissioner for Fundamental Rights promotes and protects human rights by carrying out social consciousness and awareness-raising activities and by cooperating with organizations and national institutions aimed at promoting the protection of fundamental rights. The Commissioner for Fundamental Rights shall prepare a public report on his inquiries, setting out the findings of fact, and conclusions drawn therefrom. The published report may not contain personal data, classified data, secrets protected by law and secrets related to the exercise of a profession. Information on the action taken related to the public report as well as any other responses to the report are also public, data of public interest accessible to anyone. Furthermore, the letter from the Secretary of State for Social Affairs and Social Inclusion of the EMMI, obtained during the investigation procedure, did not contain any facts / data the disclosure of which would have jeopardised the lawful functioning of EMMI or the performance of its tasks and competences without any undue external influence, such as in particular, the free expression of the standpoint of the organ which generated the data during the preliminary stages of its decision-making process. However, it contained findings that would be of widespread interest in the protection of the homeless. At the request of the NAIH, the EMMI informed the Authority that they provided the data requester with the requested ministerial response which was given to the recommendations of the Commissioner for Fundamental Rights made in its report No. AJB-809/2018. (NAIH/2019/1626)

IV.10. TAO supports (corporate tax allowance)

The Authority received several submissions concerning the area of statutory benefits (TAO supports) in accordance with Section 22/C of Act LXXXI of 1996 on corporate tax and dividend tax (hereinafter: TAO Act). TAO supports - as „diverted" tax revenue - are public funds and the data relating to their management are considered to be data of public interest [Article 39 (2) of the Fundamental Law; Curia decision Pfv.IV.21.175/2017/14; Curia decision Pfv.IV.21.135/2017/10.].

Pursuant to the legal provisions, business organizations providing TAO support do not pay a certain part of their corporate tax to the budget, thus the state waives tax revenue and indirectly redirects it under the control of the state or sports associations, in order to finance the goals set by the state. Data related to the use of TAO support refer to public funds, even if these amounts are not actually entered in the budget but are "diverted" in the direction set by the state. The public fund nature of TAO support is also confirmed by Paragraphs 20, 58, 65 and 82 of Commission Decision C (2011) 7287, which is mandatory under Article 288 of TFEU. Furthermore, the nature of the support is confirmed by the fact that if the supported organisation does not use the support or does not use it for the purpose for which the tax allowance is provided, it must be repaid not to the sponsor but to the state, pursuant to Section 14 (2) of the Government Decree 107/2011 (VI.30.).

In its judgment No. Pfv. IV. 21.175/2017, the Curia stated that the amendment of Act XCII of 2003 on the Rules of Taxation (hereinafter: Taxation Act), which entered into force on 24 October 2016, is not applicable to data generated before it, with regard to the constitutional principle of the prohibition of retroactive legislation. Accordingly, the reference to tax secrecy as a restriction to publicity cannot be accepted. According to the judgment of the Curia, the amount of support offered to a given beneficiary during this period is, specifically item by item, accessible. In the case of data generated after the amendment, pursuant to the Taxation Act currently in effect, both the taxpayer offering the support and the beneficiary may restrict access to the data by reference to tax secrecy. (On the 1st January 2018, Act CL of 2017 on the Order of Taxation entered into force, which contains the rules of tax secrecy in accordance with the above). However, the Authority urges that a legitimate interest test should be carried out in all cases, in a documentable manner, in order to prevent possible disputes. A detailed justification shall be provided as to whether, in the specific case, there is a greater public interest in the transparency of the use of public funds or in the confidentiality of data that may be considered tax secrets. Furthermore, the aspects on the basis of which the release of data would harm the business interests and privacy of the taxpayer or the beneficiary must be taken into account. The Authority draws the attention of data controllers to the fact that pursuant to Section 31 (2) of the Privacy Act, the data controller must prove the lawfulness of the refusal and the reasons for the refusal. It should be emphasized that the Taxation Act, in legal relationships under tax law, defines data as tax secrets in connection with the process of 'offering' support. If the access to data in the public interest is requested not for the purpose of obtaining data related to the taxpayers offering

the support, but related to the use of the support, the request cannot be lawfully rejected by referring to tax secrecy.

IV.11. Football academies

In one case of the Authority, the applicant complained that the Hungarian Football Federation (MLSZ) and the Investment, Technical Development, Sports Management and Public Procurement Ltd. (BMSK Ltd.) had violated his right to access data of public interest and data accessible on public interest grounds by failing to provide the sub-reports, to the submission of which the clubs concerned are obligated according to the grant agreements concluded for the development of the football or sports academies concerned. The MLSZ, as a national sports association performing tasks specified by law and exercising special rights, as well as BMSK, are considered to be bodies performing public duties, so the data processed and generated in connection with their activities are generally data of public interest and data accessible on public interest grounds.

The sports clubs concerned, as beneficiaries, have (partial) reporting obligations and are accountable to the MLSZ as a supporter, but the (partial) reports and accounts are received, controlled and kept by BMSK Zrt. on behalf of the MLSZ. Thus, MLSZ qualifies as a data controller, and BMSK Zrt. qualifies as a data processor mandated and managed by MLSZ.

As a result of the investigation, the Authority found that the MLSZ had violated the data applicant's right to access data of public interest and data accessible in public interest grounds and requested the MLSZ to send the documents that are the subject of the data request to the data requester. Following the request of the Authority, the MLSZ made available (provided) all the accounting documents submitted to BMSK Zrt. with regard to four academies. However, with regard to the other five academies, MLSZ informed the Authority that it did not possess a closed, publishable partial report, as the audit of the partial reports was still ongoing, or the beneficiary did not submit the report or remedied its deficiencies despite the (repeated) notifications of BMSK Zrt. The investigation and assessment of this omission, however, does not fall within the scope of duties and competence of the Authority. (NAIH/2019/1111)

In another case, the applicant objected to EMMI's rejection of a request to provide a copy of a football academy's investment concept („the requested data underlies future decisions"). However, in the opinion of the Authority, the invest-

ment concept approved by the Government is not affected by these subsequent decisions, consequently the investment concept is not a data underlying a future decision, therefore the disclosure of this data of public interest cannot be restricted based on the Privacy Act. EMMI could have relied on the basis of the decision-making process only until the investment concept was completed, given that the final, approved form of the concept was the decision itself. The fact that the implementation of the investment is in progress after the approval of the concept, shall no longer restrict the disclosure of the data, unless the success of the implementation would be jeopardized by the release of the data. However, no circumstance to that effect has been revealed during the examination of the request for data. (NAIH/2019/4445)

IV.12. Prison regulations

According to Act CXXX of 2010 on Legislation, the Director General of the Hungarian Prison Service Headquarters (BVOP) may regulate the organization, operation and activities of the bodies under its management, direction or supervision in a normative instruction, and these regulations shall be published, except for those containing classified data. In respect of this, the BVOP instructions are, as a general rule, available to anyone, and detainees are also entitled to know them. As their right to electronic administration is suspended during the execution of a custodial sentence, the detainees may also file a request for access to the BVOP instruction with the institution of the place of detention, or request from their contact person or legal representative to print and hand over the regulation.

By contrast, special instructions, circulars, and other internal regulations are regulatory tools of management tasks addressed to the staff of the organization, which can be issued for general, technical issues of the day-to-day activities of penitentiary institutions, if not regulated by law or public regulatory instrument and the issuance of a public regulatory instrument is not mandatory. All BVOP instructions (except those containing classified information) are available in various legislation database and on the website of the Hungarian Prison Service. Special instructions, circulars and other internal regulatory instruments are not considered to be public regulatory instruments thus, their publication is not obligatory. Accordingly, the BVOP is entitled to decide whether it wishes to publish them. As the publication of BVOP special instructions may pose a security risk to the operation of the prison service, in order to prevent large numbers of pro-

hibited objects from entering and to prevent corruption offenses, the BVOP has decided to strengthen its security measures in all areas, to review the special instructions already published and if necessary, amend and no longer publish its special instructions. (NAIH/2019/4389)

IV.13. Environmental information

According to its importance, the Authority treats environmental information as "privileged" data of public interest, as without access to environmental information, citizens cannot properly exercise their rights to a healthy environment enshrined in the Fundamental Law. It is therefore important to emphasize that pursuant to Act LIII of 1995 on the General Rules of Environmental Protection (Environmental Protection Act), data related to environmental impact, environmental hazard and environmental endangerment must be provided not only by organizations performing public duties or managing public funds, but also by all organizations and companies.

In 2019, the Authority examined a number of cases related to environmental information where it was necessary to draw the attention of organs performing public duties to broadest possible interpretation of the concept of environmental information, as supported by the Implementation Guide to the Aarhus Convention (promulgated by Act LXXXI of 2001), as well as the case law of the Convention Compliance Committee and the European Court of Justice.

In one case, the request to access noise measurement data was not fulfilled because the data had not yet been evaluated. It is possible that the evaluation and validation of the raw data leads to a different result from the original data, but the raw data is also environmental information[23], and when disclosing such data, the data requester shall be informed about the lack of processing. (NAIH/2019/5627)

In another case, the local government did not make the air pollution test report ordered from the National Meteorological Service available to local government representatives because 'no far-reaching conclusions can be drawn from its findings'. The protocol stated that 'the concentration of the highly carcinogenic benzo (a) pyrene exceeds the daily limit value for 4 days, reaching almost four times that on the most polluted day. […] However, it is necessary to take into account

23 See the findings of the Aarhus Convention Compliance Committee on communications ACCC/C/2010/53

the fact that far-reaching conclusions should not be drawn from such a short measurement program, a reliable determination of the sources of pollution would require long-term measurement, possibly testing of additional components.' The Authority emphasized that the data being able to draw conclusions from is not a requirement for the disclosure of data. (NAIH/2019/7779)

In cases where the controller is vested with discretionary powers, significant weight must be given to the public interest in disclosure of environmental information. We drew the attention of the local government of a city with county rights to this factor, when it did not want to publish a feasibility study and cost-benefit analysis containing environmental data. The feasibility study was prepared in connection with the invitation to tender of the Integrated Transport Development Operational Program 'Development of Sustainable Urban Transport and Improvement of Suburban Rail Access in Less Developed Regions' and clearly included environmental information, because measures and programs related to the environment, as well as activities and cost-effectiveness and other economic analyzes that are likely to have an impact on environmental elements and environmental impact, are also considered as such pursuant to Section 2 (e) of Government Decree 311/2005 (XII.25.) on the Rules of Public Access to Environmental Information.

A project that will determine the development of a city's public transport for decades will have a significant impact on the environment of the people living in the city, the air quality and the level of noise. Important environmental information is whether environmental values are properly "priced in" and how the costs of environmental impact are incorporated into the cost-benefit analyses used to make decisions that affect the environment. Thus, the publicity of cost-benefit analyses and feasibility studies ensures the transparency of whether environmental costs and values have been taken into account when deciding on a project. In addition, the feasibility study contains a number of emission data, the disclosure of which is subject to even stricter rules than the general rules applicable to environmental information, prevailing over the interests of the protection of personal data, business secrets and tax secrets. (NAIH/2019/1016)

In another case related to emission values, a civil organisation of local residents requested access to an acoustic expert reports commissioned by a Budapest district mayor's office. The mayor's office rejected the data request, arguing that according to the clauses of the acoustic expert report they 'constitute a business secret and intellectual property', and they are subject to copyright, thus the publication of expert reports is subject to the consent of the authors. The

Environmental Protection Act classifies the establishment of local noise protection rules among the environmental protection tasks of local governments, in the capital the district representative body may issue a decree on the establishment of local noise protection rules. The mayor's office is obliged to analyse, assess the state of the environment in its area of competence and inform the public about it at least once a year. The office commissioned the preparation of acoustic expert reports, the purpose of the investigation was to examine the noise level in the streets of the district and to propose a plan of action to reduce noise. Based on the above, the acoustic expert reports are data of public interest, as they are processed by a body performing public duties, they were generated in connection with the performance of the public duties of this body and the expert reports were paid from public funds. Acoustic expert reports are considered to be data of public interest not only under the Privacy Act, but also according to the Environmental Protection Act. Section 12 (2) of the Environmental Protection Act states that 'everyone has the right to have access to environmental information considered as data of public interest in accordance with specific legislation'. Section 2 (b) of Government Decree 311/2005 (XII. 25.) classifies information related to 'environmental impact, including the direct or indirect release of noise into the environment' as environmental information.

With regard to the copyright restriction, it should be noted that Act LXXVI of 1999 on Copyright does not restrict the right of access to works protected by copyright as data of public interest; Section 15/A. of the Act only allows for stricter procedural rules than those contained in the Privacy Act: 'In order to protect the author's personal rights, the body performing public duties shall be empowered to comply with any request for access to works protected by copyright as data of public interest or data accessible on public interest grounds, by allowing access - inside the time limit prescribed for compliance with the request - to review sections of the work that contain the data of public interest or data accessible on public interest grounds, instead of the form and means desired by the requesting party.

On the basis of the above, the Authority established that the controller violated the applicant's right of access to data of public interest by not giving access to the parts of the acoustic expert report requested by the applicant concerning the measurement results and noise maps. Following the notification of the Authority, the mayor's office fulfilled the data request. (NAIH/2019/2549)

The concept of "party" was the subject of the case, in which the complainant requested access to a decision on a final authorisation by the Environmental

Protection Agency and to an opinion from a national park directorate on the decision (hereinafter: NP opinion) from a government office. The reason for the rejection of the data request was that the data requester does not qualify as a 'party' pursuant to Section 10 (1) of Act CL of 2016 on General Administrative Procedure. In its decisions, the Authority explained that the Administrative Procedure Act does not contain a restrictive provision on the disclosure of a specific set of data of public interest. The right to inspect documents specified in Section 33 of the Administrative Procedure Act shall not be confused with the right of access to data of public interest, as the restriction formulated therein does not apply to data of public interest. The publicity of the final decisions - the legal basis of which is stated in the Privacy Act – is, however, also highlighted in Section 33 (5) of the Administrative Procedure Act. Furthermore, the authorisation by the Environmental Protection Agency and the NP opinion contain environmental information.

In its judgment in Case C-321/96 (Mecklenburg judgment), the European Court of Justice stated that any act which adversely affects or protects the situation of an environmental sector, is considered as environmental information. It is not necessary for this act to be a decision closing the procedure. Accordingly, the (intermediate) decision of the the Environmental Protection Agency is environmental information, provided that it affects the decision approving the construction plans. The public interest in the publicity of an authorisation by the Environmental Protection Agency for a specially protected natural area and the opinion of the national park taking into account the values of the area, as well as in the transparency of the procedure is paramount, therefore the Authority repeatedly ordered the government office to comply with the data request. (NAIH/2019/78)

It is important to note that a wide range of environmental information is handled by several bodies, making it difficult for citizens to find out which environmental information they can request from where. Therefore, bodies holding environmental information are particularly expected to fulfil their obligation of publication, with special regard to the publication of the list of environmental information [see Section 12 (3) of the Environmental Protection Act and Section 3 f) and Section 4 of Government Decree 311/2005 (XII. 25.)]. In the case of the air pollution test report described earlier, the Authority also ordered the local government to fulfil its obligations regarding the publication of environmental information. The local government complied with the Authority's request and published the list of environmental information, as well as uploaded the air pollution investigation report to its website.

IV.14. Publicity of the media and the Internet

According to the Organizational and Operational Rules of the Authority, the FOI Department is responsible for handling data protection cases where, in addition to the right to the protection of personal data, there are other fundamental rights related to the publicity of data (in particular fundamental rights related to the publicity of data of public interest or data accessible on public interest grounds as well as to freedom of the press and freedom of expression) co-existing or conflicting with each other. In 2019, the Authority issued reprimands to the data controller in two cases (without imposing a fine) in data protection authority procedure, in two cases the procedure was terminated and the other cases are still pending. Typically, online publicity (i.e. social media) is the scene of alleged violations. In this connection, the Authority would like to draw the attention to the fact that it is recommended to report the disputed content, pages, groups and profiles to the data controller (Facebook) in the first instance, furthermore, their deletion can also be requested here[24].

In one of its decision , the Authority found that the mayor's report on decisions taken in a closed session of the body of the representatives was unlawfully published on the website of the mayor's office of a large municipality in such a way that the personal data of a former employee in a labour lawsuit with the municipality were not obscured. Furthermore, the data subject's request for erasure was rejected on the grounds that the decision of the body of representatives taken in a closed session was public, and accordingly the mayor lawfully provided objective information on the decision of the closed session as a mandatory agenda item. In the present case, it had to be considered whether the legal proceedings initiated due to the termination of the employment of a civil servant are directly related to the activities and operation of the local government. The mere fact that the mayor's office, as an organ performing public duties, is involved in a labour lawsuit with a former civil servant shall be considered data of public interest related to the office. Thus, the fact of a labour lawsuit may be disclosed without disclosing the identity of the former civil servant. Accordingly, the personal data of the data subject must be made unrecognisable, as suggested in the NAIH guide on the local governments referred to earlier.

24 Information on when and how to report something on the social network can be found in the FB Help Center by using „Rules and Reports" link, „Report Abuse" menu point, which can be accessed without registering or logging in.

In its other decision[25], the Authority issued reprimands to the individuals who posted on Facebook a court judgment and a decision of the prosecution containing personal data of the complainants. Regarding the restriction of the visibility of the posts (to friends), the Authority noted that in this case the data processing cannot be considered as purely personal or household activity, as the files were not uploaded by the data subjects themselves, furthermore the data controllers have more than 1000 friends on the community site, who thus all had access to the documents. (NAIH/2019/69)

However, in another case, a municipality notary approached the Authority with the question of whether a court judgment involving the local government could be shared by the plaintiff on the Facebook community site. To ensure the publicity of court decisions, Act CLXI of 2011 on the organization and administration of the courts provides for the tasks related to the Register of Court Decisions, including the scope of decisions to be published, the procedural rules for publication and the protection of personal data. Section 166 (2) of this Act specifies that, unless otherwise provided for by law, in the decision published in the Register of Court Decisions it is not necessary to erase the following data:

a) the surname and forename or forenames (hereinafter referred to collectively as “name”) and position of a person performing governmental or local governmental tasks, or other public duties specified by law, if that person was participating in the proceedings in connection with performing his public duties, unless otherwise provided by law,
b) name of the attorney or bar association legal counsel acting as an agent, and the name of the defence counsel,
c) name of the natural person, who has been unsuccessful as a defendant, and the name and registered office of the legal person or entity without legal personality if the decision was adopted in a case in which a claim in the public interest can be enforced in accordance with the relevant legislation,
d) name and address of the association or foundation, and the name of its representative,
e) data accessible on public interest grounds.

25 https://www.naih.hu/files/NAIH_2019_3114_hatarozat.pdf .

The court judgment in the proceedings in question (initiated for unlawful termination of employment) contained the name and address of the plaintiff, the name, registered office of the law firm representing the plaintiff and the name of its lawyer, the name and registered office of the defendant (local government) and of the representative lawyer of the defendant as well as the name of the mayor of the municipality. With the exception of the data of the plaintiff, which was not obscured by its own decision, the data to be published are considered to be data of public interest and data accessible on public interest grounds pursuant to the Privacy Act, which data should not have been erased according to Act CLXI of 2011 even if the judgment had been published in the Register of Court Decisions. In view of the above, the Authority found that, from a data protection point of view, the publication of the judgment by the applicant cannot be objected to. (NAIH/2019/2631)

IV.15. Search engines

Complaints about the rejection of requests to be removed from the Google Search results list are not subject to the one-stop-shop mechanism introduced by the GDPR, i.e. in such cases not the Irish data protection authority (as the supervisory authority of the main European establishment of Google) is competent to act, but the national data protection authority to which the complaint has been lodged.

The GDPR also provides for exceptions to the 'right to be forgotten':

- if the processing is necessary for exercising the right of freedom of expression and information (freedom of information in the broadest sense)
- the public interest justifies the need for data processing
- there are private interests to be protected (i.e. the data processing is necessary for the establishment, exercise or defence of legal claims)

In 2019, the Authority also received a number of submissions in which complainants objected that Google had not deleted certain URLs from Google Search results despite their request.

In several cases, Google accepted the authority's argument that there was in fact no public interest against the data subject's right to erasure. The Authority also received a complaint in which the data subject complained that his name

had been linked to a political party. Thus, he did not in fact seek to remove the indicated URL, but merely to have Google remove the expression linked to his name from the search engine. The Authority found that the removal of the link between the name of the data subject and the contested expression did not affected Google's interests and did not restrict either the freedom of expression or the public's right to information. At the Authority's request, Google deleted the expression linked to the complainant's name from the search engine. (NAIH/2019/7821)

Several data subjects, whose data are listed in the business register, complained that by entering their name in the google.com internet search engine, their name, mother's name and address will be also available in the search results list. In the case, the Authority addressed a recommendation to the Minister of Justice to review the rules on access, dissemination and searchability of personal data accessible on public interest grounds, processed in the business register. In particular, access to Internet search engines and the enforcement of the principle of data minimisation is required at a level, which can proportionately ensure the original objectives of the business register, i.e. transparency and fairness of business, so that direct access to company data, including personal data, is differentiated, taking into account the requirements of necessity and proportionality. In 2019, the Ministry of Justice addressed the revision of the disclosure requirements for company information, however, the legislative changes described by the press, which would have made access to data contained in the company register subject to registration and payment of fees, were not realized. Thus, the Decree of the Ministry of Justice[26] complained of in the recommendation was not amended contrary to preliminary plans.

IV.16. Identity of the data requester

The Authority has received several submissions for consultation aimed at clarifying the identity of the data requester:
'Can an organ performing public duties be required to provide data on the basis of a request from which the identity of the applicant cannot be identified?

26 Pursuant to Section 5 (3) of the IRM Decree 47/2007 (X. 20.) on free company information:
(3) The data referred to in paragraph 1 may also be accessed by means of Internet-based search engines. In this case, it is not necessary to use a name and password to access the data.

Which data is the minimum necessary to clearly identify an applicant?
Given that applicants never indicate the purpose of their request or their subsequent use of data, is the applicant required by law to indicate any purpose in his request?‘

The basic requirement of the Privacy Act, arising from the Fundamental Law, is that “anyone” may submit a request for access to data of public interest or data accessible on public interest grounds, without having an obligation to tell and / or justify his or her identity (or even in other respects). The category of anyone includes all natural and legal persons, or entities without legal personality. However, when an individual request for access to data is received by the organ via mail, and without any identifying information, the data request may not be fulfilled. The circumstances of each request for data must be examined on a case-by-case basis and, if the request can be fulfilled in another way, even by electronic means, that way shall be chosen. In summary, the data controller is not entitled to verify identity and cannot request a statement on either the purpose of the data request or on the motivation of the requester.

V. Activities of the Authority Related to Legislation

V.1. Statistics on Legislation-related Activities

The Number of Legislation-related Cases by Year and Legal Source			
Legal Source/Year	**2017**	**2018**	**2019**
Law	82	72	61
Government decree	89	47	49
Ministerial decree	94	55	41
Government decision	33	40	34
Others (parliamentary decision, instruction etc.)	23	17	29
Total	**321**	**231**	**214**

In 2019, the trend observed for several years, i.e. the decrease in the number of draft legal proposals and legislation to be commented by the Authority, continued. The reason for this is unknown, however, the role of the following factors can be assumed:

1. Previous experience shows that, national legislation activity is moderate in those years when parliamentary or local government elections are held.

2. The GDPR narrows the scope of Member States' legislation on data processing compared to the previous situation, as under Article 6 (2) Member States may maintain or introduce more specific provisions to adapt the application of the rules of the GDPR with regard to data processing rules if the data processing is necessary for compliance with a legal obligation who which the controller is subject, or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. Compliance with this rule still required national legislation in 2018, as legal standards, that fell outside the regulatory framework of the Member States as defined by the GDPR, had to be repealed. Following the deregulation and the completion of the adaption of Hungarian law to the GDPR, in the future it can be expected that, as the GDPR does not allow for national legislation in relation to certain legal bases of data processing, less legislation will be enacted in these areas in the future.

3. The Authority also considered the possibility that the number of draft legal proposals to be commented on may be reduced due to the failure of the ministries preparing the draft legislation to involve the Authority in the coordination of drafts related to the protection of personal data and the publicity of data of public interest. However, random checks showed that the situation did not deteriorate in this respect compared to previous years.

In 2019, the number of comments on draft legal proposals sent to be commented on in relation to the total number of cases did not change significantly compared to the previous years. The proportion of comments on freedom of information has increased, but overall, the number of comments related to data protection remains dominant.

Comment subject matter	**Észrevételek száma**		
	2017	**2018**	**2019**
Data protection	461	487	323
Freedom of information	28	22	39
Other	92	79	78
Total	**581**	**588**	**440**

V.2. Experience gained during the public consultation on legislation

This is also surprising because according to Act CXXXI of 2010 on Public Participation in Developing Legislation, during the public consultation, it must be ensured that the widest possible range of opinions is reflected in the opinion forming process, especially with regard to the opinions of disadvantaged, socially and economically marginalized groups. During the preparation of legislation, it is necessary to ensure the transparency of consultations and their fullest possible publicity. The general form of consultation on draft legislation is submitting opinion through the contact details provided on the website. Pursuant to Section 5 of the Act, in the case of draft legislation to be submitted for public consultation, a general consultation is always mandatory. During the general consultation, the draft and concept submitted for public consultation as well as the summary of the preliminary impact assessment specified in Act CXXX of 2010 on Legislation shall be published on the website together with the draft. The draft should be published at the same time as it is submitted to the governmental bodies for con-

sultation, so that sufficient time is available for a substantive assessment of the draft and the expression of opinions. Published drafts cannot be removed from the website for one year from the date of publication. There have been cases in the past, albeit infrequently, where a draft has not been published or has been delayed due to a misinterpretation of the law or an administrative error. However, in 2019 we were faced with the fact that the publication of the drafts on the Government's website had almost completely ceased.

The disruption in the application of the disclosure rules set out in the Act on Public Participation in Developing Legislation should not be disregarded because the submission of draft legislation for public consultation is not some kind of grace or convenience on the part of the state but, as stated in the preamble of the above-mentioned Act, by involving the widest possible sections of society in the preparation of legislation, they help to provide a comprehensive basis for legislation in the public interest, thereby improving the quality and enforceability of legislation, which together are essential conditions for a good state. The Minister of Justice who submitted the draft of the above-mentioned Act to the Parliament, aptly summed up this idea in the general explanatory memorandum to the Draft Act No. T/1382., saying that 'the opinion of the people is not an obstacle but the solution itself'.

According to the Authority's unchanged position, the content of draft legislation is data of public interest which has an overriding public interest in its disclosure. In its Decision 32/1992. (V. 29.) AB, the Constitutional Court stated that free access to information of public interest is a constitutional guarantee of the controllability of the activities of bodies exercising public power. Publicity is a test of the democratic functioning of public power. Thus, access to data of public interest also means the guarantee of public power and the transparency of the management of public affairs as a fundamental democratic institution. The publicity of and access to data of public interest is therefore a fundamental constitutional guarantee of the democratic rule of law. The reasoning of decision 34/1994. (VI. 24.) AB stated that freedom of information, publicity of the exercise of public power, as well as transparency and controllability of the activities of the state and the executive power are conditions for the right to criticism, freedom of criticism and free expression. This fundamental right, in the context of the assessment of constitutional constraints, therefore enjoys at least as much constitutional protection as the right to freedom of expression. Open, transparent and verifiable exercise of public authority, usually the functioning of state bodies and the executive in public, are one of the cornerstones of democracy, and a guarantee of the rule of law. Without the test of the public, the state becomes "alienated from the citi-

zens", as well as its operation becomes unpredictable, incalculable, especially dangerous, because the opacity of the operation of the state poses an increased threat to constitutional freedoms.

During the administrative consultation on draft legislation, using the means available, the Authority notifies the ministry responsible for consultation if the publication of the given draft legislation has not been published, furthermore the Authority publishes its resolutions on the draft legislation on its website (https://naih.hu) on a monthly basis.

V.3. Legislative changes related to the Data Protection Reform of the European Union

Although most of the sectoral legislative amendments related to the application of the GDPR as well as the harmonization of the Privacy Act with the Police Directive took place in 2018, but some of the necessary corrections were postponed to 2019. In connection with the current year, the following should be highlighted:

1. The proposal to amend individual laws in the context of the data protection reform of the European Union brought together a number of legislative amendments into a large "Reform Act" package, which by its nature raised a number of legal issues and problems, the negotiation of which had already begun earlier and continued in 2019. The Authority maintained, inter alia, its previous comment related to Act CXIX of 1995 on the processing of name and address data for research and direct marketing purposes. According to this comment, in view of the GDPR becoming applicable, a substantive revision and deregulation of the Act is necessary, taking into account that the legal basis for direct marketing in the GDPR system is typically Article 6 (1) (f). However, the legislature of the Member State does not have the power to regulate the conditions of the data processing in relation to such data processing relations.

The Authority recommended to consider the repeal of the Act by adding, that the rules related to the provision of data could be incorporated into Act LXVI of 1992 on the Registration of Personal Data and Addresses of Citizens.

In the above-mentioned "Reform Act", in connection with Act LXVIII of 1997 on the employment of judicial staff, the opinion of the Authority pointed out that in

case of mandatory data processing the legal basis of the data processing cannot be the consent of the data subject. (NAIH/2019/835)

2. On the basis of a notification, the Authority examined the rules on the processing of personal data of Act CXXII of 2013 on certain provisions and transitional rules related to transactions in agricultural and forestry land, following which the Authority approached the Minister of Agriculture, initiating the correction of the Act. In its resolution the Authority indicated that the above-mentioned Act did not define the purpose of the processing of personal data with sufficient precision. Furthermore, it pointed out that, in view of the regulatory requirements arising from the GDPR, the registration of data could only be required as mandatory data processing, but the codification solution in the normative text, i.e. that the data controller is „entitled to process" the personal data, should be avoided. Thus, the data controller is not and cannot be in a decision-making position regarding the processing of data, but it shall be prescribed by law with regard to the necessary scope of data, and the data processing body may not deviate from this. Therefore, the Authority recommended that instead of the challenged regulatory construction, an exhaustive list of the types of data to be mandatory processed should be included in the law. (NAIH/2019/2067)

3. In commenting on the draft Act on entitlements to social security benefits and on funding these benefits, it was necessary to clarify, among other things, the legal possibilities of regulating the rights of data subjects in a sectoral law. In this respect, the Authority drew attention to the fact that the GDPR rules guaranteeing the data subject's right to access are neither necessary nor possible to repeat in the Member States' data processing law, without prejudice to EU law. Furthermore, the resolution stated that the law providing for mandatory data processing should avoid formulating the rules on the registration and transmission of data in a conditional manner (e.g. 'may process', 'may transmit'). Instead, the tasks and obligations related to mandatory data processing should be regulated in the law. (NAIH/2019/74800)

4. Several mail-order companies have applied to the Authority for information in connection with the provisions of Section 17 (2) of Government Decree 210/2009 (IX. 29.) on the Conditions for Conducting Trading Activities. That provision provided for the following: 'Where a mail order operator is required to seek admission into the register of data processing operations pursuant to the Act on the Right of Informational Self-Determination and on Freedom of Information, the mail order operator shall indicate in the catalogues and other brochures of products his register number for data processing operations in addition to the

information requirements prescribed by specific other legislation.' The quoted norm text contained an anachronistic rule, as the rules on data protection register have been deregulated in connection with the EU data protection reform. Although the cited legal norm no longer created any obligation to provide data due to the termination of the data protection register and the obligation to register in it, the Authority initiated the repeal of the redundant rule in order to provide a reassuring solution to the legal situation for mail-order providers as well. (NAIH/2019/5137)

V.4. Big data controllers and data processing systems

1. The State Secretary for Administration of the Ministry of Interior requested a resolution from the Authority on the draft legislation, according to which, in the framework of catching up with economically and otherwise underdeveloped areas, in order to improve public safety, legal possibilities would be created for the installation of surveillance cameras in such areas without local public surveillance, where the installation of surveillance system is not possible within the current legal framework. In such areas, it is planned that the notary would be responsible for data processing related to the visual surveillance system.

In its opinion on the case, the Authority agreed that the operation of public image surveillance systems can contribute to crime prevention and law enforcement even if the surveillance of camera images is not continuous, but the recordings are used only afterwards if, in connection with a criminal offense, the investigating authority requests data from the image streams of the municipal image surveillance system available for a period of thirty days. It can be assumed that it has a dissuasive effect on potential offenders if they become aware of this possibility. At the same time, the Authority indicated that the operation of image surveillance systems and the use of data shall be regulated at the legal source level of an Act, as the mandatory processing of personal data cannot be prescribed by a local government decree. The Ministry of Interior has accordingly prepared the necessary amendment to the law. (NAIH/2019/6074)

2. The functioning of modern information societies is highly dependent on the availability and proper functioning of information communication infrastructures, IT systems and services. Therefore, the need to maintain cyber security arises as a fundamental sovereignty and national security issue in developed states. Strengthening cyber protection also contributes to the protection of personal

data by strengthening data security, which is why the Authority agreed to the establishment of the Civil Information and Cyber Security Center, which was envisaged in a government proposal submitted in 2019.

The information security and defense of the state and the country are matters of national security interest, and the national security services must have sophisticated IT capabilities that are also required for cyber defense. Therefore, in general, it is not objectionable for a central cyber defense institution to be established within the organizational system of national security services. At the same time, this type of organizational development also raises sensitive issues that are worth further consideration. For example, the question may arise if a national security service receives access to all important Hungarian state and possibly large-scale IT systems as well as the data stored in them in order to perform its cyber defense tasks, what is the guarantee that this will not lead to a situation in the long term, that the National Security Service uses the access obtained for cyber defense to establish a comprehensive covert surveillance infrastructure. Within a legal framework, and with the application of appropriate data protection guarantees, gathering of intelligence for national security and law enforcement purposes can, of course, also be carried out lawfully in a democratic state governed by the rule of law. However, the increase in the amount of data sources and data available for this purpose, as well as the automation of data processing and use, may over time lead to risks related to the protection of personal data and the democratic rule of law, which the current legal guarantee system may not be sufficient to address. It is therefore important that cyber defense activities are carried out separately from other national security tasks and are monitored by appropriate independent external control.

During the definition of the future role of Hungarian cyber defense and the planning of its possible activities, it was also considered that not only defensive cyber operations could take place, but also offensive ones, primarily in order to prevent cyber attacks. In the opinion of the Authority, the fundamental legal framework for cyber-attack operations requires legal regulation. Namely, it should be specified at the legal source level of an Act, in which areas and under what circumstances it is possible to carry out a cyber-attack operation, as well as for what purpose such an operation may be permitted. Consideration should be given to creating rules that limit offensive cyber operations that could result in the influence of, for example, Hungarian state bodies, parties, churches, non-governmental organizations, the press, or the public. The Authority agrees that offensive cyber operations should be included among the assets subject to ex-

ternal licensing in the regulatory framework of the National Security Services Act. (NAIH/2019/2443)

3. The draft Act amending certain laws related to defense issues, submitted for administrative consultation, envisaged the creation of a unified, centralized register of data on potential conscripts, conscripts and trained reserve officers, using many data sources for updating and also kept in peacetime. In this respect, the Authority pointed out that due to the insufficient information available on the need for the proposed regulation, it was not possible to form a reasoned opinion on whether certain elements of the planned data collection were necessary. And if so, what content, detail and frequency of data collection is required; and whether the planned regulation is in line with the declared purpose of the amendment. Subsequently, during the consultation with the replenishment and data protection experts of the Ministry of Defence and the Hungarian Defence Forces, it was established that a possible mobilization would involve short-term tasks for the Hungarian Defence Forces, the implementation of which would require continuous maintenance of the replenishment database, even in peacetime.

The above-mentioned draft Act also concerned the processing of biometric data collected for defence purposes. The collection of these data is regulated in such a way that the data processing is performed by the Military National Security Service (Katonai Nemzetbiztonsági Szolgálat, hereinafter 'the KNBSZ'), but the Defence Forces participate in the recording of the data as data processors.

The tasks of the national security services and the rules of data processing performed by the services are regulated by Act CXXV of 1995 on National Security Services (hereinafter 'the Security Act'). Therefore, the Authority recommended that the tasks of the KNBSZ related to the processing of biometric data regulated in the Act on the Processing of Military Data, be defined in such a way that they are in accordance with the relevant provisions of the Security Act. The amendments proposed by the Authority extend to the legal conditions for the collection of biometric data, the rules for the transfer of biometric data abroad and the period of retention of biometric data. The latter is a neuralgic issue. The Authority maintained its position, already emphasized related to the legislative amendment in 2018, that the 50-year mandatory retention period of biometric data is contrary to the principle of purpose limitation data and clearly requires data collection on a stockpiling basis from the KNBSZ. Therefore, the Authority proposed a differentiated reduction of the mandatory retention period based on, for example, data types, categories of data subjects, and data processing purposes.

The draft Act submitted for comment provided for a procedure for the transfer of classified data abroad, which, according to the Authority, is contrary to the provisions set out in Act CLV of 2009 on the protection of classified data. (During the administrative consultation, the objected part was corrected.) The Privacy Act provides that if the planned processing is of a high risk, prior consultation with the Authority is mandatory. In the case of mandatory data processing, the preliminary consultation is initiated and carried out by the preparer of the legislation prescribing the data processing within the framework of the legal preparatory procedure.

Finally, in its resolution on the draft Act, the Authority indicated to the Ministry of Defence that the amendment to the Act is likely to include rules on high-risk data processing, such as the processing of health data and biometric data. The Privacy Act provides that if the planned processing is of a high risk, prior consultation with the Authority is mandatory. In the case of mandatory data processing, the prior consultation is initiated and carried out by the preparer of the legislation prescribing the data processing within the framework of the legislative preparatory procedure. Although the commented government proposal included sections on 'Risk Management' and 'Data Protection Impacts', its one and a half page length and outline explanation was disproportionate to the volume and complexity of the planned data processing. Therefore, in order to make a well-founded assessment of the data protection impact, the Authority proposed to complement the data protection impact assessment, emphasizing that it is the task and responsibility of the preparer of the draft legislation to carry out the preliminary data protection impact assessment and to initiate consultations with the Authority on this matter in time, in view of the time limit specified by the Privacy Act.

4. The Authority became aware of a plan to use drones as a mobile observation platform (e.g. patrol drone) from a draft government decision on the provision of resources for the acquisition of assets necessary for the expansion of the capabilities of the Counter-Terrorism Center and for the performance of tasks at a higher level. Without disputing the appropriateness of the idea, the Authority pointed out that it certainly goes beyond the taking of video and audio recordings in accordance with Act XXXIV of 1994 on the Police (hereinafter: Police Act). Therefore, the implementation of the planned developments can only take place to the extent that they are permitted by the relevant law in accordance with the requirements of the protection of personal data. The Authority recommended that a preliminary data protection impact assessment of the planned data processing be prepared during the preparation of the legal regulation allowing for new uses of drones. (NAIH/2019/3734)

5. An amendment to the law prepared in 2019 allowed the police to identify the person subject to the measure during identity check on the basis of a facial image, with the aid of machine facial recognition. The aim of the amendments was to reduce the number of arrests involving restrictions of personal freedom, to make personal identification simpler and faster, and to increase the effectiveness of the measure. (According to the justification of the government proposal, IT support for identification can also be used for the identification of corpses of unknown identity.) The identification process is as follows: if the person subject to the identity check cannot prove his or her identity because he or she does not have an identity card, the police officer performing the measure will take a photo of the person subject to the measure with the device equipped with the NOVA. mobil application. Based on the portrait, the application offers five hits from the central biometric portrait profile register, of which the police officer decides on the spot which one matches the person subject to identity check. The application then downloads from the central personal data and address register the data required for identification of the person, selected on the basis of the facial image. Portrait files are temporarily stored on the mobile device and then deleted automatically. The NOVA.mobil application is part of the Robot Cop system used by the Police. A log file is created for each operation performed in the Robot Cop system.

The Authority found that the data processing facilitates the processing of data required for police action. The operation of the application is semi-automatic, i.e. the identification of the person subject to identity check is not done by the software, but by the acting police officer. The need for live labour creates a bottleneck in the process of using data that does not allow for mass data collection. (NAIH/2019/4523)

V.5. Draft legislations on freedom of information

The provision of Act V of 2006 on Public Company Information, Company Registration and Liquidation (hereinafter: Company Act) concerning free access to company information has been amended as of 1 October 2019 so that within the framework of free company information, ten queries per month are allowed, available after pre-registration on the website of the Company Information Service. The Company Act also stipulated that '*free company information may not result in the acquisition of all or a substantial part of the company register*'. According to the explanatory memorandum to the Act, '*in order to prevent the*

misuse of the free company information service available on the Internet, the Company Act requires the identification of the person requesting company information'. In its resolution on the amendment of the Act, the Authority emphasized that the described amendments do not serve the purpose of transparency and protection of property (creditors), furthermore they significantly restrict the access to data by individuals and non-governmental organizations as well as journalists involved in the fight against corruption. The Authority questioned the need for the amendment of the Act, as the proposal for the amendment did not provide specific evidence of the misuse of public company data that made the contested restriction necessary. The Authority also indicated that restricting access to data or making it payable with regard to other company data, such as company accounts, is a significant step backwards from previous provisions providing free access to the general public. (NAIH/2019/8645)

VI. Supervision of Data Classification, Classified Data and Public Data with Limited Publicity

VI.1. IT system facilitating the performance of covert surveillance tasks and arrest warrant

On the basis of a notification, the Authority initiated an investigation on the lawfulness of the data processing by the National Security Service (Nemzetbiztonsági Szakszolgálat, hereinafter: NBSZ) using an IT system facilitating the identification of individuals in accordance with Act LXXXVIII of 2013 on the Warrant Registration System and the Search and Identification of Persons and Things (hereinafter: Warrant Act). The Warrant Act essentially stipulates that the NBSZ is entitled to take over the face image data of the warrant database and if, during the operation of its IT system facilitating the identification of individuals, it detects a hit that facilitates the identification of a wanted person whose data is accessible on public interest grounds and does not interfere with the performance of its duties, the system shall notify the body conducting the warrant procedure of the hit. The legal regulation described above only refers to the IT system of the NBSZ facilitating identification of individuals, but neither the Warrant Act nor any other law clarifies its purpose and the rules of its application. Therefore, the Authority contacted the Director General of the NBSZ to clarify the facts.

According to the reply of the Director General of the NBSZ, the data controller of the facial recognition system is the NBSZ. The basic aim and purpose of the system is to facilitate the service activities of NBSZ specified in Section 8 (1) (a) of Act CXXV of 1995 on National Security Services (hereinafter: Security Act). The system facilitates the identification of persons related to whom the NBSZ carries out surveillance tasks upon the request of bodies authorized to gathering intelligence. In addition, the system set up to facilitate the performance of surveillance tasks may also be used to identify and locate the wanted in accordance with the rules of the Warrant Act. (According to the Warrant Act, there is no independent application of devices.) Beyond facial recognition, the system does not aim to identify data subjects, and the technical solution for this is not part of the system.

The facial reference data required for the operation of the system (facial recognition) may be received from the bodies authorized to use the services of the NBSZ or, in the case of warrant procedure, from the body keeping the warrant register. In order to facilitate the warrant procedure, the NBSZ is entitled to take over data accessible on public interest ground of the warrant register with direct

access. If the NBSZ detects a hit on a wanted person during the operation of the system, it shall notify the body conducting the warrant procedure in order to take further measures.

The system acquires motion picture data at permanent locations as well as using mobile data collection points. The data collection sites, as well as the duration of the data collection are determined by the location data included in the requests of the bodies authorized by the Security Act. The size and location of a given site determines the number of data collection points. The primary consideration in locating data collection points is the full coverage of the approach routes of the given site. The NBSZ decides, on the basis of the time interval specified in the requests and the prior consultation with the contracting authority, whether a permanent deployment or mobile data collection will take place.

In the system, the biometric image reference database is created by algorithmic analysis of the individual characteristics of the facial images attached to the written requests of the bodies authorized by the Security Act, to which the image data from the data collection points are automatically compared during the operation of the system, with human intervention. The NBSZ shall enter the image data processed in order to fulfill the requests of the bodies authorized to gather intelligence under the Security Act, into the biometric image reference database of the system for the period of validity of the request (duration of its fulfilment). The data processed related to the warrants is synchronized to the warrant register, with a continuous data connection.

If the NBSZ detects a hit on a wanted person during the operation of the system, that facilitates the identification of that person, it shall notify the body conducting the warrant procedure. In order to be able to react during the operation of the system, in addition to the personal presence of the NBSZ staff at a given location, the staff of the body applying the measure must also be present in order to take measures against the wanted person. The NBSZ employees participating in the operation of the system only see the portrait, the unique identification number assigned to it, and the name of the requesting body. No warning signs or other signs indicating the taking of images by the NBSZ are placed at the data collection points.

In 2018, the system indicated about 6,000 portrait identities, based on which the open action bodies carried out a total of 209 identity checks at the sites and arrested 4 people.

On the basis of the information received, the Authority concluded that the primary purpose of the system operated by the NBSZ is to facilitate the implementation of monitoring tasks through gathering intelligence. This explains why the details of the operation of the system are not regulated in an implementing regulation, and why the NBSZ does not place a warning sign for taking pictures at the monitoring sites. Nevertheless, based on the answers of the data processing body described above, it can be stated that the operation of the examined NBSZ system, in the case of persons recognized in image files recorded hidden, partially automated and at data collection points, the aim is to filter out the wanted persons in comparison with the current (monitoring and warrant) reference database. However, it can be stated that the data processing does not exceed the statutory authority of the national security services to gather and process intelligence specified in the Security Act, in particular with regard to the following:

1. The data processing body answered the question of the Authority regarding the number of data collection points, the data collection sites (names of settlements) and the location of data collection points by stating that the data collection sites, as well as the duration of the data collection are determined by the location data included in the requests of the bodies authorized by the Security Act. The Authority concluded from this that the system operated by the NBSZ is not a permanent monitoring system established in a large geographical area, but it is locally operated at locations defined by certain specific monitoring tasks, in line with the deadlines of the given task.

2. The system operated by the NBSZ is not suitable for data collection involving stockpiling and mass identification by automatically identifying the persons appearing in the camera's field of vision at the data collection points, but it only performs face image comparisons based on the current data content of the reference database. The retention period of the data content of the reference database related to monitoring tasks is limited to the duration of that task. The image data stored in the reference database in connection with the warrant is synchronized with the warrant register.

3. Machine-assisted face image comparison and response require human labour. The need for live labour creates a bottleneck in the process of data use that precludes mass, stockpiling biometric data collection.

In the course of the investigation, the Authority did not receive any information that would indicate that the NBSZ's covert surveillance system, which assists in the performance of surveillance tasks and is also used in accordance with the

Warrant Act, would operate as a continuous, automated, filter-research-type infrastructure for mass covert surveillance over a large geographical area, causing massive violation of the right to personal data protection. The Authority therefore closed its investigation.

VI.2. Access to data of police informants

One citizen lodged an objection to the Authority because the National Police Headquarters (ORFK) did not comply with his request for data as to whether the persons he designated were members of the police staff or police informants. On the basis of the notification, the Authority initiated an investigation into the case and turned to the Office of the ORFK in order to clarify the facts. Based on the information obtained, it was established that the Office of the ORFK provided the requester with written information substantially in line with the actual legal situation stating that the identity of the persons secretly cooperating with the police ('informants') and their cooperation with the police do not belong to data of public interest or data accessible on public interest grounds, but these are personal data to be protected and cannot be disclosed on the basis of a request for access to data of public interest. According to the Authority, the position of the ORFK is also supported by the fact that if the data of persons cooperating with the police were found out, the persons concerned should fear the revenge of the criminal circles against whom they assisted in the work of criminal investigation. Under such circumstances, no one would undertake to co-operate with the police, which would seriously jeopardize the effectiveness of the police's criminal investigation activities. Furthermore, persons who secretly cooperate with the police are not subject to Section 26 (2) of the Privacy Act[27], as a person secretly cooperating with the police does not belong to the persons acting within the functions and powers of the organ performing public duties.
On this basis, the Authority concluded that the complaint concerning the refusal to answer the question on the status of the persons indicated in the complain-

27 'The name of the person acting within the functions and powers of the organ performing public duties, as well as his functions and duties, executive mandate, his other personal data relevant to performing public duties, and his personal data to which access is ensured by an Act, shall qualify as data accessible on public interest grounds. Personal data accessible on public interest grounds shall be disseminated in compliance with the principle of data processing limited to the intended purpose. [...]'.

ant's request as police informants, was manifestly unfounded. Therefore, the Authority closed the investigation and informed the complainant accordingly.

Regarding the other question, the Office of the ORFK justified its refusal to answer the question concerning the affiliation of the persons indicated in the complainant's letter with the police personnel by stating that, pursuant to Section 26 (2) of the Privacy Act, the fact whether or not a certain natural person belongs to the personnel of the Police shall be considered data accessible on public interest grounds only if the request to access data of public interest relates to some activity of the indicated person, which is related to the performance of the public task of the police or the exercise of its official authority. Furthermore, data accessible on public interest grounds can only be disseminated in compliance with the principle of purpose limitation and, according to the ORFK Office, 'in the present case the data request did not indicate any purpose or reason to consider that, if the designated persons were members of a police force, this would constitute data accessible on public interest grounds in relation to the request for data and thus, the right of data subjects to personal data could be restricted'.

The Authority pointed out that the line of reasoning described was incomplete because it did not take into account Section 276 (2) of Act XLII of 2015 on the employment of the professional staff of law enforcement agencies, according to which in addition to the data included in Section 26 (2) of the Privacy Act, the rank, citizenship, place of service of the member of the professional staff, as well as the awarded honorary title and the date on which the title was award are also data accessible on public interest grounds. The rule referred to does not contain a restriction that the information listed may be disclosed only in connection with an activity or event related to the employment relationship (for example, the award of an honorary title). Although the list does not specify the fact of belonging to the Police staff as data accessible on public interest grounds, the scope of data defined in the normative text, such as rank and place of service, implies the publicity of this information too. Therefore, the request for data with regard to data accessible on public interest grounds specified in Section 276 (2) of Act XLII of 2015 cannot be refused. The Authority added that of the data specified in Section 26 (2) of the Privacy Act and Section 276 (2) of Act XLII of 2015, those which constitute national classified data, for example in the case of undercover investigators, should not be released.

As regards the purpose limitation concerning the dissemination of data accessible on public interest grounds, the Authority stated that it should also be taken into account that the body processing data accessible on public interest grounds

is not entitled to make the disclosure of the requested data conditional on the communication of the data requester's intended purpose of data use or the content of the statement on the purpose of data use. However, when disclosing data accessible on public interest grounds, the data controller can draw the data requester's attention to the fact that he is responsible for the lawful use of the data accessible on public interest grounds obtained as a result of the data request as well as for the proper dissemination in accordance with the principle of purpose limitation as required by law.

Finally, the Authority asked the data processing body to notify the Authority if in the future it receives a data request or requests that could be interpreted as part of an action to systematically map and list the police personnel in violation of fundamental rights, as mass misuse of data related to police personnel is just as unacceptable as it is for any other citizen.

As a result of the exchange of letters, the Office of the ORFK fulfilled the complainant's data requests concerning the data accessible on public interest grounds. (NAIH/2019/6373)

VI.3. Restrictions to the Authority's right to access data

It is a requirement arising from the purpose of the Authority's data protection control established by the Fundamental Law to have access to all the data necessary to perform its tasks. The rights to access data (e.g. to enter the data processing site, request written information, etc.) are provided for by statutory provisions for each type of procedure (e.g. investigation procedure, data protection authority procedure, authority procedure for the review of data classification), and the scope of data are set out in Section 71 of the Privacy Act. Pursuant to this provision, in the course of its procedure, the Authority shall be entitled to process, to the extent and for the duration necessary for the procedure, in principle, all personal data as well as data that qualify as secrets protected by an Act and secrets obtained in the course of professional activities, which are related to the given procedure or which have to be processed for the purpose of concluding the procedure effectively. The Authority may use the documents, data or other tools of evidence acquired lawfully during its procedures in other procedures it conducts. In procedures related to the processing of classified data, the vice-president of the Authority and the public officials acting as executive officers, as

well as the investigators, shall, if they possess a personal security certificate with the appropriate level of clearance, be entitled to access classified data, even without the authorisation for use set forth in the Act on the protection of classified data. (The powers of the President of the Authority in relation to classified data are set out in the Act on the Protection of Classified Data.)

However, the Privacy Act, as an exception to the general rule, imposes restrictions which, in respect of a number of data sets, essentially preclude access to data by the Authority. These restrictions have so far not prevented the Authority from carrying out its tasks. However, in 2019, several authority procedures for the review of data classification were initiated in which these restrictions appeared as a circumstance significantly affecting the merits of the case, because the classified information subject to the case falls under this restriction. It is therefore worth mentioning this in more detail.

Pursuant to Section 71 (3) of the Privacy Act, in the course of its procedures specified in the Privacy Act, in the case of certain data sets listed in Act CXI of 2011 on the Commissioner of Fundamental Rights (hereinafter: Ajbtv.), the Authority shall have access to data as specified in the Ajbtv. The rules of Ajbtv referred to in the Privacy Act list the types of documents that the Commissioner for Fundamental Rights may not have access to during his investigation concerning the Hungarian Defence Forces, national security services, police, customs and customs directorates of the National Tax and Customs Administration and the investigative body of the Prosecutor's Office. According to the Privacy Act, the Authority is also prohibited to have access to about twenty-four of the documents listed in the Ajbtv. For example, in the case of its procedures concerning the Hungarian Defence Forces, the Authority may not have access to the following documents:

a) documents concerning the invention, product, defence investment and the development of the defence capability, which is of outstanding importance for the defence of Hungary, from which their essence can be learned,
b) documents containing the military order extract of the Hungarian Defence Forces up to the army level and containing aggregated data on the establishment, maintenance and dismantling of military stockpiles,
c) documents containing plans for the application of the Hungarian Defence Forces during the period of special legal order,
d) documents related to the protected management system of state and military senior management,

e) documents related to the combat readiness, alert and sales system of the Hungarian Defence Forces, summary documents on mobilization skills, the level of capability for war, as well as the overall combat readiness plans of military areas, military organizations of the same or higher level and the related documents for the whole organization,
f) the summary plan of reporting by the ministry headed by the Minister of Defence and the Hungarian Defence Forces, the key and other documentation of the special information protection devices that are systematized or applied,
i) documents containing the means of military reconnaissance, their operation, and documents containing aggregated data concerning the protection of the Hungarian Defence Forces against reconnaissance.

According to the Privacy Act, the Authority '*shall have access to the data […] in accordance with Section 23 (7) of the Ajbtv*.'[28] Section 23 (7) of the Ajbtv provides in the case of such data that if the Commissioner for Fundamental Rights considers it necessary to examine the listed documents in order to fully investigate the matter, he may request the Minister responsible to examine them. The Minister responsible shall carry out or have carried out the inquiry requested by the Commissioner for Fundamental Rights and shall inform the Commissioner for Fundamental Rights of the outcome of the inquiry within a period specified by him. The time limit may not be less than thirty days.

As a law enforcement body, the Authority acts in accordance with the law in force, but in our opinion the provisions outlined above raise a number of legal issues which, taken as a whole, put into question the constitutionality and applicability of these rules. The main problems are

1. The described legal construction does not allow for an independent, external monitoring of the legality of data processing in the case of the documents and data listed in the Ajbtv., as the independent external monitoring body cannot get to know their content. Thus, it should rely solely on the opinion of the responsible minister, that is, someone who may have a direct interest in maintaining the classification.

28 'Section 71 (3a) - (3c) of the Privacy Act alleviate the restriction of access to data in some respects, but they do not substantially change the regulatory construction, therefore their description is not necessary from the point of view of our subject

2. Not to mention that if the Authority were to review the lawfulness of the classification of data classified by the Minister that is subject to the restriction described above, on the basis of this regulatory structure, the Minister would ultimately decide for himself whether he had lawfully classified the data. Thus, the Authority would not have a say on the merits.

3. The weight of the problems outlined in the previous points is increased by the fact that the initiation of the authority procedure for the supervision of data classification by the court was regulated in the Privacy Act because of AB Decision 4/2015. (II. 13.). The AB decision found that there had been a violation of the Fundamental law due to the fact that, in case of the classification of data of public interest or data accessible on public interest grounds, the legislator did not ensure the possibility to enforce the fundamental right to access data of public interest directly through a procedure for the supervision of the content of data classification. According to the reasoning of the AB decision, the Constitutional Court established that without the substantive control over the data classification, the necessity and proportionality of the restriction of the right to access data of public interest cannot be ensured. In the absence of an effective procedure in the legal system to review and overturn the decision of the classifier restricting publicity, there can be no guarantee that data classification will only apply to data of public interest and data accessible on public interest grounds for which it is truly unavoidable. Nor can it be guaranteed that the classifier will comply with its obligation to state reasons and will take due account of the public interest in publicity. Therefore, on the basis of the right of access to data of public interest, a direct initiable substantive control over the data classification must be ensured, which is suitable not only for verifying compliance with the formal and procedural requirements of the classification, but also for reviewing the substantive justification and substantiation of the classification as well as the necessity and proportionality of the restriction on publicity. The Constitutional Court called on the Parliament to fulfil its legislative role by 31 May 2015. As a result, the Privacy Act has been modified by adding that if the request for access to data of public interest is refused by the controller due to the classified nature of the data, and the requesting party turns to court for the judicial review of the dismissal of his request, the court shall initiate an administrative authority procedure for the review of the data classification with the Authority and shall simultaneously suspend the court proceedings. Thus, according to the described AB decision and the text of the law, the Authority's authority procedure for the review of the data classification must play the role of substantive control over the data classification. It is incompatible with this requirement for the law to regulate the procedure of the Authority

in such a way that, in the case of certain scope of data, a minister may in fact have the final say on the lawfulness of the classification of the data.

4. Within the framework of the contested legal structure, the Authority has only one means of clarifying the facts in the authority procedure for the review of the data classification, namely to ask the Minister to examine documents whose contents it is not allowed to access. The exclusive nature of that means of proof is incompatible with the system of free proof of general administrative order.

5. It may also reasonably give rise to unnecessary and disproportionate restriction of the data applicant's right to a due process if a data requester seeks a legal remedy before a court because the data controller has refused to comply with his or her request for access to data of public interest and the court initiates authority procedure for the review of the data classification in accordance with Section 31 (6a) of the Privacy Act, then in the authority procedure for the review of the data classification the Authority must establish in its decision that the classification of the data was lawful, relying only on the opinion of the Minister responsible for the data (who may be the classifier himself, or the superior of the classifier, or otherwise a person interested in maintaining the classification).

VII. International Affairs and Public Relations

The European Data Protection Board (hereinafter „the EDPB") was established by the EU General Data Protection Regulation on 25 May 2018. The year 2019 was the first full calendar year in the operation of the Board. The Authority actively participates in the activities of the EDPB, and we will present in detail the work in the expert subgroups below. The Authority is represented in all expert subgroups and, in addition, is involved in performing tasks of major international importance. Such is the annual review of the Privacy Shield mechanism, playing a significant role in the relations between the United States of America and the EU, in which a Hungarian expert also regularly participates.

VII.1. Activities and legal interpretation work of the European Data Protection Board

The activities of the EDPB are diverse, however, it has powers that it has not yet exercised. Thus, for example, decision in dispute resolution has not yet been adopted by the EDPB. The EDPB is more active in the field of legal interpretation, preparing and publishing guidelines, recommendations and opinions.

VII.1.1. Legal interpretation work of the EDPB

1. *Guidelines of the EDPB*

In 2019, the EDPB adopted five guidelines. The Guidelines on Codes of Conduct and Monitoring Bodies provides interpretative assistance in relation to the application of Articles 40 and 41 of the GDPR. In another guidelines, the EDPB provides guidance on the applicability of the contractual legal basis [Article 1 (1) (b)] in the context of the correct application of online services.[29]

29 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdft

The guidelines on data processing through video devices is one of the most anticipated documents.[30] The EDPB finalized this guidelines too following a public consultation. The EDPB adopted two other guidelines of technological relevance back in 2019: one dealt with the issue of data protection by design and by default[31], while the other summarized the criteria of the right to be forgotten[32]. The latter will be supplemented by a second part in the next period, however, the EDPB has already published its recommendations on which it has reached a consensus.

2. *Opinions of the EDPB*

Most of the opinions were issued by the EDPB in the framework of the consistency mechanism. In the consistency mechanism, the measures of the supervisory authorities at Member State level are subject to the approval of the EDPB. Through these procedures, the GDPR sought to ensure the consistent application of the Regulation throughout the Union. The list of processing operations subject to the requirement for a data protection impact assessment has been adopted by the supervisory authorities pursuant to Article 35 (4) of the GDPR, all of which have been finalized through consistency procedure. Some of these decisions were adopted in 2019, so some of the EDPB's opinions affected these lists.

In the framework of the same procedure, the authorities shall determine the data processing which are not subject to the obligation of data protection. In 2019, three such opinions and related Member State decisions were issued.

Important issues of legal interpretation were also dealt with in the consistency mechanism, in the framework of which the EDPB adopted an opinion on the interplay between the ePrivacy Directive concerning the processing of personal data in the electronic communications sector and the GDPR[33], as well as on the

30 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf
31 https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_en
32 https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-52019-criteria-right-be-forgotten-search-engines_en
33 https://edpb.europa.eu/our-work-tools/our-documents/noukogu-arvamus-artikkel-64/opinion-52019-interplay-between-eprivacy_en

competence of a supervisory authority in case of a change in circumstances relating to the main or single establishment of the data controller in the EU[34].

In the framework the consistency mechanism, the Board approves binding corporate rules (BCRs). In 2019, two such opinions were issued, but their number is expected to increase significantly in the future. In addition to the above, the Board exercises powers to regulate the transfers of data to third countries, which is essential to promote the consistent application of the GDPR and, in this context, to ensure a uniform level of protection.

3. *Other documents of the EDPB*

The EDPB issued a joint opinion with the European Data Protection Supervisor on the processing of patients' data and the role of the European Commission within the eHealth Digital Service Infrastructure[35].

The EDPB also laid down the rules of the procedure for the approval of certification criteria resulting in a common certification, the European Data Protection Seal.[36] There are few developments in the field of certification mechanism in the European Union, and it would be desirable for data processing organizations to make use of voluntary means of ensuring compliance, including certification. The adoption of this document points in this direction.

VII.1.2. Expert Subgroups

The documents adopted at the plenary session of the EDPB have been presented above. The decision-making forum of the board work is the plenary session, however, most of the work is done in the so-called expert subgroups. This work is presented in details below by subgroups.

34 https://edpb.europa.eu/our-work-tools/our-documents/valdybos-nuomone-64-str/opinion-82019-competence-supervisory-authority_en

35 https://edpb.europa.eu/our-work-tools/our-documents/valdybos-nuomone-64-str/opinion-82019-competence-supervisory-authority_en

36 https://edpb.europa.eu/our-work-tools/our-documents/procedure/edpb-document-procedure-approval-certification-criteria-edpb_en

1. *Key Provisions Expert Subgroup*

The „Key Provisions" subgroup of the Data Protection Working Party set up under Article 29 of the former Directive 95/46/ EC continued its work after the establishment of the European Data Protection Board, under the name „Key Provisions" expert subgroup (hereinafter „KPESG"). In the expert subgroup, national experts from EU Member States represent the supervisory authorities of each Member State. KPESG's main task is to develop general guidelines to promote the consistent interpretation and application of European data protection law, in particular the GDPR and the Police Directive. It also involves those applying the law and other experts in its work in the form of public consultations.

To be highlighted is the EDPB Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, developed by the KPESG. The subject of this document is the interpretation of the provisions of the GDPR relating to the contractual legal basis, as well as practical guidance on issues arising in its application. The guidelines, which have also been released for public consultation, can be found on the EDPB's website[37].

2. *IT User Expert Subgroup*

The IT User Expert Subgroup is one of the youngest subgroups in the EDPB. Its role is to facilitate the development of consistent user practices for the information systems operated by the EDPB and to oversee the development and expansion of the systems, in particular the Internal Market Information System (IMI).

The expert subgroup focuses on the development of the IMI system and the resolution of existing system problems. At group meetings, members provide feedback and suggestions to the system development team and monitor the schedule of improvements.

During the meetings of the expert subgroup, it discusses the latest system developments, takes stock of the development proposals received from the authorities, and decides on issues related to major changes affecting the system.

37 https://edpb.europa.eu/our-work-tools/our-documents/smjernice/guidelines-22019-processing-personal-data-under-article-61b_en

In addition, meetings will provide an opportunity for Member States' experts to share details of their internal case management practices, and the EDPB Secretariat may call on the members to develop good and consistent user practices.

Although the focus is on the IMI system, this expert subgroup also deals with other IT systems that support the functioning of the EDPB. Examples are the EDPB videoconferencing system and the EDPB Confluence, a knowledge base and document sharing system for internal cooperation between Member States' authorities.

3. *Financial Matters Expert Subgroup*

The task of the Financial Experts Subgroup is to examine issues related to the application of data protection provisions in the financial sector. In 2019, the subgroup's tasks included examining the Foreign Account Tax Compliance Act aiming to monitor the tax obligations of US citizens living abroad (FATCA), drafting an opinion on an administrative agreement with the European Securities and Markets Authority (ESMA) and preparing a questionnaire related to the OECD standard reporting system (CRS).

The main task of the expert group this year was to prepare guidelines on the interplay between the GDPR and Directive 2015/2366 / EU on payment services in the internal market (PSD2), given that a number of data protection issues have arisen since the implementation of PSD2 into Member States. In February 2019, the subgroup organized a PSD2 workshop with market stakeholders in order to identify all the substantive issues that the guidelines should address. The text of the guidelines is being drafted and will be made public after its adoption by the EDPB, which is expected in the second half of 2020.

In addition, the expert subgroup is working on a recommendation on the online processing and retention of credit card data, and is working with the technology expert subgroup to develop comprehensive guidelines on blockchain and cryptocurrencies.

4. *Cooperation Expert Subgroup*

The outside world has little insight into the activities of the expert subgroup, as it deals with issues related to cooperation between authorities. The documents

prepared by the Cooperation Expert Subgroup are not addressed to the citizen or data controller concerned, but to the data protection authorities themselves. The subgroup has an important role to play in ensuring a smooth application of the GDPR between authorities, based on a consistent approach to procedural rules.

5. *Social Media Expert Subgroup*

The expert subgroup set up in 2018 met four times in 2019. In accordance with the established practice, in order to ensure transparency, mutual information and the sharing of relevant information, members delegated to the subgroup shall briefly report on their social media activities at national level at the beginning of the meetings, including any guidelines, recommendations issued and the status of major inquiries.

In view of the fact that there were European elections as well as national elections in several Member States in 2019, the exchange of experience and information on the processing and use of personal data in elections and the use of social media by political parties was also a recurring element of the meetings.

The drafting of guidelines related to the targeted advertising to social media users has been a permanent feature of the meetings, but the document has not yet been finalized due to the limited number of meetings and the lack of consensus on certain parts of the guidelines.

The expert subgroup prepared a document for supervisory authorities containing proposals for common strategic priorities for supervision, which was also approved by the EDPB.

The expert subgroup received a mandate from the EDPB to prepare a document on the functioning of social networks. It is planned that the document will focus only on front-end data processing and will include recommendations and best practices, but would not analyze back-end processes. The compilation of the document and the substantive work will continue in 2020.

6. *Technology Expert Subgroup*

As in previous years, the Technology Expert Group of the EDPB participated in the preparation and wording of several important guidelines in 2019. The drafting of the guidelines on camera surveillance was completed during 2019, and the group also prepared guidelines on the issue of data protection by design and by default[38].

The expert group also drafted guidelines on connected vehicle[39] , as well as draft opinions on the interplay between the ePrivacy Directive and the GDPR[40].

As last year, another important task of the expert group was to analyze the consistency of the list of data processing operations submitted by the supervisory authorities under Article 35 (4) of the GDPR. By 2019, all Member State lists were completed and all submitted lists were followed up by the expert subgroup. In 2019, several authorities submitted a list of types of data processing operations submitted under Article 35 (5) for which no data protection impact assessment is required. The expert subgroup also analyzed these lists and submitted the draft decisions to the Plenary Meeting.

In addition to the above, work continued on the drafting of a number of recommendations and guidelines, including a draft on the risk analysis of personal data breach and on blockchain.

7. *Compliance, eGovernment and Health Expert Subgroup*

The EDPB's Expert Subgroup on Compliance, eGovernment and Health is responsible for compliance with codes of conduct, certification, data protection impact assessment, principle of data protection by-design and by default pursuant to GDPR, as well as issues related to e-government and health data processing. In 2019, the expert group held a total of eleven meetings.

38 https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_en

39 https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-12020-processing-personal-data-context_en

40 https://edpb.europa.eu/our-work-tools/our-documents/noukogu-arvamus-artikkel-64/opinion-52019-interplay-between-eprivacy_en

At its first meetings in 2019, the expert group finalized the text of the guidelines on codes of conduct and monitoring bodies. The guidelines were approved by the EDPB, which then published the text finalized after the public consultation under number 1/2019. The guidelines have since been available in Hungarian, on both the EDPB's and NAIH's websites[41].

One of the main tasks of the expert subgroup is to provide an opinion on the criteria for the accreditation of the body monitoring the codes of conduct to be issued by the supervisory authorities. Pursuant to Article 64 (1) (c) of the GDPR, such a draft decision must be adopted in a consistency mechanism. In 2019, the EDPB issued an opinion on a set of criteria drawn up by the national supervisory authorities of a total of two Member States (Austria, United Kingdom). Furthermore, three other Member States (Spain, France, Belgium) initiated proceedings before the EDPB, which were still ongoing in early 2020. The NAIH plans to submit its criteria to the EDPB for comment in the first half of 2020.

Another main task of the expert subgroup is to provide opinions on additional criteria for the accreditation of certification bodies, the decision on which should also be adopted in a consistency mechanism. In 2019, a total of two Member States (UK, Luxembourg) initiated proceedings before the EDPB, which were still ongoing in early 2020. The NAIH plans to submit its criteria to the Board for comment in the first half of 2020.

8. *Enforcement Expert Subgroup*

The Enforcement Expert Subgroup of the EDPB shall be responsible for all matters related to substantive and procedural law that do not fall within the remit of any other subgroup. In the subgroup, there are typically more consultations related to the application of law by the authorities, however, as the application of law also requires legal interpretation, issues concerning the data controller-data processor side as well as the data subjects themselves may also be on the agenda.

In line with the practice of 2018, the subgroup has meeting every two months. The recurring item on the agenda of the subgroup meetings is to discuss the substantive and procedural legal issues and practical problems proposed by the su-

41 https://edpb.europa.eu/our-work-tools/our-documents/wytyczne/guidelines-12019-codes-conduct-and-monitoring-bodies-under_hu

pervisory authorities of each Member State, usually through a legal case arising in the practice of the initiating authority. In 2019, for example, the subgroup discussed legal issues related to large public registers, the use of cookies, postal service providers, the interpretation of Article 15 (3) of the GDPR, the application of Article 57 (4) of the GDPR, the sharing of experiences related to the investigative powers of the authorities, the possibilities of joint handling of complaints, the tasks related to the identification of the authorities concerned and, in the case of cross-border processing of personal data, the sharing of the final decision taken by the lead supervisory authority.

In addition to the above, the subgroup will continue to be responsible for developing guidelines for the consistent application of the law and, if necessary, for reviewing documents already issued. In 2019, the subgroup presented the first part of the draft guidelines on the criteria of the right to be forgotten to the plenary, which was adopted by the plenary under number 5/2019 and submitted for public consultation[42].

9. *Fining Taskforce*

This expert subgroup was separated from the Enforcement Expert Subgroup of the EDPB. Its task is to help bring the fining practices of Member States' supervisory authorities as close as possible.

In order to achieve the above objective, in 2019, the group continued to assess the fining practices of individual Member States in several questionnaires, such as for minor, recurrent and persistent data breaches by natural persons. The information obtained from the questionnaires on the imposition of fines can serve as a starting point for the development of one or more guidelines to facilitate the harmonized imposition of fines.

One of the key tasks for 2019 in the subgroup was the interpretation of the definition of „undertaking" specified in recital 150 and in Article 83 (4) to (6) of the GDPR.

42 https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-52019-criteria-right-be-forgotten-search_en

10. *International Transfers Expert Subgroup*

The International Transfers Expert Subgroup (ITS) of the EDPB held a meeting six times in 2019. The year 2019 has been defined by work on the interpretation of the provisions of Chapter V of the GDPR on the transfer of personal data to third countries or international organisations.

Earlier this year, the EDPB adopted Opinion 4/2019 on the draft Administrative Arrangement for the transfer of personal data between European Economic Area (EEA) Financial Supervisory Authorities and non-EEA Financial Supervisory authorities. In this, the EDPB gave an opinion on the provisions to be included in an administrative agreement concluded between public authorities or other bodies performing public tasks in accordance with Article 46 (3) (b) of the GDPR. The examination of the agreement and the preparation of the opinion of the EDPB took place within the framework of ITS. The opinion is also the starting point for the guidelines prepared by the subgroup on the means of data transfer between public authorities and bodies, the wording of which has not been completed by the end of 2019. These guidelines would aim to summarize the minimum requirements for the instruments set out in Article 46 (2) (a) and Article 46 (3) (b) of the GDPR.

The subgroup also started preparing a code of conduct as well as guidelines on certification as a means of data transfer, in which the EDPB would summarize how and under what requirements these two new tools, introduced by the GDPR, provide adequate guarantees for the transfer of personal data to third countries.

During 2019, experts of ITS also held professional consultations and exchanges of experience on a number of specific issues related to the approval of Binding Corporate Rules ('BCRs') and other data transfers. In two cases, the EDPB also issued an opinion on the draft decision of the competent supervisory authority approving the BCR (Opinions 15/2019 and 16/2019), which were also prepared within the framework of ITS.

Furthermore, a BCR workshop was organized within the subgroup by the Norwegian Supervisory Authority in Oslo on 11-12 June 2019, during which experts with extensive experience in the field gave presentations, as well as practical tasks related to BCR opinion were solved.

VII.2. Third Annual Review of the Privacy Shield Agreement

The third annual joint review of the Privacy Shield adopted by the European Commission in 2016 (under which organizations subject to the EU-US Privacy Shield provide an adequate level of protection for personal data) was held in Washington, DC on the 11-13th September 2019, with the participation of a staff member of NAIH. During the review, the Union examination group consisting of members of the European Commission and the delegated experts of the EDPB, and the delegation of the United States met to discuss developments following the second annual review and the issues related to the obligations under Privacy Shield Framework.

In the course of the review, presentations and consultations were made in connection with data processing for business and commercial purposes under the Privacy Shield Framework, and topics related to data processing for national security and law enforcement purposes were discussed by the parties.

Following the review, the European Commission and the EDPB prepared and published a separate report on the results. The main findings of the EDPB's report are as follows:

1. *Findings related to data processing for business and commercial purposes*

   – The EDPB welcomes that the Department of Commerce ('DoC') as well as the Federal Trade Commission ('FTC') also undertook new ex officio oversight and enforcement actions as regards the compliance of Privacy Shield certified organizations with the requirements under the Privacy Shield.

   – *However, one of the main concerns already expressed by the EDPB remains that such enforcement actions still do not focus on the actual, substantive compliance with the Privacy Shield's principles. One example for which the EDPB sees the need for more substantive checks are onward transfers.*

   – In its report, the EDPB recommended tightening the deadlines for the re-certification process so that the length of the procedure does not create uncertainty for the EU organisations transferring the data or for the data subjects.

2. *Findings related to data processing for national security and law enforcement purposes*

   – The Report welcomes the appointments of a permanent Ombudsperson and of the last missing members of the Privacy and Civil Liberties Oversight Board (’PCLOB’). The latter will thus be able again to issue opinions and reports on national security data collection after a long time.

   – The Report maintained some of the concerns raised in previous years regarding data processing for national security and law enforcement purposes, such as the lack of a remedy in the case of collections of data under Section 702 of the Foreign Intelligence Surveillance Act (‚FISA’) and Presidential Decree 12333.

   – The Board reiterated its concern that very limited information on the collection of data for national security purposes is shared by the US delegation during the review, which makes it difficult to analyse the existence of an adequate level of protection.

VII.3. International Relations of the Authority

The Authority considers a priority to exchanging experiences with data protection and freedom of information organisations in both the European Union and non-EU countries, and is open to receiving delegations, professionals and university students from abroad. A good example of this is a multi-year cooperation in which students of the Kiev University of Law of the Ukrainian Academy of Sciences regularly participate in the programs announced by the Authority. Furthermore, the cooperation agreement signed in November 2019 between the Commissioner for Human Rights of the Ukrainian Parliament and the NAIH should be highlighted. The purpose of the agreement is for the Hungarian and Ukrainian parties to ‘strengthen their efforts to promote the development and effective implementation of international standards in the field of human rights and fundamental freedoms, the rule of law and democratic development, in particular the protection of personal data’.

1. *Foreign delegations visiting the Authority in 2019*

Between 7-8 March 2019, Bosnian data protection experts visited our Authority. Through the lectures given by our staff, they got to know the Hungarian aspects of the application and implementation of the GDPR and the Police Directive, in accordance with the interests previously sent by Bosnian colleagues.

On 26 April 2019, a delegation representing Turkey visited the NAIH. The purpose of the visit for the staff of the Turkish authority established in 2016 was to get to know the operation and organisational structure of the NAIH, as well as the competencies and tasks of the individual organisational units, in order to make their own operation more efficient with the knowledge gained from them.

Between the 16th and 18th September 2019, the Authority received students from the Kiev University of Law of the Ukrainian Academy of Sciences. In the framework of the cooperation between the University and the NAIH, a call on data protection was announced for the third time. The authors of the best entries were able to travel to Hungary and, in addition to our Authority, to learn about the Office of the Commissioner for Fundamental Rights and the operation of the Constitutional Court.

On 19 September 2019, a 14-member Japanese delegation arrived at the Authority to take part in a study visit aimed at gaining insight into practical experience in Hungary and Europe in relation to the GDPR. In the course of the consultation, following the presentations of the Authority's staff, participants discussed law enforcement issues.

2. *Participation of the President of the Authority at Professional Conferences and Events in 2019*

5 February 2019 - Budapest - Data Protection Breakfast organized by ARB Privacy Consulting Kft. - ***Experience in the application of GDPR*** - round table discussion

8 February 2019 - Budapest - First Hungarian Decision-Making Think Tank (Challenge) professional-methodological conference organized by the OPH Group - ***Challenges of GDPR, experiences of its implementation, especially with regard to critical issues of application***

11 February 2019 - Budapest - „GDPR from the side of practice - valuable answers the first hand" conference organized by Adatvedelmi.hu - ***Experiences of applying GDPR through the eyes of NAIH***

20 February 2019 - Budapest - „FRAUD 2019, PSD2 and IT Security Challenges under a Magnifying Glass" conference organized by IIR Hungary - ***Fraud Aspects of GDPR***

26 February 2019 - Budapest - Security Market 2018-2019 conference organized by GTTSZ, MRTT and Biztonságpiac Média és Kiadó Kft. - ***IT innovations, data protection, information security trends in Hungary*** - podium discussion

4 March 2019 - Balatonakarattya - Hungarian Defence Forces Data Protection Conference - ***2018 from the point of view of the Authority, the experiences of the GDPR so far***

7 March 2019 - Zamárdi - Lecture for students participating in the Hungarian Administrative Scholarship Program organized by the Administrative Scholarship Programs and Government Office Training Department of the Prime Minister's Office - ***Basics of Information Security and Data Protection***

10-13 March 2019 – Johannesburg – ICIC 2019, International Conference of Information Commissioners – ***Right of access to information and the impact on vulnerable groups – panel moderator***

20 March 2019 - Budapest - Training for local government leaders and condominium managers organized by the National Data Protection Association - ***Presentation of the book 'Guide to the GDPR'***

21 March 2019 - Szekszárd - Tolna County Government Office's first regular meeting of the year - ***First experiences with the application of the GDPR***

25 March 2019 - Budapest –'GDPR Reform Act 2019 - What changes can be expected during the adaptation of sectoral laws to GDPR rules?' conference organized of the Infoszféra - ***National Application of the GDP***R

1 April 2019 - Budapest - National University of Public Administration Acta Humana - Human Rights Bulletin Periodicals conference, presentation of the volume 'Administrative justice' - opening

25 April 2019 - Budapest - Conference entitled “GDPR Reform Act 2019, Spring Amendments to the GDPR Act” organized by Infoszféra - ***Hungarian application of the GDPR, Reform Act, statistics***

29 April 2019 - Budapest - Hungarian Decision-Making Think Tank (Challenge) Conference Series organized by the OPH Group - ***The Impact of EU Data Protection Reform in Hungarian Legislation***

14 May 2019 - Balatonszemes - GDPR data administrator meeting organized by OTP - ***GDPR in Hungary***

15 May 2019 - Budapest - 1 year of GDPR - focus on recent sectoral legislation and last year’s practice - thematic training in the presentation of NAIH and data protection experts organized by Adatvedelmi.hu - ***Changes in sectoral legislation, or will the situation be exacerbated from now on?***

23 May 2019 - Budapest - Criminal Professional Day organized by the National Tax and Customs Board - ***Data protection issues considering the specialty of criminal personal data from the perspective of NAIH***

24 May 2019 - Lillafüred - Hungarian Law Society Forty-second Meeting of Lawyers - ***First experiences with the amended Privacy Act and the application of the GDPR***

28 May 2019 - Budapest - ISACA Budapest Chapter Conference - 2019 - ***GDPR 2.0***

3 June 2019 - Budapest - Board Meeting of the Hungarian Banking Association - ***Current data protection issues related to the banking secto***r

4 June 2019 - Budapest - IT Security Professional Day 2019 organized by the Nádor System House - ***First experiences with the amended Privacy Act and the application of the GDPR***

14 June 2019 - Budapest - GDPR training and experience exchange event organized by the Hungarian Chamber of Auditors Education Center - ***First experiences with the amended Privacy Act and the application of the GDPR***

14 June 2019 - Debrecen - Hajdú-Bihar County Legal Day organized by the Hajdú-Bihar County Organization of the Hungarian Bar Association - ***Practical application of the EU data protection regulation***

11 July 2019 - Budapest - Guide to avoid fines - official control conference organized by Menedzser Praxis Kft. - ***NAIH fines based on GDPR***

26 September 2019 - Budapest - The last 1 year of the GDPR - national and international practice, fining experience in the organization of KLART - ***Imposition of fines in practice and balancing of interests***

27 September 2019 - Budapest - Researchers' Night organized by the National University of Public Service - ***Experiences with the application of the GDPR***

30 September 2019 - Madrid - Global Technology Governance for the Fourth Industrial Revolution Conference organized by the Digital Future Society

2 October 2019 - Budapest - Current issues of data protection conference organized by the Department of Cybercrime of NKE RTK - ***Experiences with the application of the GDPR***

3 October 2019 - Budapest - Conference of Legal Advisers organized by the Legal Advice Section of the Budapest Bar Association - ***Experience with the amended Privacy Act and the application of the GDPR***

8-9 October 2019 - London - ***Intelligence Oversight Forum organized by the Office of the High Commissioner for Human Rights***

15 October 2019 - Budapest - Data Protection Breakfast organized by ARB Privacy Consulting Kft. - ***Experiences with the application of GDPR*** - round table discussion

16 October 2019 - Balatonfüred - X. Infotér Conference - OUR Person! - ***The individual and his data in the age of MI***

17 October 2019 - Budapest - Ministry of Interior Probono training – Experiences with the application of GDPR and the Privacy Act - ***The links between data protection and artificial intelligence***

29 October 2019 - Budapest - GDPR: Practical Experiences Workshop organized by the Budapest Chamber of Commerce and Industry and NAIH - ***Practical experiences in connection with the GDPR (official inspections, fines)***

6-7 November 2019. - Moscow - 10th International Personal Data Security Conference - ***GDPR effects on the Hungarian legislation and data protection***

8 November 2019 - Esztergom - Lawyers' Conference for Lawyers Working for Catholic Dioceses - ***Practical Experiences in the context of the GDPR***

14 November 2019 - Debrecen - 1st Conference of University Data Protection Officers - GDPR - Official Experiences

25 November 2019 - Balatonföldvár - Law enforcement data protection professional days organized by the Directorate General for National Disaster Management of the Ministry of Interior - ***Regulations of the new data protection decree***

8-9 October 2019 - London - Intelligence Oversight Forum organized by the Office of the High Commissioner for Human Rights

26 November 2019 - Budapest - Annual Data Protection Conference (National Police Headquarters) - ***Regulations of the new data protection regulation***

3-4 December 2019 - Gibraltar - 2nd Case Handling Workshop on Freedom of Information and Access to Information

5 December 2019 - Budapest - Human Rights Conference, Dialogue or Monologue: The Future of the European Union - ***New European Data Protection Regulation and National Sovereignty***

11 December 2019 - Budapest - Infoszféra Conference: Data Protection 2019-2020, The Practice of Applying the GDPR - ***NAIH's Experiences, Decisions, Plans***

12 December 2019 - Budapest - „Latest developments in data protection law" conference in memory of Giovanni Buttarelli, VII. Conference of KRE-ÁJK Department of Infocommunication Law co-organized with NAIH - ***Recent Developments in the Practice of NAIH***

VII.4. Application for the post of European Data Protection Supervisor

The institution of the European Data Protection Supervisor (hereinafter: EDPS) was established in 2004 with the aim to monitor the data processing of the institutions and other bodies of the European Union, with powers similar to those of the data protection authorities of the Member States. The European Data Protection Supervisor is appointed for five years. Before the end of the term of office, a public call shall be announced for candidates who meet the established professional conditions.

A Hungarian expert also applied as candidate for the European Data Protection Supervisor post for the 2019-24 term of office. The Vice-President of the NAIH, as the first Hungarian candidate in the history of the European Data Protection Supervisor, was added to the shortlist of three experts drawn up by the European Commission, along with a Polish and a French candidate. The Permanent Representatives of the Governments of the Member States to the Council of the European Union (Coreper) and then the Committee on Civil Liberties, Justice and Home Affairs of the European Parliament (LIBE) hold individual hearings for each of the three shortlisted candidates.

At the end of the selection procedure, the Polish candidate, Wojciech Wiewiórowski was appointed as EDPS, however, the candidacy of Endre Győző Szabó can be considered a success of Hungarian data protection. The candidate told the Hungarian Telegraph Office that the strength of the Hungarian data protection culture and the active role of the Hungarian authority in the EU are also indicated by the fact that a Hungarian candidate remained standing in the standard senior management selection procedure of the European Commission. Last but not least, candidacy also means an institutional experience that is useful for Hungarian candidates applying for a similar position in the futur.

The three shortlisted candidates for the European Data Protection Supervisor post at the European Parliament in Strasbourg on the 25th November 2019, following the hearing before the LIBE Commission (from left: Wojciech Wiewiórowski (PL), Yann Padova (FR), Endre Győző Szabó)

VIII. NAIH Projects

VIII.1. Projects STAR I and STAR II

In cooperation with the Vrije Universiteit (VUB) in Brussels and the British Trilateral Research Ltd (TRI), the NAIH participates in two data protection projects co-funded by the European Union

VIII.1.1. A STAR projekt

The Project STAR ('Supporting Training Activities on the Data Protection Reform') is a project co-financed by the European Union under its Rights, Equality and Citizenship program for 2014-2020 (belonging to project REC-RDAT-TRAI-AG-2016 with number 769138) covering the period from the 1st November 2017 till 31st October 2019.

The STAR project has developed new training materials for data protection authorities and other stakeholders, specifically tailored to the needs and challenges of the sector and easily adaptable to it, in order to facilitate the proper application of the General Data Protection Regulation. The STAR Consortium held a conference for data protection officials on 17 October 2019 in Brussels, furthermore, it participated in a panel for data protection authorities on 22 October 2019, which was included in the events of the 41st International Conference of Data Protection and Privacy Commissioners (ICDPPC).

11 Microsoft PowerPoint presentations in the topics below have been developed with detailed guidance that can be used by anyone and can be easily adapted to the user's needs. These educational materials are freely available and can be downloaded from the project's website in English at http://www.project-star.eu/training-materials, as well as from the NAIH website in Hungarian[43].

- *Introduction to the European Union Data Protection Regime*
- *Purposes and legal grounds for processing personal data*
- *The rights of the data subject and their exercise*

43 https://www.naih.hu/eredmenyek.html

- *Responsibilities of data controllers and processors*
- *Role of the DPO*
- *Role of the DPA*
- *Technical and organisational measures*
- *Risk-based approach to data protection*
- *Data Protection Impact Assessments*
- *Data Protection Communication*
- *It's not just the GDPR – GDPR related laws and special provisions*

Each training module provides the instructor with guidance on the pedagogical approach to be applied, includes links to additional materials and resources, and helps to tailor the slide shows to the needs of a particular audience. In addition to the training materials, a handbook has been developed to provide guidance to trainers on the use of STAR training materials, as well as a list to assess the quality and comprehensiveness of other GDPR training.

VIII.1.2. Project STAR II

The Project STAR II ('SupporT small And medium enterprises on the data protection Reform II') is a project co-financed by the European Union under its Rights, Equality and Citizenship program for 2014-2020 (belonging to project REC-RDAT-TRAI-AG-2017 with number 814775) covering the period from the 1st August 2018 till 31st July 2020.

The project aims to support the development of good data protection practices, taking into account the structure and needs of small and medium-sized enterprises, as well as promote the consistent application of the GDPR, cross-border cooperation and the dissemination of best practices between Member States.

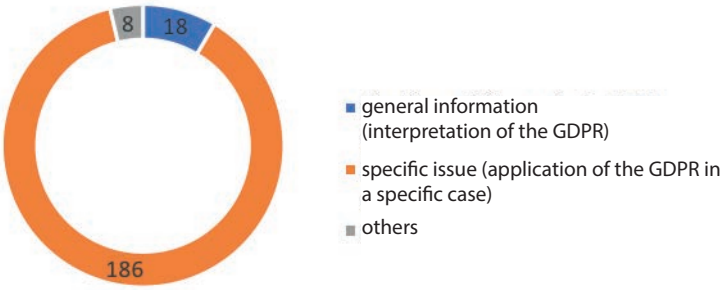
During the project, the Partners assess how EU data protection authorities support small and medium-sized enterprises (SMEs) to comply with the GDPR and develop a guide for data protection authorities to facilitate their communication with small and medium-sized enterprises.

Within the framework of the project, NAIH receives questions from SMEs operating in the EU by e-mail (kkvhotline@naih.hu) within the framework of a hotline created specifically for this purpose and operating between 15 March 2019 and 15 March 2020. The Authority's staff responds to SME consultation questions quickly and, of course, free of charge, thereby helping the operation of the SME

sector (in a way that is unique in the EU). During the project, building on the experience of the hotline, a handbook will be developed, that will be widely available and used across the EU.

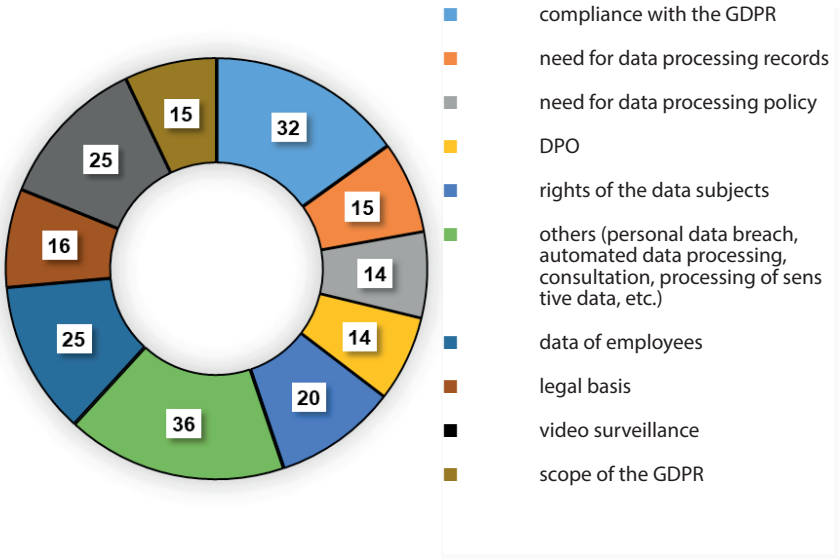
In the first ten months of operation of the SME hotline, the Authority received 212 questions. Of the questions received, 186 related to the application of the GDPR concerning a specific case, 18 to the interpretation of the GDPR, and 8 did not fall within the scope of the hotline.

Breakdown of questions received by the SME hotline by topics

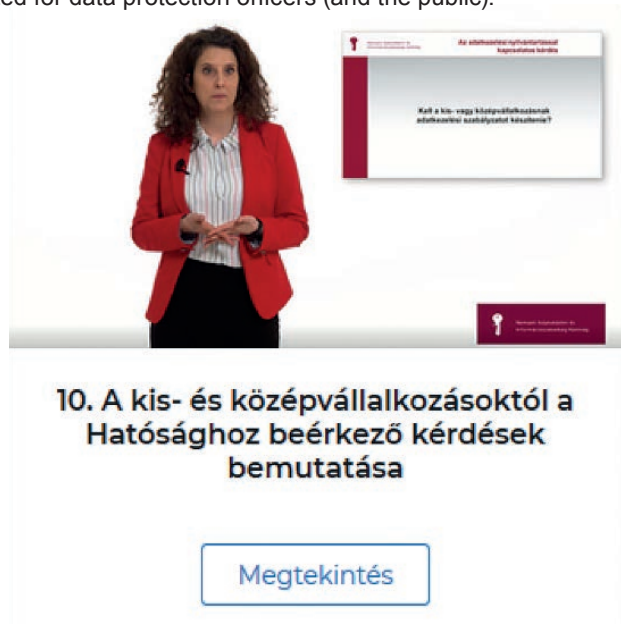


By subject, most of the questions concerned the compliance of a specific data processing with the GDPR, followed by questions related to the rules on video and audio recording, the processing of employees' personal data, the exercise of data subjects' rights, the legal basis for data processing and the need for data processing records, furthermore the scope of the GDPR.

Distribution of the questions received



The experiences with the hotline were also presented at the electronic conference organized for data protection officers (and the public):



VIII.2. Project KÖFOP

The project '*Review of the scope of data subject to statutory disclosure obligations*' was named by amending Government Decision 1004/2016 (I. 18.) on the establishment of the annual development framework of the Public Administration and Public Service Development Operational Program at the end of November 2018. In August 2019, the NAIH, as the beneficiary named in the Government decision, submitted an aid application for the implementation of the priority project '*Mapping and increasing the efficiency of the domestic practice of freedom of information*'. The aid application is still pending.

VIII.3. Project IJR of the NAIH to support the preparations for the application of the GDPR and the implementation of its specialist tasks

In the framework of the KÖFOP 1.0.0. – VEKOP-15 priority government project based on Government Decision 1004/2016. (I.18.), the Integrated Legislation System (hereinafter: 'the IJR ') was established to decrease the administrative burdens of budget organs.

In the framework of this project, the development of procedural, administrative, information technology and information security of the NAIH, aligning to the changes in legislation arising from the European Union obligations, was implemented in 2019.

In April 2017, the first amendment of funding contract of the IJR project under Government Decision 1585/2016 (X. 25), which includes the NAIH among the consortium partners and the tasks supported by the project and arising from the GDPR.

The fulfilment of the requirements under the GDPR required a full-scale optimization, redesigning of the legal professional areas of NAIH and their implementation in 2019. Furthermore, it has become necessary to create and ensure the operation of an IT environment that supports redesigned processes, while ensuring flexible redesignability.

The organizational framework of the NAIH also has to shift towards authority operational requirements, implying a tighter and more controlled approach to operation in 2019.

The support and operation of the results of the legal-professional and IT development carried out within the framework of the project also had to be adjusted, while the new organizational structure created during the legal-professional organizational development had to be set up.

Under the IJR project, the Data Breach Notification System (DBN) and a Processing Assurance System (DBP) were established in 2018, which handled more than 500 personal data breach notifications in 2019.

In 2019, in the framework of the IJR Project, the work of developing an integrated, intelligent administration and decision-preparing module for NAIH continued. Furthermore, the IT implementation as well as the security and organizational implementation of the systems also took place.

In 2019, the result products of the IJR project are the administrator and decision editing module, the introduction and organizational implementation of which is in progress. The leader of the Consortium (Ministry of Justice) initiated the extension of the project implementation period with the KÖFOP IH until 31 December 2020.

IX. Annexes

IX.1. The Financial Management of the NAIH in 2019

On the 31th December 2019, we closed the eighth year of operation and management of the National Authority for Data Protection and Freedom of Information. Hereafter, a brief overview of the data related to the financial management is presented.

IX.1.1. Revenue Appropriations and Performance Data in 2019

The NAIH budget for 2019, initial appropriation, was HUF 1,156,700,000, of which the special staff appropriation was HUF 747,400,000, health and pension levies HUF 128,400,000, supplies expenses HUF 255,900,000, and the accumulation-purpose appropriation HUF 25,000,000.

The adjusted appropriation for 2019 was HUF 1,476,792,000, including the original appropriation, the balance of 2018 including commitments of HUF 252,799,000, and the others revenue of HUF 21,190,000 from the EU project STAR I and II. Additional revenues included the other operation-purpose revenue of HUF 22,766,000. In addition, in 2019, there was revenue from the repayment of housing loan for accumulation purposes of HUF 336,000 and revenue related to the power of state (procedural fee) of HUF 498,000. The second advance of the KÖFOP project was realized in the amount of HUF 22,047,000. The wage compensation amounted to 456,000 HUF. The figures are shown in the following table:

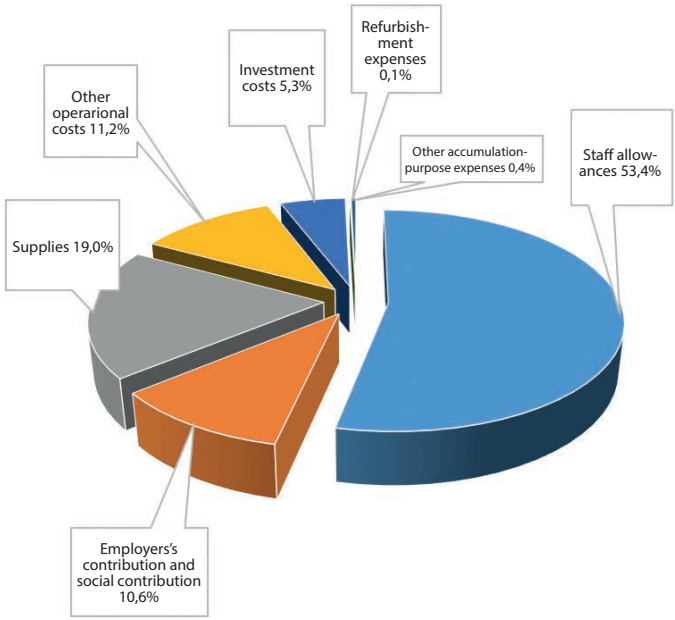
Denomination	Initial appropriation thousands	Adjusted appropriation	Performance	2019 balance including commitments
Initial appropriation	1 156 700			
Other operation-purpose subsidies (KÖFOP)		22 047	22 047	
Revenue related to the power of the state		498	498	
Exchange rate profit		1 519	1 519	
Damages payed by insurer		1 779	1 779	
Other operation-purpose revenue		19 468	19 468	
Other operation-purpose subsidies (STAR I&II)		21 190	21 190	
Repayment of housing loan for accumulation purposes		336	336	
2018 balance		252 799	252 799	
Central, governing agency subsidy	1 156 700	1 157 156	1 157 156	
From this: guaranteed wage minimum		*456*	*456*	
Total revenue appropriation	***1 156 700***	***1 476 792***	***1 476 792***	-
Staff allowances appropriationa	747 400	724 871	715 663	9 208
Employer's contribution and social contribution tax	128 400	143 307	141 557	1 750
Supplies expenses appropriation	255 900	322 925	253 929	68 996
Other operation-purpose expenses	-	150 410	150 410	-
Investment-purpose expenses	25 000	99 161	71 571	27 590
Refurbishment-purpose expenses		1 118	1 118	-
Other accumulation-purpose expenses		35 000	5 000	30 000
Expenses appropriation:	***1 156 700***	***1 476 792***	***1 339 248***	***137 544***

IX.1.2. Expense appropriations and performance data

The initial budget appropriation for 2019 was HUF 1,156,700,000. The adjusted expense appropriation was HUF 1,476,792,000, of which the performed staff allowances appropriation was HUF 715,663,000. The settled employer's contribution and social contribution tax were HUF 141,557,000. Expenditure on supplies totalled HUF 253,929,000, other operating expenses amounted to HUF 150,410,000, and the accumulation-purpose expenses were HUF 77,269,000.

The following graph shows the distribution of the performance of adjusted appropriations in percentages:

Distribution of completed expenditure appropriations in 2019



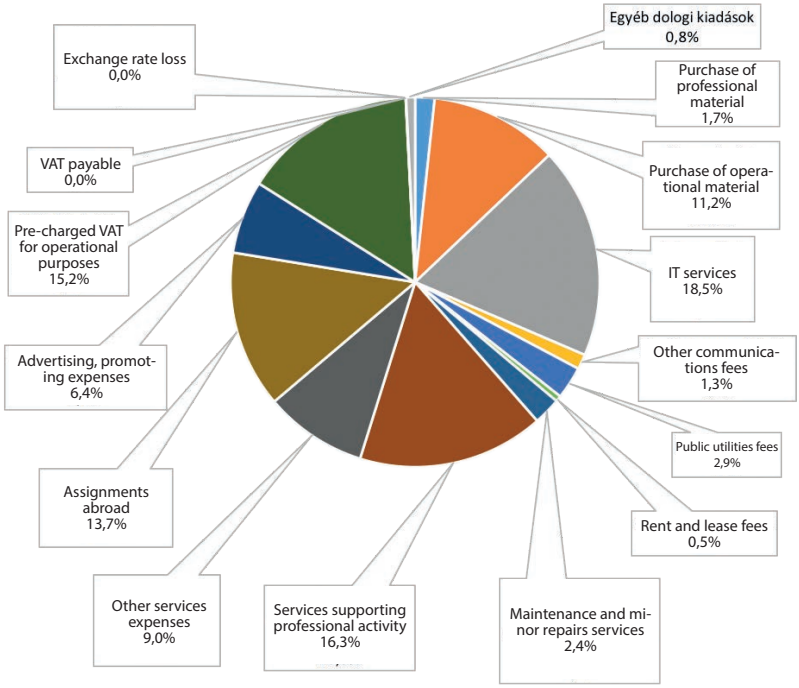
53,4% of the adjusted appropriations for 2019 were made in the form of personal allowances. The employer's contribution and social contribution tax was 10,6% of the total expenditure. The priority supplies appropriations amounted to 19% of the total adjusted budget. Accumulation-purpose expenditures amounted to 5,5% of the total budget. Other operating expenses were over 11%.

The balance of the Authority's core business in 2018 amounted to HUF 137,544,000, of which a balance of HUF 68,811,000 including commitments was generated.

IX.1.3. Distribution of Supplies Expenses

The following diagram shows the distribution of supplies expenses performed according to the order of headings in percentages.

The distribution of supplies expenses in 2019



The largest part of the material expenses is the expenses of the service supporting professional activities, which is HUF 41,430,000, i.e. 16%. Consulting expenses related to the KÖFOP 2.2.6-VEKOP-18 project significantly increased the amount of this expenditure category.

Pre-charged VAT for operational purposes - as our Authority is not in a reclaimable position - is 15% of the total material expenditure, which is HUF 38,648,000. Assignments abroad expenses in 2019 amounted to nearly HUF 35,000,000.

The value of operating materials was HUF 28,510,000, and for the use of IT services the Authority paid HUF 47,005,000.

In total, our Authority paid HUF 7,247,000 for public utility charges.

IX.1.4. Revenue from fines

The fine the Authority imposed and received amounted to HUF 112,734,000, which was entirely the proceeds of the central budget.

IX.1.5. Development of the Authority's staff

As of 31 December 2019, the number of staff of the Authority was 105. Our authority employs professionals with specific knowledge and skills, typically lawyers and IT specialists, whose expertise and experience have been valued significantly more in the labour market with the introduction of the GDPR in 2018 (similarly to other Member States). As a result, it is almost impossible to retain qualified professionals without providing an adequate level of competitive salaries. I should also be noted that, in the case of qualified professionals with outstanding experience in this field, the 'labour drain' effect on the labour market is not limited only to the private sector but also comes from some public sector employers able to provide more favourable employment conditions than the Authority. Unfortunately, due to these factors, the rate of labour migration from our Authority has recently increased. Nevertheless, our Authority strives to retain its workforce as possible.

IX.2. The Awardees of the NAIH Medal

On the basis of the Rules 19/2012 on the presentation of the 'Commemorative Medal of the National Authority for Data Protection and Freedom of Information', the Medal may be awarded to those who have achieved outstanding, high-quality, exemplary results in the field of data protection as well as the right to informational self-determination and freedom of information. The commemorative medal is made of silver, the work of master goldsmith Tamás Szabó. It is handed over annually, on the occasion of Data Protection and Freedom of Information Day.

On 25th January 2019, Dr. Attila Péterfalvi, President of NAIH, presented two awards.

One of the silver commemorative medals was awarded to Wolters Kluwer Hungary Kft. 'for its outstanding activities in promoting and disseminating legal knowledge related to the protection of personal data'.

Katalin Kézdi, Managing Director of Wolters Kluwer Hungary Kft., receives the Medal of the National Authority for Data Protection and Freedom of Information - Budapest, January 25, 2019

In 2019, another medal was awarded to Dr. Tamás Bendik, Chief advisor to the President of NAIH, an expert previously representing Hungary's position during the negotiations on data protection reform within the formations established by the European Union institutions (Council, Commission), 'for his outstanding work in the consistent representation of the Hungarian position in the process of adopting the EU data protection reform package, as well as the professional aspects during the related domestic legislative process'.

Dr. Tamás Bendik receives the Award of the National Authority for Data Protection and Freedom of Information - Budapest, January 25, 2019

IX.3. References to law and abbreviations mentioned in the report

- Accounting Act, Act C of 2000 on Accounting
- Act CLXI of 2011 on the organization and administration of the courts
- Act CXIX of 1995 on the processing of name and address data for research and direct marketing purposes
- Act CCXXXVII of 2013 on Credit Institution and Financial Enterprises
- Act LXIII of 1992 on Personal Data Protection and the Publicity of Data of Public Interest
- Act LXXVI of 1999 on Copyright
- Act XLII of 2015 on the employment of the professional staff of law enforcement agencies
- Administrative Procedure Act, Act CL of 2016 on the Code of General Administrative Procedure
- Ajbtv, Act CXI of 2011 on the Commissioner of Fundamental Rights
- BVOP: Hungarian Prison Service Headquarters
- Civil Code, Act V of 2013 on the Civil Code
- Company Act, Act V of 2006 on Public Company Information, Company Registration and Liquidation
- Complaints Act, Act CLXV of 2013 on complaints and notifications of public interest
- Condominiums Act, Act CXXXIII of 2003 on Condominiums
- Criminal Code, Act C of 2012 on the Criminal Code
- Designation Decree; Capital General Assembly Decree 20/2012 (14 March) on the performance of traffic management tasks in Budapest
- DPO: data protection officer
- EHSA: Electronic Health Service Area (EESZT: Elektronikus Egészségügyi Szolgáltatási Tér)
- EMMI: Ministry of Human Resources
- Environmental Protection Act, Act LIII of 1995 on the General Rules of Environmental Protection
- Fundamental Law, The Fundamental Law of Hungary (25th April 2011)
- Health Data Act: Act XLVII of 1997 on the protection and processing of medical and other related personal data
- Health Act: Act CLIV of 1997 on Health
- GDPR, General Data Protection Regulation: REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the

processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC
- Government Administration Act (Kit.), Act CXXV of 2018 on Government Administration
- ICO: Information Commissioner's Office in the UK
- Identification Act, Act XX of 1996 on the methods of identification and using of identification codes which replace the personal identification mark
- KNBSZ: Katonai Nemzetbiztonsági Szolgálat, Military National Security Service
- Kttv., Act CXCIX of 2011 on Public Service Officials
- Küt., Act CVII of 2019 on special status bodies and the status of their employees
- Labour Code, Act I of 2012 on the Labour Code
- Local Government Act, Act CLXXXIX of 2011 on the Local Governments of Hungary
- MLSZ: Hungarian Football Federation
- MNB: Hungarian Central Bank
- MOHOSZ: Hungarian National Fishing Association
- National Assets Act, Act CXCVI of 2011 on the National Assets of Hungary
- NBSZ: Nemzetbiztonsági Szolgálat, National Security Service
- OIF: Országos Idegenrendészeti Főigazgatóság, National Directorate-General of Aliens Policing
- Penalty Enforcement Act, Act CCXL of 2013 on the enforcement of penalties, measures, certain compulsory measures and administrative confinement
- Police Act, Act XXXIV of 1994 on the Police
- Police Directive, Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA
- Privacy Act, Act CXI I of 2011 on the right to informational self-determination and on the freedom of information
- Security Act, Act CXXV of 1995 on National Security Services
- SIS II, Regulation (EU) 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System

- SIS II Act, Act CLXXXI of 2012 on the Exchange of Information Framework of the Second Generation Schengen Information System, as well as the Amendment of Certain Policing Acts and thereby the Hungarian Simplification Programme X
- TAO Act, Act LXXXI of 1996 on corporate tax and dividend tax
- Taxation Act (applicable till 31 December 2017), Act XCII of 2003 on the Rules of Taxation
- Taxation Act (entered into force on the 1st January 2018), Act CL of 2017 on the Order of Taxation
- VIS Regulation, Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas
- Warrant Act, Act LXXXVIII of 2013 on the Warrant Registration System and the Search and Identification of Persons and Things

Other laws:

- Aarhus Convention on Access to Information, Public Participation in Decision-Making and Access to Justice in Environmental Matters (promulgated by Act LXXXI of 2001)
- Act CLV of 2009 on the protection of classified data
- Act CXXII of 2013 on transactions in agricultural and forestry land
- Act CXXX of 2010 on Legislation
- Act CXXXI of 2010 On Public Participation in Developing Legislation
- Act LXVI of 1992 on the Registration of Personal Data and Addresses of Citizens
- Act LXVIII of 1997 on the employment of judicial staff
- Act LXXXIV of 1999 on the Road Traffic Register
- Act XLI of 2012 on Passenger Transport Services
- Archives Act: Act LXVI of 1995 on Public Documents, Public Archives and the Protection of Private Archival Material
- Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II)
- Council Regulation (EU) No 1053/2013 of 7 October 2013 establishing an evaluation and monitoring mechanism to verify the application of the Schengen acquis and repealing the Decision of the Executive Committee of 16 September 1998 setting up a Standing Committee on the evaluation and implementation of Schengen

- Data Protection Directive, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
- European Data Protection Board Guidelines 3/2019 on processing of personal data through video devices
- Government Decision 1004/2016 (I. 18.) on the establishment of the annual development framework of the Public Administration and Public Service Development Operational Program
- Government Decree 42/2015 (III.12) on the protection of the IT system of financial institutions, insurance and reinsurance companies, as well as investment companies and commodity exchange service providers
- Government Decree 210/2009 (IX. 29.) on the Conditions for Conducting Trading Activities
- Government Decree 301/2016. (IX. 30.) on the amount of the cost reimbursement chargeable for performing a request for data of public interest
- Government Decree 311/2005 (XII.25.) on the Rules of Public Access to Environmental Information
- Government Decree 451/2016 (XII.19) on the detailed rules of electronic administration
- EMMI Regulation 39/2016 (21 December) containing detailed rules related to the Electronic Health Services Area (EHSA)
- IRM Decree 47/2007 (X. 20.) on free company information
- Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of ‚Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice
- Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and

amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011

- Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC

Contents

Nemzeti Adatvédelmi és
Információszabadság Hatóság

1125 Budapest, Szilágyi Erzsébet fasor 22/c
Postal address: 1530 Budapest, Pf.: 5

Tel: +36 (1) 391-1400
Fax: +36 (1) 391-1410

Internet: http://www.naih.hu
E-mail: ugyfelszolgalat@naih.hu

Published by: National Authority for Data Protection and Freedom of Information
Publisher: Dr. Attila Péterfalvi, President
Translation: Dr. Katalin Siklósi-Somogyi
Proofreader: Dr. Zsófia Tordai
ISSN 2064-3098 (Printed version)
ISSN 2064-3128 (Online)

National Authority for Data Protection and Freedom of Information

National Authority for Data Protection and Freedom of Information

1125 Budapest, Szilágyi Erzsébet fasor 22/c
Postal address: 1530 Budapest, Pf.: 5

Tel: +36 (1) 391-1400
Fax: +36 (1) 391-1410
Internet: http://www.naih.hu
E-mail: ugyfelszolgalat@naih.hu

Published by: National Authority for Data Protection and Freedom of Information

Publisher: Dr. Attila Péterfalvi, President
Translation: Dr. Katalin Siklósi-Somogyi
Proofreader: Dr. Zsófia Tordai
ISSN 2064-3098 (Printed version)
ISSN 2064-3128 (Online)