National Authority for Data Protection
and Freedom of Information

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

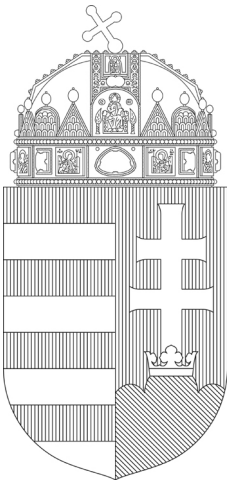
2020

Report of the
Nemzeti Adatvédelmi és Információszabadság Hatóság
(Hungarian National Authority
for Data Protection and Freedom of Information)

on its activities in 2020

B/14647

Nemzeti Adatvédelmi és Információszabadság Hatóság
(Hungarian National Authority for Data Protection and Freedom of Information)
Budapest, 2021.



Introduction

Greetings Dear Reader,

2020 marks the end of the first presidential mandate in NAIH's life. There is a separate chapter in this Report on the general experiences of the first nine years, but a few words about 2020 itself are also worth highlighting. The pandemic left its mark on the past year and it had a global impact on all aspects of life. This was no different in relation to informational rights either: the data protection authorities had to react to various challenges, thus NAIH also issued guidelines concerning digital education, mandatory measurement of body temperature and other restrictions related to the crisis situation. With regard to data in the public interest, NAIH received many requests and complaints, the access to data on the epidemic gave rise to many issues.

Mandatory distance work because of the epidemic in the spring, then the move from the Buda headquarters to Falk Miksa Street in September posed hitherto unprecedented challenges to NAIH's organisation, but we can now confidently say that our staff members successfully met these challenges and in the meantime gained valuable experience in the process that may be utilised in the future.

However, the two years since the start of applying GDPR brought about a kind of consolidation: work at the Authority and EU cooperation now run like a clockwork. At the same time, it is unfortunate that the EU data protection authorities do not use uniform case statistics, yet the main tendencies can still be demonstrated.

Finally, let us remember the change in regimes of 1989-1990. On 23 October 1989, Act XXXI of 1989 on the Amendment of the Constitution was promulgated. Amending the text of the former socialist Constitution, its Chapter XII on fundamental rights and obligations declared for the first time at the level of the fundamental rights that in the Republic of Hungary everybody had a right to the protection of personal data and to access and disseminate data in the public interest. The first data protection – freedom of information act was enacted in 1992; in 1995, the parliamentary commissioner responsible for the protection of personal data and access to data in the public interest was elected and the Office of the Data Protection Commissioner began its operation. The number of years that have passed – especially the 25th anniversary – deserve respect as well as a kind of reckoning, which is why we are looking forward to the ambitious project with high hopes to assess and improve the state of freedom of information in Hungary to be launched in 2020.

Budapest, ... March 2021

Dr. Attila Péterfalvi
Honorary university professor
President of
the Hungarian National Authority for Data Protection and Freedom of Information

I. Statistical data on the operation of the Authority

I.1. Statistical characteristics of our cases

The best way to illustrate the Authority's activities may be to monitor incoming cases by type of case and the related substantive and procedural law criteria. Having reviewed and supplemented the criteria developed over the past years in 2020, our case flow evolved as follows.

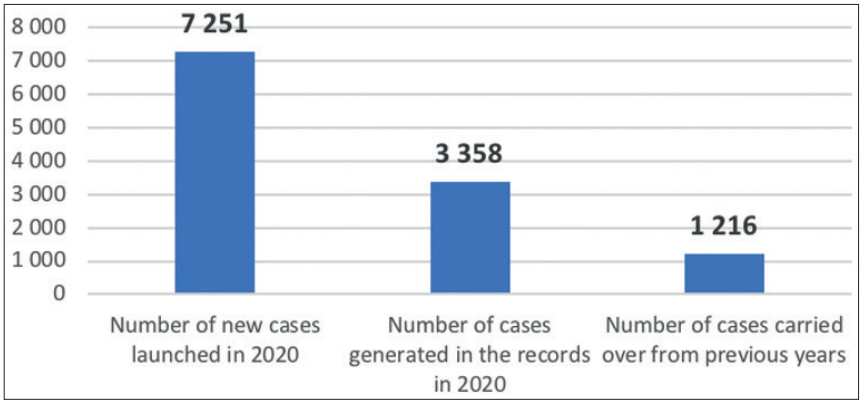
The Authority filed 7,251 new cases in its electronic filing system. Together with cases carried over from previous years (1,216), altogether 8,467 cases were in progress.

The number of documents received and filed in the transformed electronic registration system (Data Protection Officers Records) was 3,358.

In summary,, 10,609 cases were launched at the Authority in 2020, and including cases carried over from previous years altogether 11,825 cases were in progress.

The most spectacular change was in the decline in the number of submissions for consultation and the rise in the number of investigative procedures.

Number of cases before the authority in 2020

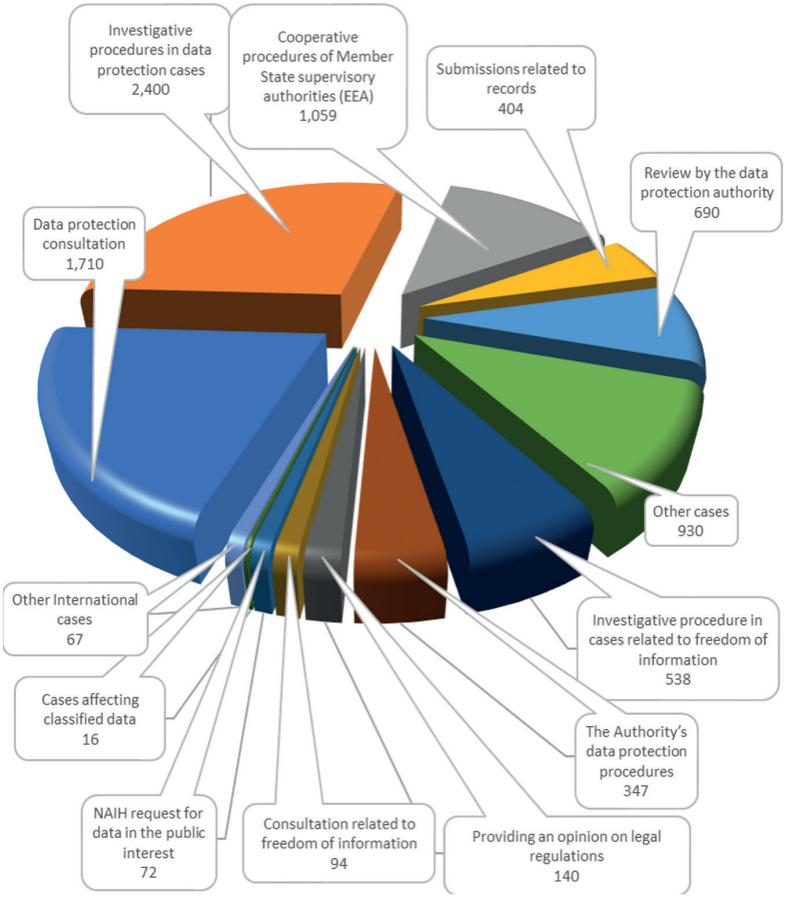


Number of cases before the Authority in 2020 (and their changes relative to 2018 and 2019) per case type

Case type	**2018**	**2019**	**2020**
Data protection consultation, request for an opinion	2,409	2,053	1,710
Investigative procedure in data protection cases	827	1,738	2,400
Cooperative procedures of Member State supervisory authorities (EEA)	606	1,158	1,059
Submissions related to records	1,305	745	404
Review by the data protection authority	234	568	690
Other cases	131	449	930
Investigative procedures in cases on freedom of information	375	325	538
The Authority's data protection procedures	67	276	347
Providing opinion on legal regulations	195	186	140
Consultation related to freedom of information	88	86	94
NAIH request for data in the public interest	74	73	72
Cases affecting classified data	15	14	16
Other international cases	85	13	67
Cases in progress in total:	**6,411**	**7,684**	**8,467**
Electronic reports received in the DPO records	1,786	4,796	3,358
Annual case number in total:	**8,197**	**12,480**	**11,825**

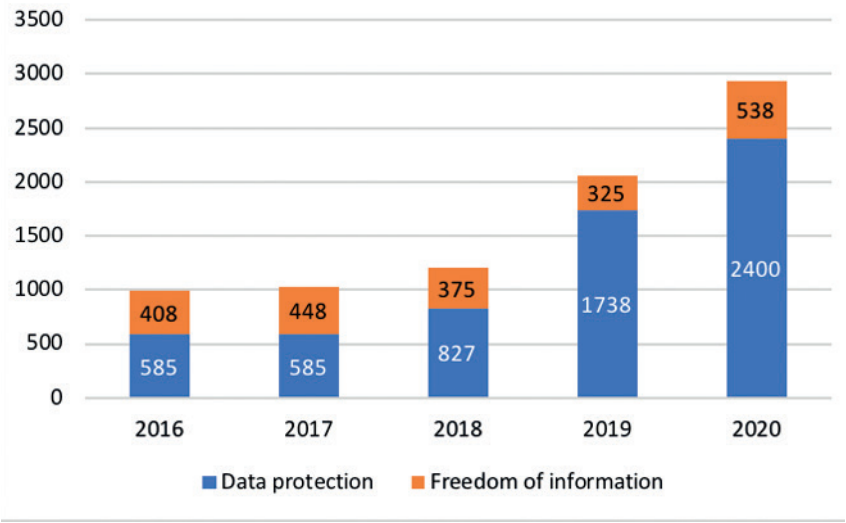
Cases in progress before the Authority in 2020

(without DPO records)



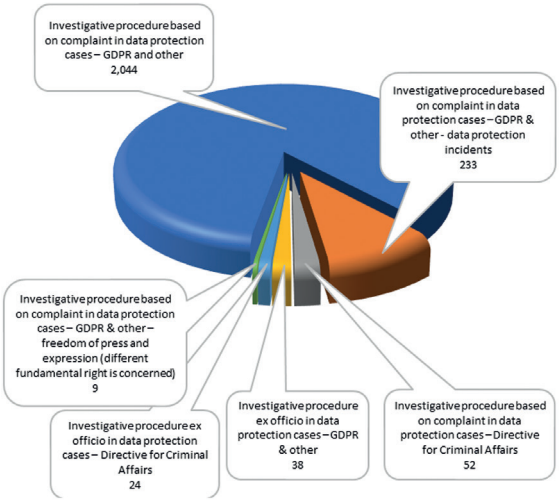
The number of consultation-type cases has shown a declining tendency year after year, while the number of data protection investigation-type cases has been rising since 2018. The following figures illustrate the continuous rise in the number of investigative procedures.

Number of investigative procedures



The following statistics present the number of cases in data protection investigative-type procedures in 2020 by case type:

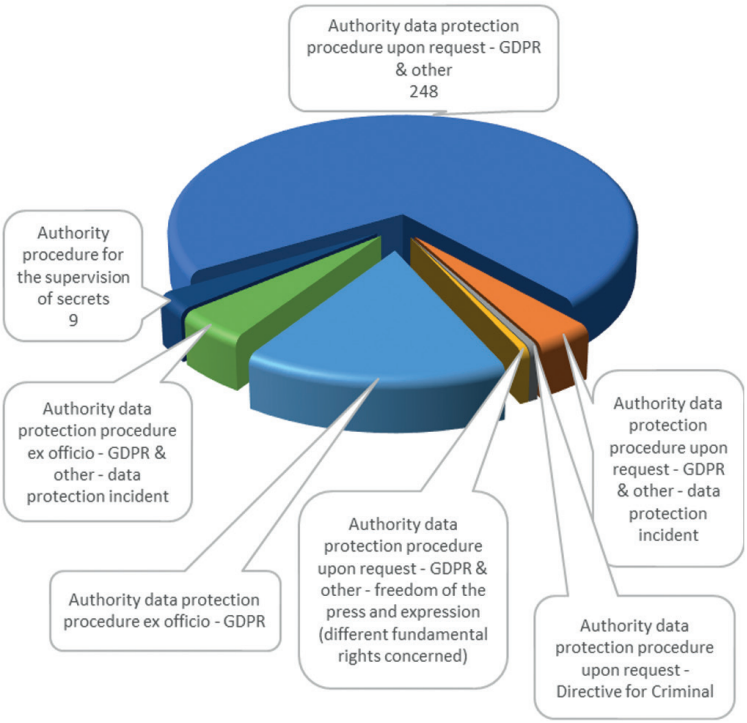
Data protection investigative-type cases by case type



The changes in the procedural environment since 2019 have resulted in a continuously rising burden on administrators. The number of authority procedures launched since the law amendments related to the data protection reform of the European Union increased further in 2020.

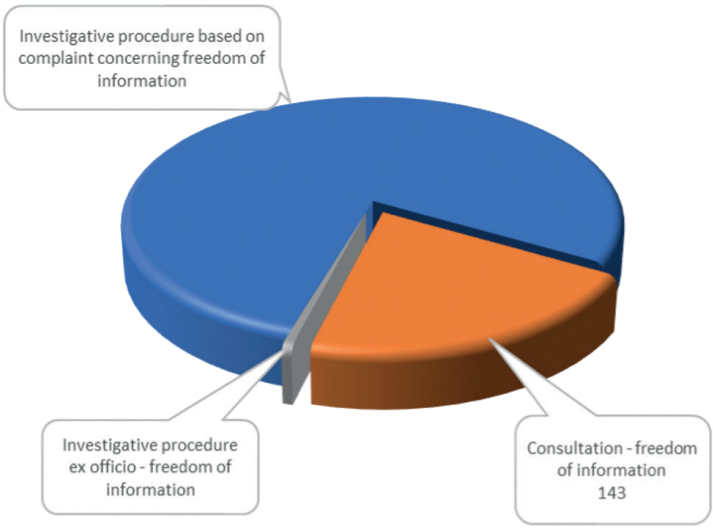
Case type	Number of cases
Authority data protection procedure upon request - GDPR & other	248
Authority data protection procedure upon request - GDPR & other - data protection incident	13
Authority data protection procedure upon request - Directive for Criminal Affairs	2
Authority data protection procedure upon request - GDPR & other - freedom of the press and expression (different fundamental rights concerned)	2
Authority data protection procedure ex officio - GDPR & other	57
Authority data protection procedure ex officio - GDPR & other - data protection incident	16
Authority procedure for the supervision of secrets	9
Authority procedures in total:	347

Authority procedures by case type



Case type	Number of cases in 2020
Investigative procedure based on complaint concerning freedom of information	534
Consultation - freedom of information	143
Investigative procedure ex officio - freedom of information	4
Freedom of information cases in total:	**681**

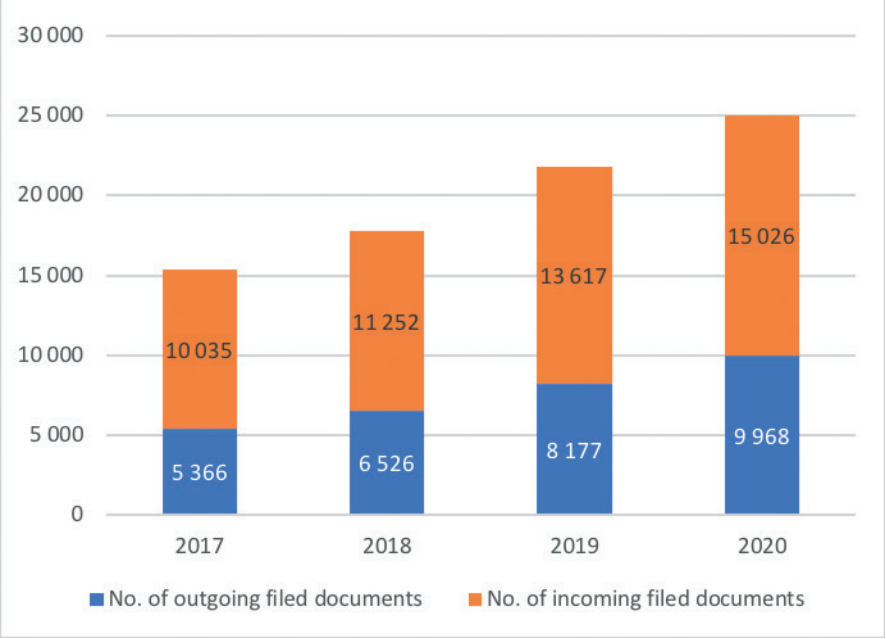
Freedom of information cases by case type



The ongoing increase in the number of cases can be established also on the basis of the Authority's document flow statistics.

Document type	2017	2018	2019	2020
Number of **outgoing** filed documents	**5,366**	**6,526**	**8,177**	**9,968**
Number of **incoming** filed documents	**10,035**	**11,252**	**13,617**	**15,026**

Document flow statistics



The pandemic caused by the coronavirus in 2020 had an impact on the customer service activities of the Authority. Relative to earlier years, the number of calls received by the telephone customer service increased (totalling 2,992), while uncertainties about data processing related to the pandemic could be seen also on the basis of the questions paused. The Authority assisted in the development of the lawful practice of controllers and processors with regard to these data processing operations through the information published in its website.

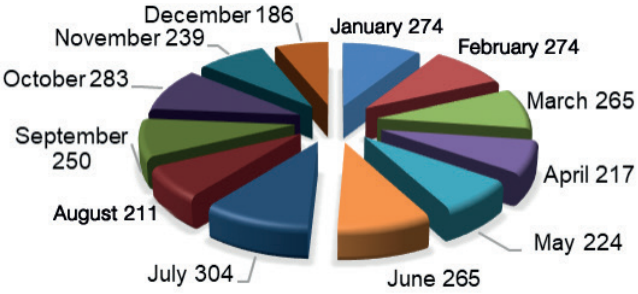
Outstanding interest was noted concerning the measurement of body temperature by employers and in schools, as well as the control of digital distance education and work from home.. With regard to the calls received in connection with data processing related to the webpage launched by the Government of Hungary at the end of the year, which allows registration for vaccination, the Authority provided assistance in exercising the rights of data subjects, including information on how to contact the data controller or how to initiate proceedings before the Authority.

The Authority continued to receive a number of calls, when data subjects asked for information about the legal possibilities available to them concerning the data transmission practice of claims management companies acting on the basis of assignment or commission, in the event that they were not appropriately informed, or not at all, on the circumstances of processing, the source of the personal data and the possibilities of exercising their data subject's rights.

Data subjects frequently requested information from the Authority about how they could enforce their right to the issue of copies within the framework of their access rights according to the General Data Protection Regulation. Beyond providing general information, the Authority usually called attention to the statements published in its website and the related decisions concerning the subject matter. Several questions were received also about the extent of the right to the issue of copies since exercising this right cannot have a detrimental impact on the rights and freedoms of others, providing the copy may only relate to the personal data of the data subject and does not automatically mean a right to copies of complete files or unedited video recordings.

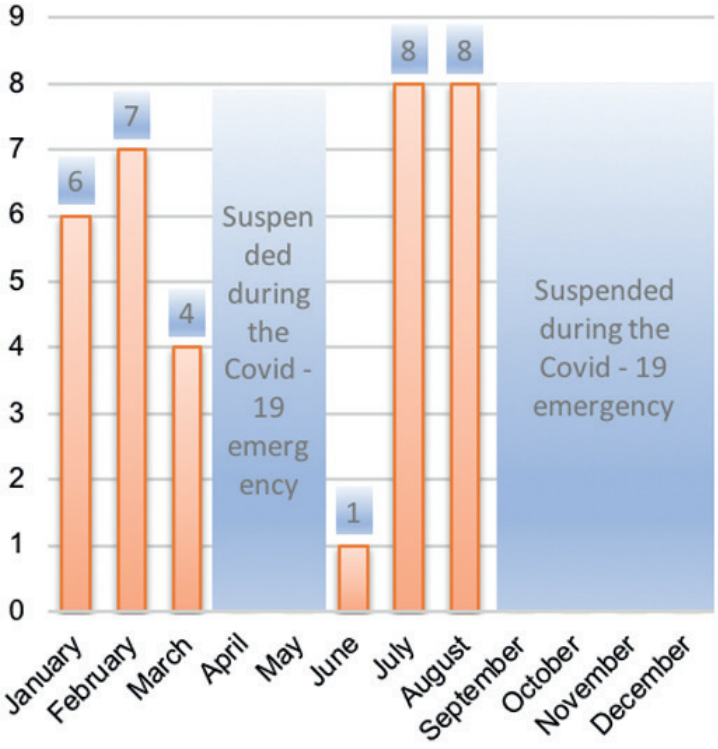
The Authority's customer service activities in figures:

Telephone customer service in 2020 (number of calls)



In view of the risks threatening customers and the Authority's staff, the personal customer service of the Authority was suspended. In the periods of the year when the personal customer service of the Authority was available, clients were received on 34 occasions. In 2020, the vast majority of the clients visiting the personal customer service desk exercised their right to inspect documents of the Authority procedures in progress.

Personal customer service in 2020 (no.)



Since its establishment, 8,890 reports were received by the Data Protection Officer Notification System of the Authority. The Authority registered 3,075 reports in 2020, in addition to the 180 cases requesting the erasure of notifications made earlier.

I.2. Annual conference of data protection officers

The President of the Authority convened the annual conference of data protection officers in November 2020. In accordance with the provisions of Section 25/N of the Privacy Act, the conference is called to assist in the regular professional contacts of the Authority and the data protection officers with the purpose of developing a uniform legal practice when applying the legal regulations pertaining to the protection of personal data and access to data in the public interest.

The law does not require the maintenance of professional contacts with the controller, but primarily with the data protection officers notified to the Authority currently by some 7,600 entities.

Once GDPR became applicable, training has to be made accessible to significantly more participants than before with a view to developing a uniform legal practice; as pursuant to the Privacy Act, all of them have a right to participate despite the epidemiological situation, so the annual conference of data protection officers was again administered exclusively electronically in 2020. By applying e-learning solutions, the conference may have contributed to a higher-level utilisation of the professional contents presented as the presentations can be viewed several times and they may be used even for internal training courses.
In the spirit of professional cooperation, the Authority also provided an opportunity for the data protection officers to shape the content of the presentations. The President of the Authority assessed the needs of the data protection officers, their professional expertise and their questions and problems related to data protection and the freedom of information in the wider community through an on-line questionnaire accessible from the invitation to the conference

I.2.1. The results of the preliminary questionnaire survey

The officers notified to the Authority reached the questionnaire almost exclusively (98.2%) through the link accessible from the e-mail inviting them to the conference, thus it can be assumed that the questions really reached the data protection officers. The Authority received 390 answers to the survey, roughly the same as in 2019, but in view of the increase in the number of notified officers, the number of those reached by the survey declined in proportion.

More than half of the voluntary respondents have been working on data protection and performing the tasks of data protection officers for one to three years, while

close to 13% have been involved in this field only for a few months. 33% of the respondents have been working on data protection for more than three years, showing an increase of 7% relative to last year's results.

This year, almost half of the respondents (49%) also discharges tasks related to freedom of information, so it can be assumed that most of them work in the public sector. At the same time, less than 9% of the respondents were notified by organisations performing data processing activities subject to the scope of the Privacy Act, so presumably the data protection officers of entities performing data processing for law enforcement, defence and national security purposes have not been reached by the survey or attracted less of their attention, hence their processing related issues could appear only moderately among the subject matters of the conference.

The results concerning to currency of the officers' knowledge revealed that relative to 70% of them in 2019, last year only 45% of the officers expanded their data protection knowledge through participating in one-day or multiple-day training courses; at the same time, the ratio of those participating in on-line training rose from 8% to 33.5%, presumably due to the pandemic. 22%, i.e. 89 officers again discharge their duties without having participated in any data protection-related training at all.

Did you participate in an organised data protection training over the past year?	Answers	Ratio
University	65	16.7%
Multiple-day course	77	19.7%
One-day course	96	24.6%
On-line	130	33.3%
Held by a superior entity/ parent company	32	8.2%
Neither	89	22.8%
Other...	13	3.3%

Two-thirds of the respondents were supported by their organisations in expanding their data protection knowledge characteristically by subscribing to professional content for them, while the support for participation in organised training courses declined by 12% relative to 2019.

Did your organisation support the expansion of your data protection and data security knowledge?	Answers	Ratio
Through paid time off work	64	16.4%
Through internal training	57	14.6%
Through organised training	119	30.5%
Through subscription to professional content	76	19.5%
Neither	125	32.1%
Other...	27	6.9%

More than 67% of the respondents were informed of the change in the seat and mailing address of the Authority as of 26 October 2020 before filling in the questionnaire. With regard to the knowledge that they can obtain independently, it is noteworthy that 76% of the respondents already read the guidance issued by the Article 29 Data Protection Working Party on data protection officers, but more than half of them did not (20%), or only glanced through (33%) the 2019 annual report of the Authority. There was, however, a slight increase in the number of officers visiting the Authority website weekly or more frequently (from 40% to 46%) relative to last year.

How often do you visit the www.naih.hu website?	Answers	Ratio
Weekly or more frequently	179	45.9%
Monthly	129	33.1%
Rarely	70	17.9%
Never	12	3.1%

Although in addition to data protection news of other Member States, guidelines on consent according to GDPR became also accessible for the first time in the European Data Protection Board's website (as draft guidelines published for public consultation with a view to the post-GDPR development of a uniform legal practice) 48% of the officers continue to visit this website less frequently than monthly. It is, however, a positive development that this ratio shows an improvement of 12% relative to the 2019 data as then 60% failed to visit the website even monthly.

How frequently do you visit the website of the European Data Protection Board?	Answers	Ratio
Weekly or more frequently	77	19.8%
Monthly	124	31.9%
Rarely	139	35.7%
Never	49	12.6%

Data processing activities in connection with the corona virus were also in the focus of the Authority's 2020 activity; the Authority endeavoured to enhance data protection awareness by issuing several information reports. A large number of the respondent data protection officers, close to 76% of them, read the Authority's information concerning this topic, which can be regarded as particularly significant because close to 56% of the entities appointing/entrusting them conducted temperature measurements of the persons entering their building/premises.

In terms of the officers' activities, the percentage almost identical to last year's figures shows that a significant majority fulfil their advisory tasks to controllers or processors and staff conducting processing work and typically the management of their organisations request their professional opinion, as defined under GDPR Article 39. Similarly to last year's results, the majority, however, did not conduct any audit related to internal data protection compliance, or if they did, it was not documented, and no plans were made in relation to the audit activities, which could improve the enforcement of the principles of accountability, as well as the level of data protection awareness and transparency within their organisation ever since their appointment.

Since your appointment as data protection officers, have you	Yes	No
provided an opinion on draft internal rules concerning the processing of data?	348 (89.2%)	42 (10.8%)
received an invitation from the head/management of the organisation to state your position concerning an issue related to data processing?	361 (92.6%)	29 (7.4%)
produced an internal audit plan?	167 (42.8%)	223 (57.2%)
conducted a documented internal audit?	158 (40.5%)	232 (59.5%)

The answers demonstrated that close to 75% of the respondent officers already held data protection awareness training, while close to 59% data security awareness training at the organisation and that requests for data protection impact assessment have not yet arisen in many places.

Since your appointment as data protection officers, have you	Yes	No
held data protection awareness training?	290 (74.4%)	100 (25.6%)
held data security awareness training?	228 (58.5%)	162 (41.5%)
contributed to drafting an answer related to the exercise of data subject's rights?	239 (61.3%)	151 (38.7%)
contributed to the management of a data protection incident?	183 (46.9%)	207 (53.1%)
conducted data protection impact assessment?	184 (47.2%)	206 (52.8%)

In addition to the above, data protection officers were encouraged to provide feedback concerning the presentations of the 2019 conference, which showed that they were adjusted to the average level of preparedness of the participants. The Authority took the questions and feedback received into account when compiling new training materials.

As to NAIH's 2019 online conference for data protection officers...						
	1	2	3	4	5	
I have not seen its materials	70	53	111	75	78	I have seen all the videos and documents
there was nothing new because of my work	29	77	205	64	12	most of the materials were new to me
it was about too fundamental issues	16	64	281	21	5	it was too complicated, difficult to follow

I.2.2. Electronic training materials of the conference for data protection officers

On 23 December 2020, the President's welcoming address and ten training videos were published under the aegis of the conference on an independent platform created on the Authority's website. The Deputy President of the Authority and members of the staff gave presentations on the experiences of the data protection issues of 2020 and the position taken by the Authority in many cases through practical examples in presentations that lasted close to an hour longer than during the conference last year.

Following the welcoming address of the Authority's President, dr. Ibolya Tóth, head of division at the Department of Certification and Social Relations, presented the guidance drafted by the Authority concerning data processing related to the corona virus and published on its website and spoke of some of the specific questions received from controllers, processors and data subjects (for instance in relation to employment relationships or the transfer of the results of PCR tests).

In terms of the accessibility of data related to the coronavirus pandemic, dr. Éva Tóth, an investigator of the Department for the Freedom of information, presented the Statement of the International Conference of Information Commissioners on the evolution of the right to access information in the public interest during the period of the pandemic and reported on the derogations from the general rules of requesting data and presented the relevant cases before the Authority (disclosure of the fact of infection, disclosure of information on the control of the pandemic and disclosure of financial management data in relation to the corona virus pandemic).

Based on a prior survey, 68.5% of data protection officers discharged their tasks at controllers or processors where video surveillance or video recording is in place, and as the finalised version of Guidelines 3/2019 of the European Data Protection Board on processing of personal data through video devices was adopted early in 2020, hence the central theme of the annual conference was video surveillance.

Krisztián Pataki, data protection expert of the Deputy President's Cabinet, presented the most important provisions of Guidelines 3/2019 of the European Data Protection Board; after this, dr. Gergely Barabás, Chamber counsellor, outlined the challenges of interest assessment and compliance with the principle of accountability in relation to data processing using video devices.

Dr. Szilvia Horuczi, data protection expert for the Department for Licensing and Incident Reporting, explained the rules of video surveillance at workplaces, mentioning the sectoral rules relevant for data protection, the decision of the Constitutional Court and the provisions of GDPR (highlighting the expectations and requirements related to the purpose of processing, its legal basis, the principles of data protection and those related to providing information in advance).

Dr. Róbert Fischer, data protection expert with the Regulatory and Secret Supervisory Department, delivered the presentation on the rules of video surveillance in public areas, discussing the rules applicable to the agencies authorised to survey public areas by individual legal regulations (most of which are required in relation to data processing purposes subject to the Privacy Act) and called attention to the need to develop adequate data security measures, while also discussing good practices.

Dr. Attila Kiss, head of the Department for Certification and Social Relations, provided information on the lawfulness of data processing through video devices in the light of a few requests for consultation received by the Authority. He also spoke about the fake cameras and the so-called “household purpose” data processing as exceptions from the application of the data protection requirements and outlined the fundamental data protection expectations in relation to video surveillance. After this, he presented the position of the Authority concerning the use of traffic surveillance cameras in the absence of express legal requirements based on specific requests, he spoke of a few submissions related to body cameras and the most important information concerning video surveillance in condominiums.

Another important topic in 2020 was the relevant judgment of the Court of Justice of the European Union and its impact on transferring data to third countries. In view of this, the Deputy President of the Authority Dr. Endre Győző Szabó presented the sections of GDPR related to transferring data to third countries, the Commission’s “Safe Harbour” decision, the Schrems I judgment, the “Privacy Shield” decision of the Commission and the Schrems II judgment examining it and their impact on international data transfers and the related challenges.

In relation to data protection incidents, Dr. Dániel Eszteri, head of division at the Department for Licensing and Incident Reporting, presented a few important decisions of the Authority concerning data protection incidents (for instance, the Authority’s procedure No. NAIH/2020/952 related to medical findings and referrals, which could be accessed and downloaded by the public through the website of the controller and a procedure currently in progress under No. NAIH/2020/1160 before the Authority, initiated by an Internet service provider).

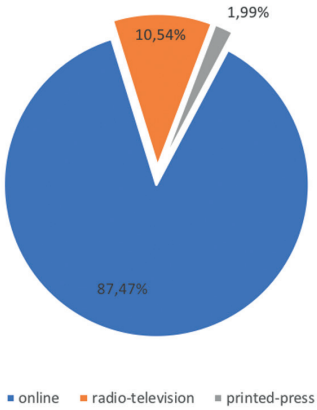
Finally, Renáta Nagy, project assistant at the Department for the Freedom of information briefly summarised the publication "*GDPR simply for small and medium-sized enterprises*", the SME manual, produced with a view to supporting small and medium-sized undertakings (SMEs) in their data protection compliance.

The videos will remain in the website of the Authority and they can be played using the MTVA Médiaklikk streaming service – so those viewing the videos will not become subjects of data processing in any third country – while the presentations are expected to remain available for downloading from the website of the Authority.

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

Below, we summarise the Authority's media appearances in 2020. Between 1 January and 31 December 2020, members of the media published altogether 854 news items about the Hungarian National Authority for Data Protection and Freedom of Information. As to the types of media, most of the time news on the activities of the Authority were broadcast by the online media altogether on 747 occasions (87.47%). NAIH was presented in the printed press in 90 cases (10.54%) and in 17 cases (1.99%) in the electronic media.

Share of NAIH's appearances in the various media in 2020



Source: Observer Budapest Médiafigyelő Kft.

II. Application of the General Data Protection Regulation

II.1. Data protection cases

II.1.1. The Authority's guidances related to the coronavirus and its procedures and consultations on corona virus-related data processing

In the course of the first and second waves of the coronavirus pandemic, the Authority published several position papers and guidances on its website in order to improve data protection awareness.

1. The scope of its first *Guidance on Data processing related to the coronavirus* published on 10 March 2020[1] extended to data processing operations related to employment relationships and third persons outside employment (for instance, customers) and those participating in health care in the context of the coronavirus pandemic. In terms of its subject matter, the guidance extended to questionnaires compiled by employers and to be completed for the purpose of infection risk assessment as well as the use diagnostic devices. In terms of employment relationship, the guidance expressly underlined the importance of the obligation to cooperation also on the part of employees.

As a main rule, the provisions of the General Data Protection Regulation apply in the course of data processing related to the coronavirus pandemic, of course excluding data processing for the purposes of law enforcement, defence and national security by the agencies authorized to do so. The Authority formulated similar expectations from a data protection viewpoint with respect to data processing operations related to those in an employment relationship, as well as third persons and customers in these guidances.

In general, the controller is expected to comply with the principles of accountability, lawfulness, purpose limitation, data minimisation, accuracy, data security, prior information of data subjects and other data protection requirements, including for the processing of data related to the coronavirus.

It is a general expectation, applicable also to data processing related to the coronavirus, that the controller comply with the principles of data processing, in particular the requirements of accountability, lawfulness, purpose limitation, data

1 https://www.naih.hu/files/NAIH_2020_2586.pdf

minimisation, accuracy and data security and it also has to provide information on data processing to data subjects in advance and meet the other data protection requirements as well. In relation to enforcing the principle of graduality, the guidance states that the controller has to endeavour to choose solutions that do not require data processing (thus, for instance, hygienic measures, ongoing use of disinfectants), and he has to opt for methods that minimise intrusion into the privacy of the data subject.

Questionnaires may be completed by the employer in the event of suspected exposure, inter alia, due to the location, date and time of travel, even for private purposes, or contact with persons arriving from certain countries. The employer, however, may not ask for data concerning health history and may not require the enclosure of health documentation. In order for such data processing to be lawful, a condition according to GDPR Article 9(2) must obtain in the case of health-related data in addition to the legal basis according to GDPR Article 6(1), such as meeting the employer's obligations arising from legal regulations regulating employment (particularly the provisions of the Labour Code).

The legal basis of screening tests using diagnostic devices (e.g. thermometer) applied not as a condition of entry, i.e. not as a shell protection measure, has to be chosen in accordance with the above, provided that such tests may be carried out only by , or under the professional liability of a health care professional. In addition, the employer may have access only to the results of the test and it is inconsistent with the data protection requirements to impose them generally on all employees, except for those employed in jobs with higher risk of exposure, such as those in customer service employees.

The guidance identifies health care providers (such as plant physicians) as independent controllers, who are authorised to process personal data according to the health care legal regulations and procedures in force applicable to them.

Finally, the Authority also discussed the rights and obligations of employees underlining that pursuant to Chapter III of the General Data Protection Regulation the employer has to ensure the exercise of data subject's rights. Moreover, it can be inferred from the obligation to cooperate in employment relations and the principles of bona fide actions and fairness that employees also have an obligation to inform the employers. Non-compliance with epidemiological measures may result in accountability according to criminal law; in relation to this, the guidance expressly mentions that the police may use a wide range of evidence in the

course of its related procedures, including the recordings of surveillance cameras in public areas.

2. The second guidance on '*The data protection and data security aspects of digital distance teaching*'[2] published on 30 September 2020 focuses on the processing of the personal data of students and teachers as data subjects and to assist controllers, it expressly mentions a few data security measures as "good practices". In relation to data processing related to students, the Authority expressly highlighted that the personal data of children are guaranteed specific protection in data protection regulations.

In the case of students, the name and other identification data, the content of reports, contributions in class and examination results qualify as personal data. In the case of teachers, their voice and facial images in relation to what they say in class and the data concerning their workplace activities are all personal data. The purpose of digital distance education is to ensure the continuity of school education as a public duty specified in law. Hence, the related processing of data is necessary for the discharge of public tasks [General Data Protection Regulation Article 6(1)(e)], so it is not based on the consent of the data subject. In relation to these processing activities, it is not the teacher that qualifies as controller, but the institution of education or the school district. A school district may qualify as controller if it sets specific data processing purposes in relation to the data of the students.

In addition, teachers have an obligation of confidentiality with regard to the data they learn about the students. The situation of controllers was definitely not made easier by the fact that the detailed rules of digital distance education were not settled by any legal regulation at the time of the publication of the guidance; in this area, however, it would be justified to regulate the circumstances of mandatory data processing in accordance with Section 5(3) of the Privacy Act.

The principles are expected to be taken into account and compliance with them to be demonstrated in the case of data processing in connection with digital distance learning, for which the controller is responsible. Thus, for instance, based on the principle of data minimisation, if a student has to verify that he completed a school task (primarily a practical exercise) with a video recording, it is an expectation that no person other than the student should be seen and as little as possible is shown from the student's home and private space. It is necessary also in digital distance education to endeavour to choose first and foremost instruments that

2 https://www.naih.hu/files/Tajekoztato-a-digitalis-tavoktatas-adatvedelmi-vonatkozasairol_2020-09-30.pdf

do not require data processing or, if that is not possible, solutions that are less risky for the privacy of the data subjects (for instance, on-line video chat instead of uploading video recordings, or the real time streamlining of classes should be chosen).

Controllers have an obligation to provide information about the circumstance of data processing related to digital remote education to data subjects (with the content according to GDPR Article 13) and to ensure the exercise of their rights as data subjects to them (or to their legal representatives). For instance, in the event of an objection of a student, the controller must consider whether an instrument or processing method that is softer and less restrictive of the privacy of the concrete data subject can be applied to achieve the purpose of processing. Thus, for instance, in the case of a class or lecture streamed online, the objection of a person participating in it should be evaluated so that the processing should not be riskier for him than his personal participation in a traditional class (see: setting up the camera), this, however, must not lead to preventing the institution of education from discharging its public duties in the form of digital distance teaching in general.

Finally, the guidance mentions a few data security measures as good practices in accordance with the guidance issued by the Polish data protection authority, such as the creation of work e-mail addresses for teachers, but not within the educational framework, for communicating through Internet interfaces, or that teachers have to comply with the fundamental security requirements even if using their own devices.

3. The Authority received a number of requests for consultation about the measurement of body temperature and other data processing issues related to the coronavirus. Controllers from both the public and the private sector asked largely about data protection issues related to the measurement of the body temperature of persons in a legal relationship with them or others (customers) entering their premises, which the Authority responded to in general in its *guidance on the measurement of body temperature* published in the autumn, but also reacted specifically in its answers to individual questions.

The purpose of drafting the third guidance, published on 14 October 2020[3], was to define the expectations, devices and requirements necessary for compliance with the principles as set forth in the first guidance, in particular for the suitability of the device and to review compliance with the requirements of necessity and

3 https://www.naih.hu/files/NAIH-2020-7465.pdf

proportionality in relation to the generally mandated, universal body temperature measurement.

As the Hungarian legal regulations require that the provisions of the General Data Protection Regulation are applied to data processing operations carried out with non-automated means, the Authority found it important to underline that checking body temperature using analogue and digital thermometers also qualifies as data processing. The document presents the conditions which – if fully met – the measurement of body temperature of all persons entering the premises of the controller appropriate for the purposes of the data protection principles:

- in the course of entry to the premises of the controller;
- as a uniform protective measure for every person intending to enter ("shell protection");
- not linked to the identification of the person subject to the body temperature check for the explicit purpose of this processing, and
- it does not involve the recording, storage or transmission of data in any way.

Also in relation to this data processing, the Authority declares that compliance with the principles of data protection, in particular the principle of accountability, is the responsibility of the controller.

4. In its answer to a consultation question concerning *the results of PCR and other infection tests and transferring them to third persons*, the Authority attached importance to underlining that the result of the test – whether positive or negative – qualifies as *health data* constituting a special category of personal data; when transferring it the controller is responsible for choosing and applying the appropriate legal basis and the related higher level data security requirements.

Another question concerned whether an employer can process the personal data of a relative and a fact of infection, if a relative of an employee is infected, or whether the employer may disclose the name of the coronavirus infected employee and the fact of the infection to the other employees. In response to the first question, the Authority stated that the employer is authorised to obtain knowledge only of the fact whether his employee was in contact with a person infected or potentially infected by coronavirus (for instance a person subject to official quarantine) as in the knowledge of this fact he can take the necessary steps to protect the employees, but there is no need to identify the infected person who had contact with the employee, or to specify the kinship between the person and the employee.

The Authority's position concerning the second question was also similar, i.e. it did not regard sharing the name of the infected colleague with the other employees as necessary to achieve the purpose.

The Authority received questions also in relation to the sample certificate published on the official Government website applicable to *the minimum data content of the certificate of exemption from the curfew for the purposes of performing work,* which entered into force on 11 November 2020. As to whether an employer may process the number of the ID card of an employee, the Authority stated that the relevant government decree does not require the recording of the ID card number by the employer, hence it does not create a legal basis for its collection and processing. As it is possible to issue the certificate in a way that the employer should not become the controller with regard to the ID card number – for instance, the certificate can be issued so that the employer only fills in the data that it lawfully processes, and the employee enters the ID card number, or the certificate is completed by the employee and the employer only requests the employee to show the certificate in order to check whether it was correctly completed – the processing of the additional data can be avoided.

5. In relation to the coronavirus pandemic, inter alia, the following cases were in progress before the Authority in 2020:

5.1. Several complaints were sent to the Authority against a business organisation operating a website functioning as webshop selling face masks and other devices facilitating protection against the coronavirus (e.g. salt pipe or air purifier device) that also collects donations for a foundation:

a) A complainant mentioned in his letter to the Authority that currently face masks are sold at tenfold the price in many cases. In addition, he underlined that neither any general terms and conditions of contract, nor any privacy statement can be accessed on the website (NAIH/2020/3216).

b) According to a complaint, despite the fact that the complainant had not earlier had any contact with the business organisation, the company sent promotional materials to his private e-mail address and phone number. According to his position, the data protection practice of this company qualifies as unfair (NAIH/2020/3247).

c) In another complaint (NAIH/2020/3088) the complainant objected to receiving information in a text message in relation to the website ("Let us take care of one another! With joint forces we can slow the spread of the virus. For further information visit the [name of website]. Regards, the team of [name of website]"), in spite of the fact that he had not made his personal data available to the business organisation.

In view of the above case, the Authority launched an investigation against the controller (NAIH/2020/5147) ex officio, which is currently still in progress.

5.2. In case NAIH/2020/3467, the complainant objected to the data processing of the mayor's office of a Budapest district in relation to providing health masks for residents above the age of 65. According to the complainant, GDPR Article 6(1) (d) referred to in the Privacy Statement attached to the mask delivered to him does not allow a Member of Parliament representing this area currently in office to send him a newsletter.

In their answer sent to the Authority's questions, the Mayor's Office informed the Authority that Section 2(2) of Government Decree 46/2020. (III.16.) on the measures to be taken in the event of an emergency declared to safeguard the health and life of Hungarian citizens, concerning the prevention of a human epidemic causing mass disease and the avoidance of its consequences, which endangers the safety of life and property, made it the mandatory duty of mayors to take care of persons above the age of 70. In practice, this care means providing them with food, medication and handling of postal payments, regulated under the so-called home assistance programme. In view of the fact that Hungary's Government highlighted and regarded the ongoing provision of information to the residents as a task of outstanding importance, the mayor of the district decided to distribute health masks to the district residents above the age of 60 together with an information leaflet containing important points to know about protection, prevention and compliance with hygiene requirements.

In addition to the mask, every envelope contained a statement on data processing, instructions for use, information material called "[name of the district] Info", a letter seemingly jointly signed by the mayor and the Member of Parliament for the district, with a general form of address, not including any name.

According to Section 5 of the statement on data processing sent by the Mayor's Office to the Authority, the legal basis of data processing was Article 6(1)(d) of the General Data Protection Regulation, i.e. vital interest of the data subject or another natural person.

In relation to this, the Authority made the Mayor's Office aware of its position, according to which the legal basis of the vital interest of the data subject may be used primarily, when there is no other legal basis for processing. If processing the personal data is necessary to protect the vital interests of several data subjects, then for instance the discharge of public duties [GDPR Article 6(1)(e)] may be the appropriate legal basis.

Act III of 1993 on Social Services Administration and Welfare Benefits (hereinafter: Welfare Act) makes the state and the municipalities responsible for the provision of basic social services. According to Section 57(1)(d) of the Welfare Act, home assistance qualifies as basic welfare service. According to Section 63(3) of the Welfare Act, assistance for the prevention of the evolution of emergencies and in averting an established emergency must be provided within the framework of home assistance. Because of the above, the legal basis indicated in the statement on data processing sent to the data subject, i.e. the protection of the vital interests of the data subject or another natural person according to GDPR Article 6(1)(d) of the General Data Protection Regulation, was not correct. This, however, does not mean that the data processing did not have a legal basis because in actual fact the legal basis was the public duty specified in Section 63(3) of the Welfare Act, assistance in reverting the established emergency, i.e. GDPR Article 6(1)(e).

In view of all this, the Authority recommended that if the Mayor's Office intends to carry out such data processing activities in the future, particularly with respect to the second wave of the epidemic, it should refer to the appropriate legal basis.

5.3. Cases NAIH/2020/3204 and NAIH/2020/3299 were subject to similar legal assessment because of the similarities of the facts of these cases, in which the complainant objected to having received calls to his confidential landline and mobile phone numbers, in which he was given information on the most important details of the curfew imposed by the Government.

The Authority responded by informing the complainant that Hungary's Government launched a comprehensive information campaign on 29 March 2020 in order to notify every Hungarian citizen of the most important details of the curfew, which included short television spots, outdoor posters and videos on the Internet, but they also contacted Hungarian citizens by phone.

These phone calls were not marketing calls linked to any political party, but information on the Government's measures introduced under its decree 71/2020 (III.27.) on the curfew, in order to prevent a human epidemic and averting its consequences to protect the health and life of Hungarian citizens.

Pursuant to Article 6(1)(e) of the General Data Protection Regulation, the processing of personal data is lawful, its processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, accordingly, the provision of information by phone under the above measures of the Government and the processing of data in this context were also legitimate.

Furthermore, the complainants were given information about the possibilities of exercising their data subject's rights and, in this context, also about that under Section 1(2)(b) of Government Decree 179/2020. (V. 4.) on derogation from certain data protection and data request provisions during the state of emergency, all the measures to be taken based on a request submitted to the controller to exercise the rights according to Articles 15-22 of the General Data Protection Regulation with respect to the processing of personal data processed for the purposes of preventing, detecting and averting the spread of coronavirus infections shall be suspended until the termination of the state of emergency; the starting day of the period open for such measures shall be the day following the day of the termination of the state of emergency. Data subjects shall be notified of this immediately following the termination of the state of emergency, but within ninety days from receipt of the request at the latest.

II.1.2. Personal data processing through video devices in the practice of the Authority

The experiences of procedures to investigate data processing through video devices constitute a classic topic in the Authority's reports, as this is a widely used data processing activity affecting many, and due to the fact that cameras are easy to access and easy to operate, it leads to an increasing number of complaints on the part of employees, as well as the neighbours of controllers applying video surveillance, as well as other data subjects.

The topicality of this issue is due to the adoption of Guideline 3/2019 on processing of personal data through video devices[4] of the European Data Protection Board (hereinafter: Guideline) adopted on 29 January 2020, in addition to the number of complaints received from complainants and requests by controllers for consultation.

1. *Guidelines of the European Data Protection Board on processing of personal data through video devices*

Since the General Data Protection Regulation became applicable on 25 May 2018, the Hungarian regulatory environment of video surveillance changed on a number of points, and former provisions, which restricted the requirements of the regulation or appeared to be contrary to it for other reasons were annulled. In the absence of unambiguous legal provisions it was rather difficult for a wide

4 The Guidelines are accessible also in Hungarian through the following link: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201903_video_devices_hu.pdf

range of persons operating video surveillance systems for a purpose subject to the General Data Protection Regulation based on the legitimate interest of the controller – including condominiums and housing cooperatives, shopping malls, passenger transport service providers or employers – for instance to specify the duration of processing necessary for the purpose of data processing, to appropriately document the conduct of the interest assessment test required for applying such a legal basis, moreover in some cases even to choose the legal basis of data processing.

The Guidelines adopted after extensive preparations and the decision on the cases brought before the data protection authorities in line with the Guidelines present the requirements for video surveillance and recording, involving the processing of any personal data subject to the General Data Protection Regulation (i.e. processing not for law enforcement, defence or national security purposes), irrespective of the technological solution employed. The Guidelines provide guidance on how to distinguish camera surveillance in the home or under the private-only exception from activities that are already covered by the Regulation (e.g. surveillance extending beyond one's own property, an area in joint ownership or some public area) and therefore subject to the obligation to apply the data processing requirements.

In addition the Guidelines discuss the criteria of compliance with principles; the possible legal bases; the expected technical and organisational measures; the obligation of the controller to provide information and the criteria of ensuring the exercise of data subject's rights (in particular, the right to access). Therefore, it does not only provide guidance on the use of video devices for asset protection purposes, but can also be used as a general tool for surveillance and recording video devices used for other purposes, in order to develop the data processing practices required by the Regulation for any category of persons.

In addition, it is important to underline that the Guidelines emphasise that the controller, when choosing the technical solutions and devices to be used, should choose technologies that are advantageous from the viewpoint of protecting privacy. Such technologies include, for instance, those which enable masking or distorting the areas and third persons irrelevant from the viewpoint of the surveillance in the images prior to transferring the video recording to the data subjects in the context of the right to access according to Article 15 of the General Data Protection Regulation. Also, the solutions chosen may not contain unnecessary functions (for instance, unlimited motion and zoom capability of the cameras, wireless transmission and sound recording); available but unnecessary functions or disproportionate functions have to be switched off.

Based on the Guidelines, the majority of the protective measures to be applied to ensure the security of data processing through video devices is not different from the solutions applied in other IT systems. At the same time, the controller must ensure appropriate protection for the components of the surveillance system (the elements of the system) and the data processed therein through all stages of processing, including recording, storage, the transfer of images, inspection, erasure and override operations irrespective of the system and devices chosen. Naturally, this requires that controllers and processors equally apply the appropriate organisational and technical measures according to Article 24 of the General Data Protection Regulation.

In relation to the compliance of the measures applied, controllers have to conduct a data protection impact study prior to commencing processing, if it is likely that the planned processing would involve high risks for the rights and freedoms of data subjects. Controllers have to carry out impact studies, if the data processing qualifies as major methodological surveillance of public areas, and also if the data processing activity is included in the list of the data processing operation types according GDPR Article 35(4) published by the Authority.

It is important to note that if based on the result of the data protection impact study, processing would be of high risk for the data subjects despite the measures planned by the controller, the Authority must be consulted prior to processing.

2. Interest assessment and accountability in the context of video surveillance

In line with the Guidelines, the Authority also places particular emphasis on the expectations arising in relation to the processing of personal data through video devices and in addition to the presentations published in the framework of the 2020 conference for data protection officers, it summarises the experiences collected in the course of the supervision of video surveillance operations below.

2.1. Apart from the data processing operations of the public sector, the *lawfulness* of video surveillance is usually based on the legitimate interests of the controller or of a third person in accordance with GDPR Article 6(1)(f); it is only in exceptional cases that the legal basis of the processing is the consent of the data subject. In order to lawfully process personal data in the course of video surveillance, the controller needs to comply with this legal basis.

In relation to the legal basis of *legitimate interest* it is important to underline that

a controller may not process personal data based on GDPR Article 6(1)(f) just because there are no other possibilities and other legal basis cannot be applied. Though it is seemingly the most flexible legal basis, by applying it the controller undertakes substantial responsibility not only with the processing of the personal data taken stricto sensu, but also by undertaking to meet the related other guarantee obligations. The legal basis of legitimate interest is closely linked to the principle of *accountability* set forth in GDPR Article 5(2), which means that the controller has to undertake to meet the administrative burden of transparency, accuracy and fairness of the processing of personal data. So, this is not merely doing the paperwork, but a task of merit, which holds in particular in the case of processing personal data through video devices.

It is very important the controllers are aware that *identification and justification of the purpose and legitimate interest of data processing* is a task neither for the data subject, nor for the Authority in the course of its investigation in the controller's stead. The purposes and legitimate interests for which the controller intends to process personal data must be clearly justified, assessed and guaranteed by the controller in a clear and specific manner, at the level of the data and purposes.

2.2.1 Once the lawful purpose is identified, but before the commencement of processing, the controller has to assess whether the processing of the data *is necessary* to achieve the purpose. In this context, it has to be examined whether there are alternative solutions whose application would lead to the implementation of the planned purpose without the given data processing operation, or whether the purpose can be achieved using devices that are less restrictive than the planned data processing. If the controller can reasonably achieve the same result using modes and instruments, which are less restrictive for the right to personal data, there is no need, hence the legal basis according to Article 6(1)(f) cannot be applied.

In the context of necessity, specific facts have to be assessed taking into account the given situation – why and how the data processing solves the purpose to be achieved and, from the other side, it has to be analysed why the other instruments that could reasonably be considered are not suitable to achieve the purpose.

In the context of necessity, the following assessments have to be carried out:

- factual description of the specific situation characteristic of the controller (sphere of activities, location, clientele, security problems, etc.);

- description of why and to what extent the data processing restricts the privacy of data subjects;

- identification of the purpose to be achieved;

- a description of why data processing is efficient and why it is the least restrictive instrument for the achievement of the purpose.

2.2.2. In the case of processing personal data through video devices it is necessary to specifically identify the *purpose* of using the video devices, as well as *how long* it is necessary to store the recordings with a view to the implementation of the purpose. The period of data processing necessary to achieve a purpose may be different case by case. It is the responsibility of the controller to determine the purpose for which it operates the camera and to decide how long it is necessary to store the recordings for this purpose.

2.2.3. As a next step it is necessary to determine the *legitimate interest* of the controller or of a third party as accurately as possible. The General Data Protection Regulation does not specify what interests can be taken into account – frequently trivial interest may also be the legal basis of processing. It is, however, important that it has to be indicated always by the controller and no matter what legitimate interest it identifies, it must be described always with regard to the specific situation and activity, it does not suffice to give a broad, general definition without content.

2.2.4. This step is followed by a *survey of the data subject's interests and expectations* This is a broad notion, which includes the rights that belong to the sphere of privacy and other general interests. This means not only rights to personal data taken stricto sensu; the consideration of other freedoms may also be involved.

The Authority's experience is that controllers frequently stop at the identification of their own legitimate interest, at the same time they do not analyse the impact on the data subjects, or if so, inadequately. The fact in itself that the personal data of the data subject are processed, and it is "offensive" to him does not mean any "weighing", it does not mean that the controller has appropriately taken into account the criteria, interests and reasonable expectations of the data subject. As the central part of interest assessment is the "*matching of interests*", the exploration and objective analysis of the legitimate criteria of both "*parties*", it is important this step is taken by the controller circumspectly and thoroughly.

2.2.5. Finally, the controller will have to carry out the *weighing* itself, i.e. it has to demonstrate why the legitimate interest of the controller proportionately restricts the rights of data subjects.

In this context, what needs to be presented is not only why the processing of the data is "good" for the controller, but all the aspects of the given processing operation have to be taken into account and weighed individually and in totality. This includes why the controller cannot opt for another instrument, why the given processing operation is the most suitable for the achievement of the purpose and what kind of safeguards the controller provides to the data subject for the enforcement of his rights.

The main rule to be underlined in relation to carrying out the interest assessment is that it has to be carried out in writing, with sufficient documentation prior to the commencement of data processing even though this is not expressly included in the General Data Protection Regulation.

In certain exceptional cases, the Authority accepts that, although controller has not carried out a prior interest assessment, it is able to demonstrate (see accountability) that the legal basis of legitimate interest obtains. This, however, requires that there be special facts of the case, from which the fact that the legal basis of legitimate interest obtains can be readily concluded.

2.3. The mistakes most frequently seen by the Authority in data processing through video devices:

- the generality, abstractness and theoretical nature of the definition of the controller's legitimate interest;
- although the controller's legitimate interest is defined, the concrete circumstances of the case do not verify that the legitimate interest obtains – absence of the verification of suitability (*e.g. indicating the purpose of asset security in a tobacco shop with a camera aimed continuously at the employee without recording, which the employer randomly checks*);
- the incorrect or confusing identification of the controller (*for instance in the case of a business organisation functioning at the residence of a private individual it is not revealed whether it is household data processing or data processing through video devices for the purposes of asset security*);
- neglect of the "*necessity test*" – the absence of fact-based weighing adjusted to the specific case taking into account whether there is a less offending intervention in the privacy of the data subject.

2.4. According to the experiences of the Authority, courts tend to have ever-increasing expectations vis-a-vis controllers in the assessment of the lawfulness of their processing in cases involving video devices. Controllers need to expect that they have to provide increasingly accurate and specific evidence concerning their data processing through video devices, which also reinforces the documentary expectations (written requirements). So, controllers are advised to take particular care that they are able to verify all their processing activities subsequently. The suitability of verification can be decided case by case, not only documentary evidence can be envisaged. Every "evidence", which can verify the given data processing operation can be considered, thus for instance witnesses and experts.

3 The rules of video surveillance at the workplace

The Authority received a number of complaints related to video surveillance at the workplace also in 2020. Based on the complaints and the experiences of the past years, it can be stated that mounting cameras to monitor employees, in many cases hidden cameras, is an exceedingly widespread practice on the part of employers. According to the position of the Authority, by stepping over the threshold of his workplace, the employee does not lose his rights to privacy, his image and sound recording; at the same time he has to note that the employer may check on him in the context of his employment, but only in that context. On the one hand, video surveillance restricts the employee's personality rights, on the other hand, in many cases the employer has a legitimate interest and right to subject employees to video surveillance.

With a view to compliance with the obligation of availability set forth in Act I of 2012 on the Labour Code – and also as the point of departure for video surveillance at the workplace – Section 11/A(1) of the Labour Code allows the employer to check on the employees as far as their behaviour related to their employment is concerned. In this context, the employer may also employ technical devices, of which, however, it has to inform the employees in writing in advance. The employer's right to check provided by the legislator is necessarily concomitant with the processing of personal data. Pursuant to the definitions of the General Data Protection Regulation, as well as the Privacy Act, the face and an image of a person qualify as personal data, recording images and any type of operation on the data qualify as data processing. The question frequently arises whether looking at the live image in the absence of any additional information qualifies as data processing with regard to the data subject. In the operative parts of its numerous decisions on video surveillance at the workplace, the Authority states that "with

the help of technology (for instance zooming in), by now surveillance is possible in a much wider range than through personal presence, so the observation of the streamlined images enables a more detailed check in these cases. Furthermore, the streamlining of live images and their observation generally takes place with some purpose, so it can be regarded as a partial element of an integrated data processing process, resulting in the controller bringing some kind of a decision based on seeing the live image". Looking at the images does not qualify as data processing, if "the technology applied in the course of surveillance does not offer an opportunity for the person carrying out the observation to obtain additional information in relation to the data subject natural person". In the case of video surveillance at the workplace, there are very few cases where it can be argued that looking at the images that does not qualify as data processing according to the definition of the General Data Protection Regulation, because in most cases the person observing the live images of the camera – e.g. security guard, janitor, manager at the workplace, etc. – does have additional information concerning the data subjects that get into the angle of sight of the camera, for him the data subjects can be unambiguously identified and checked and the surveillance itself takes place with a specific purpose on the basis of which certain necessary measures may be taken or decisions may be made.

During the period of employment, with a view to the appropriate operation of its commercial activity, the employer may restrict the privacy of employees – without their consent – in certain, accurately delineated cases subject to relevant guarantees.

The provisions of the Labour Code grant general authorisation for data processing related to checks by the employer, however, filling this framework with content is up to the employer in accordance with the principle of accountability. The employer has to specify the detailed rules on the devices to be used in clear, understandable, precise and detailed internal rules. When developing these rules, the employer has to pay particular attention to the requirement of proportionality with respect to every purpose of data processing.

In the vast majority of cases of workplace video surveillance before the Authority, the data processing purpose indicated is the protection of assets. In several of its decision, the Authority emphasises that it accepts the protection of assets as a legitimate purpose of processing, however, it is necessary that there be assets in the area subject to surveillance for whose protection video surveillance is a suitable, necessary and proportionate instrument. In the event that the purpose of operating a camera is the protection of a specific asset, then the angle of sight of that camera must be directed exclusively at the relevant area and under that

pretext, it cannot be used also to survey employees “incidentally”. The angle of sight of the camera may be directed at the area in line with its purpose.

In most of the cases before the Authority affecting data processing linked to checks by the employer’, the legal basis of processing is Article 6(1)(f) of the General Data Protection Regulation, i.e. the legitimate interests of the controller: “personal data may be processed, if processing is necessary for the purposes of the legitimate interest pursued by the controller or by a third party, except where such interests are overridden by the interest or fundamental rights and freedoms of the data subject, which require protection of personal data”.

It is essential that the employer in its capacity as controller has to carry out an *interest assessment* in every case in order to be able to refer to this legal basis. Interest assessment is a multi-step process, in the course of which the legitimate interest of the controller (meaning the employer) as well as the interest of the employees as the counterpoint of weighing, the fundamental rights of the data subjects have to be identified and, finally, based on the weighing, it has to be established whether the personal data maybe processed. If, as a result of the interest assessment, it can be established that the legitimate interest of the employer overrides the rights of employees to the protection of their personal data, the video surveillance system may be operated. However, it follows from the legal provisions in force and the principle of accountability that the employer has to demonstrate that the electronic surveillance system applied by it is reconcilable with the principle of purpose limitation and the outcome of interest assessment pointed to the primacy of the legitimate interest of the controller. This requirement delineates the purposes for which electronic surveillance systems may be operated in the workplace.

Respect for human dignity is an absolute limitation for video surveillance and because of this, cameras may not be operated for the ongoing surveillance of the employees and the activities carried out by them without an express purpose. The application of an electronic surveillance system whose purpose is to influence the behaviour of employees at the workplace and the permanent surveillance and checking of employees with the cameras is to be regarded as unlawful. The reason for this is that surveillance for the purpose of checking infringes the principle of necessity and proportionality as the employer has a number of other possibilities to exercise his right to check according to Section 11/A(1) of the Labour Code. Because of this, cameras, which only survey the employees and the activities carried out by them on an ongoing basis may not be operated. Workplaces where the life and limb of employees may be in direct danger constitute an exception, thus cameras may be exceptionally operated, for instance, in erecting shops,

smelters, industrial plants or other facilities containing sources of danger. It should, however, be highlighted that cameras may be operated for the purpose of protecting the life and limb of employees only if the threat is actual and direct, i.e. an eventual danger cannot be a constitutionally acceptable purpose of data processing as it follows from the practice of the Constitutional Court. All of this, however, has to be demonstrated by the employer in the interest assessment test, just as the fact that in the case of surveillance for the purpose of asset protection, circumstance, which separately warrant the location of the individual cameras actually exist and that the purpose to be achieved cannot be achieved in any other way. According to the position of the Authority, the employer in its capacity as controller has to indicate in the Privacy Statement provided to employees with respect to the application of the electronic surveillance system, the purpose for which the given camera was positioned in the given area and the exact area or equipment to which the angle of sight of the camera is directed. In the case of cameras, the employer *has to carry out the interest assessment for each purpose*, so that the cameras do not become instruments of surveillance of the employees, but should serve the achievement of the given legitimate purpose in actual fact and that the principles of purpose limitation and data minimisation are appropriately enforced in the case of every camera. Practice when the employer provides information to the employees in general terms about the fact that it applies an electronic surveillance system in the area of the workplace is unacceptable.

In addition. according to the position of the Authority, electronic surveillance systems may not be used in premises, which are designated for employees to spend their breaks in. There may be some exceptions to this, if there is some kind of an asset to be protected in such premises (for instance food or drink dispensing machine) in relation to which some employer interest may be demonstrated (for instance the employees had damaged the equipment several times and the employer had to pay damages). In this case, a camera may be used in such a room with a view to the specific purpose, however, it follows from the principle of data minimisation that the employer has to pay particular attention to directing the angle of sight of the camera exclusively at the asset to be protected. Cameras may not be located in premises whose surveillance could violate human dignity, in particular, in dressing rooms, bathrooms, toilets or surgeries and the associated waiting room.

As to the period of storing the recordings made by the electronic surveillance system, the employer has to demonstrate why the recordings made by the cameras have to be retained for the period given by it in accordance with the principles of purpose limitation and limited storability and the results of the interest assessment test.

It is an essential requirement in the case of data processing related to workplace video surveillance that the employee as data subject should receive appropriate, transparent and easy to understand *information* on the data processing. Pursuant to Recital (60) of the General Data Protection Regulation, the principle of transparent and fair processing requires that the data subject receives information on the fact of processing, its purposes and be given all other information necessary for ensuring fair and transparent processing. In every case the Authority recommends the written form because the controller i.e. the employer has to demonstrate and verify that the appropriate information was provided in advance in accordance with the principle of accountability according to GDPR Article 5(2). If eventually the information is provided orally, its content can hardly be demonstrated subsequently. Article 13(1)-(2) of the General Data Protection Regulation specifies the information that has to be provided to the data subject concerning a data processing operation.

Over the past two years, the Authority issued numerous decisions establishing infringements in the new legal environment with respect to the video surveillance systems used at the workplace. Infringements were established and fines were imposed largely because of the violation of the principle of purpose limitation, for instance in a case where the Authority acknowledged the protection of assets as the purpose of processing, but there were no assets to be protected in one of the workplace premises of the factory building, hence the purpose of protecting assets could not be interpreted in the case of the cameras in this hall. An example of violating the principle of data minimisation from one of the decisions is the camera located in a dining hall; it was subsequently proven that its angle of sight was directed not at an asset to be protected but to the entire room. The Authority established a failure to comply with the obligation to provide information in many cases, because according to the statement of the controller the information was provided orally but its content and the fact that it took place could not be demonstrated subsequently, or although the controller did have a Privacy Statement, it did not comply with the requirements of the General Data Protection Regulation.

Video surveillance in a tobacco shop

According to a complaint received by the Authority, a video surveillance system was installed in a national tobacco shop to observe the employees working there and the shoppers. The camera system was used for random spot checks of the live image, not for continuous recording. According to the complaint, there was no poster or inscription to provide information on the fact of video surveillance for the shoppers, nor did employees receive any information on the

video surveillance. According to the complaint, the controller was continuously observing the employees. In response to the complaint, the Authority launched investigative procedures and then, based on the facts of the case explored, an Authority procedure of data protection ex officio. In the decision brought in the case it established the following. The controller violated the principle of purpose limitation according to GDPR Article 5(1)(b) in view of the fact that random checking of live images in the absence of recording the images is not suitable for demonstrating infringements affecting assets/persons, thus it is unsuitable for the achievement of the asset protection purpose indicated. Furthermore, the controller violated the principle of accountability as set forth in GDPR Article 5(2) in that it was not unambiguous and subsequently could not be verified actually how frequently and for what reason it conducted checks, particularly in view of the fact that the observation of IP cameras through the web browser of a mobile phone cannot be logged centrally. The controller was unable to verify the compliance of data processing and infringed the right to access information and personal data according to GDPR Article 13(1)-(2) by failing to provide appropriate information about the processing and related matters to employees. In its decision, the Authority instructed the controller to terminate the operation of the camera system enabling the surveillance of the employees, or if it decides to transform the data processing practice of the camera system objected to, then it should do it in accordance with the provisions of the General Data Protection Regulation and the justification of the decision. In this case the Authority held the imposition of a data protection fine of HUF 1,000,000 justified. (NAIH/2020/2451/12)

4 Public area video surveillance by municipalities

The experiences of the complaints received by the Authority and investigations carried out on that ground indicate that data protection awareness primarily in small settlements is still low in relation to data processing implemented through video surveillance systems operated in public areas.

It is typical that as the municipalities decide on operating video surveillance systems and they do have their own funds, or obtain funding from a grant they applied for, the systems are quickly installed and the cameras begin operation without data protection aspects being reviewed, developing internal rules to ensure lawful data processing and bringing the appropriate data protection measures. In several cases it was revealed that the video surveillance system in a public area was operated without setting up public area supervision or having a supervisor.

The unlawful data processing situation arising from this was somewhat remedied by the amendment of Act LXIII of 1999 on the Supervision of Public Areas (hereinafter: Public Area Supervision Act), which entered into force on 1 February 2020. This amendment helped precisely the small settlements in enabling them to conduct lawful data processing even in the absence of public area supervision, if setting it up would have meant disproportionate and incalculable cost for the municipality. Under the amendment, in the absence of public area supervision or supervisor, a civil servant employed by the municipality designated for this purpose may carry out the operation of the video surveillance system in the public area including the concomitant data processing operations.

Section 7(3) of the Public Area Supervision Act allows the use of video recording devices for the purposes of public security and crime prevention. Based on the requests for consultations submitted in relation to public area surveillance systems and the investigations pursued in the wake of complaints, the Authority found that controllers were frequently not aware that data processing through public area surveillance systems meets the definition of data processing for law enforcement purposes set forth in Section 3(10a) of the Privacy Act with respect to both the purpose of data processing and the identity of the controller.

The absence of the identification of the controller is a persistent problem in several cases. The roles and responsibilities of the police controller, the municipality (eventually the supervision operated by it) the business organisation or foundation set up by the municipality comprising the entities participating in the operation of the surveillance system are confused. It happened in several cases that it was not clear from the statements made in the course of investigations and from the provisions of the rules applicable to the public area surveillance system, who was actually carrying out what activities in practice.

According to the Authority's experience, the data protection aspects of the activities carried out by persons and agents participating in the operation of the surveillance systems have not been thought through and because of this it happens frequently that unauthorised persons carry out data processing operations. Typically mayors have access to and use the recording which is, however, unlawful according to the regulations in force. In many cases, the issue of the responsibility of the persons participating in processing is not accurately defined in the course of processing.

In the course of its investigations, the Authority also found failure on the part of the data protection officer to meet his reporting obligation in several cases, despite the fact that in the event of the operation of a public area surveillance system that is mandatory pursuant to Section 25/L(1)(a) of the Privacy Act.

It is also important to note that the updating of the data processing rules is often not carried out in view of changes in the regulatory environment (the amendment of the Privacy Act in view of the application of the General Data Protection Regulation, the amendment of the relevant rules of the Public Area Supervision Act). Similarly, keeping up-to-date data processing records with the content as set forth in the Privacy Act is a common deficiency in the area of data controller obligations. Unfortunately, it happened in several cases that the records made by the public area surveillance system were made accessible to anyone through the worldwide web.

As an isolated case, but a positive example of data security awareness, the Authority investigated a complaint about data processing through a public area surveillance system of a city's public area surveillance body (NAIH/2020/4543). The specificity of data processing in this case was that the head of department of the controller was permitted to work from home as of 30 March 2020 until withdrawn in view of the health emergency. Through this, he could access the surveillance camera management software also from home and was able to see the images streamed by the surveillance cameras directly from home. The complainant objected to the fact that such a situation could provide an opportunity for abuse.

The investigation of the Authority established that the surveillance camera system directly serves public security. During the public area surveillance activity, the head of department checked the positions of the cameras and he also had the opportunity for direct intervention in the event that urgent intervention was needed. As the job of the head of department involved the need for immediate response and the efficient checking of the camera positions, granting him remote access was justified.

The Authority examined the data security measures related to working from home. It was established that the controller enacted the set of rules related to information security awareness to be complied with in the course of working from home and took action to have them observed within the organisation. In addition, the head of department was subject to the obligation of confidentiality in relation to his official activities. The processing under study proved to be appropriate also from the viewpoint of data security as far as the use of IT devices was concerned. It was found that in accordance with the provisions of the IT Security Rules, work from home was done via a VPN connection and communication takes place exclusively through IT devices owned by the organisation. Access to the surveillance camera management software was only possible from a dedicated device, which took place through the VPN server with two-factor authentication. Data security was

ensured with additional IT solutions, including a firewall, virus protection software, screen saver and two-factor authentication.

As a result of its investigation, the Authority established that all in all, the data security measures implemented by the controller were suitable for minimising data security risks and in accordance with Section 25/I(1) of the Privacy Act, the controller provided the legal and IT framework to ensure data security through technical and organisational measures adjusted to the extent of the risks. The Authority closed the investigation underlining that the investigated processing solution can be upheld during and in view of the current health emergency.

5 The lawfulness of data processing through video devices in the light of a few consultation requests received by the Authority

The Authority received a substantial number of consultation requests from the controllers in connection with data processing through video devices, the lawfulness of the majority of which can be unambiguous assessed based on the Guidelines of the European Data Protection Board.

5.1. Exemptions from the data protection regulation

The General Data Protection Regulation does not apply to *fake cameras*, i.e. cameras which do not operate as cameras and do not transmit or record any personal data.

In addition, only those cameras may be exempted from applying data protection requirements, which natural persons operate exclusively for their personal, i.e. *private purposes as part of their activities at home*, for instance they survey their own private area provided that such an operation of the cameras cannot be associated with any professional or business activities. Pursuant to Section 14 of the Guidelines, if somebody surveys and records his own garden and the property is surrounded by a fence, it is subject to the exemption of home activities ("household exemption"), provided that camera surveillance does not even in part extend to public areas or the neighbouring property. In Section 27, the Guidelines acknowledge that in exceptional cases a situation may arise when the extent of the video surveillance cannot be narrowed down to one's own area because in this way it would not provide sufficiently efficient protection. Thus, cameras in which the surveyed area is narrowed down using software or masking, so that they only monitor one's own area and its direct surroundings taken *stricto sensu*, without being directed at areas used by other such as a staircase or a

neighbouring property, may also be exempted from applying the data protection rules.

If, however, a private individual does not use solutions that cover up the public area or if a person operates a set of cameras surveying a public area and not an area in his ownership, he becomes a controller and his activities no longer qualify as private purpose processing.

5.2 Data protection aspects of video surveillance of areas in joint ownership

Several submissions were received in connection with video systems, which may have monitored the undivided common property of two or more owners, for instance, the entrance gate, the common section of the property, the parking lot of a condominium, or the containers. It is important to declare that a person's image, the sound and video recordings of him qualify as personal data according to the General Data Protection Regulation and their recording and storage, the continuous and systematic, extensive surveillance of the area qualify as data processing. Consequently, if natural persons become identifiable and recognisable in the images of the cameras, then the recordings qualify as personal data and the operator of the camera pursues data processing.

Based on the above, a camera continuously monitoring and recording the staircase through the peephole in the entrance door to a condominium apartment is not exclusively observing the area held by the controller, thus it cannot be exempted from applying the data protection provisions, it implements data processing subject to the General Data Protection Regulation. Similarly, a camera looking at the common entrance to the property or a traffic surveillance camera equipped with a motion sensor expressly directed at the neighbour's door installed in one's own car also qualify as data processing to be assessed based on the regulation.

This means that the person monitoring common areas and public areas must apply all the requirements of the General Data Protection Regulation stipulated for controllers, it becomes necessary to identify the purpose and legal basis of processing to examine compliance with the principles and the assessment whether there is a need for the data protection impact study presented in an earlier chapter. In the context of compliance with the principles, the Guidelines also underline that the personal data must be appropriate and relevant to the purposes of processing, they have to be limited to what is necessary, which we refer to as the principle of data minimisation. This means that the controller should have carried out an investigation prior to the installation of the video surveillance system as to whether this measure is, first, suitable for the achievement of the purpose and, second,, whether it is appropriate and necessary for it. Data processing can only be justified if its purpose cannot reasonably be achieved

through other means that are less restrictive of the fundamental rights and freedoms of the data subject.

In addition, the neighbours and residents of the condominium have a right to get information in advance according to Article 13 of the General Data Protection Regulation and in the course of exercising their rights as data subjects, they may request access to and copies of the recordings. In addition, they may object to data processing based on legitimate interest and the controller may be exempted from terminating the data processing vis-a-vis the data subjects, i.e. the erasure of the recording and in the given case, the obligation to dismount the cameras only if it can demonstrate legitimate interest of compelling force.

5.3. Traffic surveillance cameras

The issue of the lawfulness of using in-vehicle dashboard cameras that record a trip frequently arises, when there are no express provisions applicable to the controller providing for the operation of the cameras. A request received by the Authority concerned the assessment of the lawfulness of mounting road monitoring dashboard cameras on the front of the driver cabins of vehicles transporting fuel.

In view of the fact that the company would carry out the planned data processing as a legal entity pursuing business activities, the processing does not qualify as private purpose processing, hence the provisions of GDPR have to be applied to it. In addition to the need to comply with the principles and to substantiate that there is a genuine legitimate interest, the Guidelines mention dashboard cameras as an express example in Section 35 and explain that if such cameras are installed, for instance in order to have some evidence of the events in the case of an accident, it is important to ensure that the dashboard camera does not continuously record the traffic or the persons along the road. If this condition is not met, the interest of the controller to have a camera recording an eventual road accident is not suitable for the verification of such a substantial interference with the rights and freedoms of the data subjects, which means that the controllers' legitimate interest cannot be substantiated.

As the installation of the continuously recording dashboard cameras mentioned in the request mean an interference with the privacy of individuals potentially affected by the recordings to an extent greater than necessary based on the parts of the Guidelines referred to above, and since the information provided to the Authority in the request does not otherwise establish the existence of any other circumstances that could justify such an interference – according to the position of the Authority, it cannot be established that the data processing carried out by the Company in the course of the installation of dashboard cameras would be in line with the principle of data minimisation.

5.4. Body cameras

Because of the availability of the technical conditions and the continuously decreasing cost of implementation, several controllers asked about the lawfulness of the general application of body cameras fixed on employees, such as security guards and parking attendants.

5.4.1. The body of representatives of a municipality entrusted a property management non-profit company with the operation of parking in public paying parking lots in the administrative area of the municipality. They would like to equip them with body cameras with a view to the security of the employment of the future parking attendants, the subsequent investigation of the lawfulness and proportionality of their actions and the quality of their work.

As a first step in relation to the activities described in that submission, it is necessary to examine whether the purpose referred to can be achieved by other solutions not requiring the processing of data, such as security guards working in pairs in higher risk locations or the presence of a public area wardens. Certain data controller agencies or persons may also operate video equipment (surveillance cameras, cameras recording their actions or body cameras) in public areas expressly in accordance with legal provisions such as the public area wardens in the course of their actions.

After this, it is warranted to examine the aspects related to workplace data processing and supervision as discussed in the chapter above, as with regard to data processing related to employees, both the Constitutional Court and the Authority called attention to the fact that respect for human dignity is an absolute barrier to video surveillance. Because of this, cameras may not be operated for the ongoing surveillance of the employees and the activities carried out by them permanently without an express purpose.

According to the position of the Authority, the data processing referred to in the request, i.e. using body cameras on parking attendants for the purpose of workplace supervision does not meet the requirements of necessity and proportionality, despite the general authorisation given by the Labour Code because it constitutes an interference with the privacy of the employees concerned, which is greater than necessary for the achievement of the purpose of processing.

5.4.2. In line with the above, the Authority did not regard the practice of public transport service providers and traffic organisers employed for providing such services to use body cameras on the clothing of conductors without continuous recording as objectionable because the conductor can freely decide on starting or stopping the recording by the camera, hence the body cameras cannot be used

for the purpose of workplace supervision and there is an express authorisation by law for the operation of the cameras.

5.4.3. A fast-food restaurant requested the position of the Authority in relation to the fact that it does not use a fixed camera system within its premises, but its security staff endured numerous attacks in recent times. Because of this, it would equip security guards with body cameras, which would make recordings exclusively based on the decision of the security guard, being started in situations jeopardising his life or limb within the premises. Provided that such cameras are not directed at public areas and they do not violate human dignity, i.e. the guard may not wear the device in toilets or dressing rooms, it is the Authority's position that such a practice may be in line with the provisions of the General Data Protection Regulation after conducting a data protection impact study and incorporating its results, bearing in mind the principle of transparency.

Sections 59 and 60 of the Guidelines underline that if the investigating authority taking action in the case seizes the recordings, then the legal basis of data transfer will be the legal obligation applicable to it, in view of the requirements of the acts on misdemeanours or criminal procedures. If, however, it is the owner of the shop who decides to forward a recording made of a suspicious act to the police, for instance in the case of lodging a report, then the legal basis of data transfer may be the legitimate interest of the controller. In relation to both cases, it is important to highlight that the purpose of data processing through video devices cannot be merely to ensure that the data controller has the recordings in case an authority might want to request them, for example to increase the coverage of the city centre by cameras.

5.5 Cameras in condominiums

In relation to camera systems in condominiums, several of their representatives contacted the Authority because as of the spring of 2019 Act CXXXIII of 2003 on Condominiums (hereinafter: Condominium Act) does not specify the retention period of the recordings and uncertainty evolved also in relation to the legal basis of processing, as well as the necessary content of the data protection rules.

In this context, the Authority attaches importance to underlining that the condominium as an independent subject of the law qualifies as controller as "any body" according to the definitions of the General Data Protection Regulation. Based on the General Data Protection Regulation, the rules pertaining to data processing are *supplemented* by the Condominium Act in relation to the installation and operation of camera systems operated in condominiums by the community of residents acting as controller.

Such a supplementary rule is, for instance Section 25(1) of the Condominium Act, according to which the general meeting decides on the installation and operation of a camera system for the surveillance of parts of buildings, rooms and areas in joint ownership by a “yes” vote of the co-owners holding at least two-thirds of all the property shares. In such a case, the Rules of Organisation and Operation must contain the rules of data processing required for the operation of the camera system to be stipulated in accordance with the requirements concerning the protection of personal data. If a general meeting decision is made with the appropriate majority on the use of a camera system, it can be operated only when all the conditions set forth in the law jointly obtain.

As an additional condition, Section 25(2) of the Condominium Act stipulated that the operator of the condominium camera system may only be a person specified in the Act on the rules of the activities of security guards and private investigators based on a contract concluded by the condominium representative or the steering committee.

However, if a tenant wishes to install cameras to monitor parts of the common property and requests the approval of the general assembly, this is not a case of CCTV, nor is it the case if the tenant does not use the services of a property guard, but instead records a continuous image on a data storage medium in the condominium, for example.

However, it is not in line with the Condominium Act when a resident wishes to install cameras to monitor parts of the building in undivided joint ownership and asks the general meeting to support this, or if the collaboration of a security guard is not used but continuous recording is done on a data medium installed in the condominium. In such cases neither the private purpose exemption, nor the facilitation related to support by two-thirds of the owners shall apply.

The data protection rules expected by the Condominium Act can regulate the main features of the internal operation of the organisation of certain personal data processing operations within the condominium; it may specify procedures and principles to be followed for those participating in data processing operations, such as for instance the order of operating cameras, the period of retaining recordings, the placement of warning signs or the masking and IT tasks and responsibilities related to requests for the recordings of the camera by the data subjects (right to the issue of copies).

The templates of a number of data protection rules are accessible in the Internet, however as revealed by the above, the data protection rules must in the case of each and every condominium regulate the actually implemented data processing purposes and procedures; the basic notions and principles of the Regulation

need not be repeated in any internal rules and the Authority has not approved or authorised any such general rules.

It is important to distinguish the data protection rules and the Privacy Statements to be drawn up mandatorily for the data subjects (owners, residents, the users of the property, the condominium representative or other persons, even the postman or courier entering the property) to be made available to them prior to the commencement of individual processing operations ensuring the transparency of the processing of their data. Pursuant to Article 13 of the General Data Protection Regulation, this latter is an obligation for the condominium in relation to every data processing operation with the content specified therein (for instance information stickers in relation to the operation of video devices, information on the processing of the records of attendance at the general meetings).

It is essential that it is not a legal obligation for all condominiums to install a camera system, but if the controller – in this case, the condominium – decides to use video surveillance, then its legitimate interest constitutes the legal basis of processing, for which the Condominium Act specifies additional requirements, but irrespective of this, the controller has to carry out an interest assessment to be able to refer to this legal basis.

As for the retention period of camera recordings, the main rule is that the characteristics of the processing operation can be assessed based on the Guidelines and in the event of processing based on the legitimate interest of the controller, the national legislator can no longer determine in general how long the recording of a camera may be stored. The period of data processing necessary to achieve a purpose may be different case by case. It is the responsibility of the controller to determine the purpose for which it operates the camera and to decide how long it is necessary to store the recordings for this purpose. The video surveillance operations are carried out for the purpose of protecting assets and/or property, or to provide evidence. As most of the time, the damage caused can be discovered within a short period of time, in most cases automatic erasure of the recordings within a few days can be regarded as appropriate.

II.1.3. The most important data protection requirements related to data processing by political parties and organisations

Also this year, the Authority received many complaints in which the lawfulness of the data processing operations of political parties and organisations carried out partly in relation to the elections and partly irrespective of them was objected to.

In particular, the Authority received complaints related to the collection of recommendations by political parties and organisations for endorsements needed for the submission of candidates and lists, the building of a database of supporters, sending campaign materials to voters, the collection of signatures for achieving some political objective and political marketing activities.

1. Following the collection of endorsements carried out in relation to the general local elections and self-governing bodies of ethnic minorities in 2019, the Authority received several complaints objecting to the lawfulness of the processing of personal data shown in the endorsement sheets. As in the case of these complaints, the controllers could not be identified based on the available information, the Authority launched an official supervisory investigation to identify the controllers (NAIH/2019/6771, NAIH/2019/6802).

Based on the Authority's experience, one of the greatest deficiencies of data processing related to the elections has been the appropriate identification of the controllers and processors and the unambiguous clarification of the tasks and responsibilities of those filling these fundamental roles prior to the commencement of the data processing operation. According to the position of the Authority, a situation in which a data processing operation series does not have a person responsible for it determined in advance is not acceptable from the viewpoint of data protection. With a view to the lawful achievement of the purposes of processing, it is necessary to specify what the exact route of use of the data recorded will be and how long they are going to be stored and who are authorised to have access to the signature collection sheets and sympathiser databases prior to the commencement of data collection.

In its decisions, the Authority established that the role of every participant of the signature collection in data processing has to be clarified (controller, processor, joint processor), the content of their participation in the process of data processing and the person responsible for the discharge of obligations have to be specified prior to the commencement of data processing. The activists have

to have a contract of assignment specifying the controller or processor tasks and they have to be able to appropriately verify on behalf of which controller they carry out their activities.

2. Many objected to the fact that the persons collecting the signatures or collecting data for building up some other sympathiser database also collected other data and supplementary information from the data subjects (whether the data subject was at home or not, how he received the person collecting the signatures, etc.) (NAIH/2019/4467). In relation to this, the Authority called the attention of political parties, nominating organisations and other persons and organisations participating in the processing of the data to the fact that in the course of collecting endorsements, no other special personal data (for instance what sort of attitude the citizen exhibited vis-a-vis the person collecting the endorsement) may be recorded other than the personal data needed for the validity of the endorsement.

3. In the course of the data processing operations of parties and political organisations other than their processing operations related to elections (for instance, inviting the opinions of voters, informing citizens of the activities of the party and its achievements), it is indispensable to clarify and render unambiguous who can be regarded as controller in the course of these activities, who bears responsibility for the given processing operation and where data subjects can turn to with their requests related to the exercise of data subjects' rights. (NAIH/2020/4633)

4. With regard to the collection of signatures for the various expressions of opinion and those related to other civil initiatives, the legal regulations in force do not regulate what data need to be indicated in the collection sheets. Based on the principles of purpose limitation and data minimisation, however, the range of data has to be as narrow as possible and when collecting signatures only the personal data needed for the identification of a natural person may be collected.
If in the course of collecting signatures to support some initiative, the personal data of the data subjects are also request for the purpose of building a sympathiser database – in particular, name, e-mail address, phone numbers – this collection of data shall be considered as processing for purposes other than the original collection of the data, of which the data subjects must be informed in every case. The purposes of data processing must be unambiguously defined, the various purposes have to be delineated and information has to be provided about the individual purposes of processing and the personal data to be collected in relation to them, as well as the most important information on processing has to be

provided. (NAIH/2020/1486)

5. The principle of transparency makes it particularly important to provide adequate information to data subjects on the processing operation. The information must be drafted clearly and in a plain language, but also in simple and comprehensible terms, using appropriate sizes of fonts necessary to ensure the legibility of the text. It is important that political parties and organisations develop Privacy Statements with respect to every data processing operation carried out by them and make these easily accessible.

It is a frequent complaint that the representatives of political parties/organisations carry out targeted political marketing activities by making phone calls, whether they are contacting an age group of data subjects selected on the basis of address, asking for their opinions on some topical issue or to provide information on the current activities of the party/organisation. Those called, however, never get information on the processing of their personal data and in many cases in the course of the so-called robocalls, they had no opportunity to ask for information. (NAIH/2020/5380)

The Authority received over a hundred complaints in relation to the phone information campaign of one of the opposition parliamentary parties, in the course of which this party contacted the citizens by way of robocalls to provide information on the coronavirus situation and the position of the party. In the course of the investigation, the party gave evasive answers to the questions of the Authority or an answer that was obviously untrue and failed to respond when the Authority contacted them again. So far, the Authority never experienced non-cooperation on the part of a political party with the Authority, so the suspicion arises that the party unlawfully processes large amounts of data or uses a database whose lawfulness it cannot document. The Authority is conducting its procedure in the case. (NAIH/2020/3082)

In this context, the Authority underlines that even in the case of of calls or e-mails sent for the purposes of opinion polls or political marketing , data subjects must be provided with the most important information related to the processing operation and about where the Privacy Statement can be accessed later.

6. From a data protection point of view, with regard to campaign enquiries by political parties and organisations, it was found in several cases that during the pre-election campaign period, attempts were made to reach voters through various channels – SMS, e-mail, telephone calls, robocalls – but the data subjects did not receive any answer about the processing on their data in the course of

these contacts, even though they expressly asked for it, or the caller was unable to answer such questions. (NAIH/2019/3382, NAIH/2019/5251, NAIH/2019/6872)

The Authority received close to thirty complaints, in which the complainants objected to receiving text messages to their phone numbers, in which they were invited to a political event. In the course of the Authority's procedure, the sender of the text message stated that he sent an invitation to a political event to his old acquaintances whose phone numbers were stored in his phone and his Gmail account and he requested phone numbers from a company providing messaging services to send the messages.

The issue of the applicability of the so-called "household exemption" arose in relation to the data processing activity under study. However, the Authority established that the data processing may be outside the scope of data protection regulations only if it serves exclusively private purposes. As the sender of the text messages contacted a company in this case, requesting them to let him have phone numbers, so as to enable him to send invitations to a political event via these text messages, and also taking into account the well-known fact that the sender of the messages has been active in political life for a long period of time and he send the text messages, which named several parties and politicians, and they were not explicitly sent in his own name and with his own signature, they should be regarded as messages of political content, i.e. his data processing may be associated with his political activities. The messages were then sent not exclusively in the course of personal or home activities, hence it cannot be regarded as data processing exclusively for a private purpose. (NAIH/2020/8723)

7. In the course of its practice, the Authority met several cases when the controller political party processed the personal data of the data subject in the belief that the data subject gave his written consent to it, but in the meantime, it was revealed that the personal data processed by it, or some of them, did not originate from the data subject. (NAIH/2019/5434) To eliminate such cases, the question arose on several occasions whether the data subject may be called when collecting data to verify his identity or whether the data subject can be requested to present his ID card for this purpose.

According to the position of the Authority, there is no lawful purpose of processing, in line with the provisions of the General Data Protection Regulation concerning its principles, which would require the controller to call upon the person signing the questionnaire/signature collection sheet to identify himself, hence requesting the presentation of any kind of identification document to verify the identity of the signatories is unnecessary and disproportionate in the course of collecting

signatures. However, particular attention has to be paid to the enforcement of the principle of data accuracy, particularly in the case of data coming from different sources. To that end, it is necessary to ensure the exercise of data subjects' rights enabling them to simply and quickly indicate their requests for rectification or erasure, if they notice that their personal data are processed by undesired organisations. Furthermore, the Authority regards the two-step consent verification method as good practice.

8. Frequently, political parties and organisations carry out their data collections related to the expression of opinion or other initiatives in the online space, for instance on the website or the Facebook page of the controller – in many cases, however, appropriate information on the specific data processing is missing in the course of these data collections.

9. The Authority summarised its experiences related to the data processing activities of political organisations in a recommendation, in which it called the attention of political parties and organisations to the following most important requirements from the viewpoint of data protection:

– Prior to the commencement of data processing, they need to specify the person in charge of meeting the obligation set forth in the General Data Protection Regulation, the roles of the participants of the data processing activities (controller, processor, joint processor), as well as the content of their participation in data processing. The activists must have contracts of assignment as controllers or contracts that specify the tasks related to this and if need be, they have to be able to substantiate that they carry out their activities on assignment by a specific controller.

– The purposes of processing must be clearly defined and the various data processing purposes must be delineated. Based on the principles of purpose limitation and data minimisation, the range of data must be narrowed down as much as possible. Political parties and organisations may collect only the data indispensable for the achievement of the purpose of processing.

– Particular attention must be paid to providing adequate information to data subjects about the processing. Political parties and organisations should render their data processing operations transparent. Even in the case of telephone calls or e-mails for public opinion polls or political marketing purposes, the data subject must be informed of the most important information about the processing and the availability of the detailed Privacy Statement.

– With regard to ensuring the exercise of data subject's rights, it is necessary to draft the appropriate internal procedures, of which easily accessible information must be provided.

In this recommendation, the Authority also calls the attention of citizens to the fact that prior to giving their support to various political or other private purpose initiatives and their personal data, they should pay particular attention to the following:

– Prior to providing their personal data, it is recommended that they study the most important information related to the data processing. It is fundamentally necessary to check whether the identity of the controller is clearly specified.

– Also, if they provide their data online, they should pay attention to whether adequate information is available on the circumstances of the specific data processing operation, and they should make the decision on whether or not to give their personal data only after diligently studying it and knowing what is in it.

– If they think that the processing of their personal data is not transparent or it is unlawful, they should exercise their data subject's rights guaranteed in the General Data Protection Regulation (for instance, right to access, right to erasure). If they do not get an answer of merit from the controller to their request, or if there is a suspicion of infringement, they may initiate the procedure of the Authority or the courts.

In relation to specifying the identity of the controller, the Authority also recommended an amendment to the legal regulations to the Ministry of Justice, namely that the Ministry should examine the possibility of developing a regulatory environment that would set forth at the level of law with regard to the data processing activities of political parties and organisations carried out for a political purpose that if the identity of the controller was not clearly specified in the course of this activity or if the data subjects were not appropriately informed of this, which person of the political parties and organisations being independent legal subjects should be regarded as controllers by force of the law.

II.1.4. Other important and interesting cases

The Authority conducted a number of investigative procedures and data protection procedures also this year. Of this, a few cases can be regarded as of outstanding significance based on the following criteria:

1. amount of the fine, sanction applied;
2. processing of special categories of personal data;
3. minor data subjects;
4. the novelty of the legal issue to be decided, the significance of the issue of interpretation of the law;
5. cross-border processing of personal data.

1. *Outstanding cases from the viewpoint of the amount of the fine*

1.1. Exercise of data subject's rights related to processing through video devices

The Authority conducted its ex officio data protection procedure to investigate processing by a shoe trading limited company (hereinafter: company). In the course of its investigation, the Authority examined how the Company handled the data subjects' requests related to the processing through video devices and what sort of procedures are developed to ensure the exercise of data subjects' rights.

In the antecedent case, the data subject bought a pair of shoes from the company for cash; as he stated he was given the wrong amount of change at the cash desk, in view of which he requested the company to let him view the recording of the event, and also requested the company not to erase the recording until the situation is clarified. Although the data subject requested the above in several ways, orally on site, by phone at the customer service, in a letter sent to the managing director, the company informed him that they only issue the camera recordings to the police. The company did not restrict the recordings, but erased them after the retention period, so the data subject lodged a report with the police in vain, the recording was no longer available.

The Authority established that the company did not justify why they would not let the compliant view the recordings, and refused the exercise of the data subject's rights based on inappropriate reasons. The company did not adjudge the data subject's request to restrict processing, it did not grant the request, nor did it

provide information on the reasons for the refusal, it merely erased the recording.

During this period, the company did not have data protection rules with respect to camera recordings. The company kept systematic records of incoming messages, but it did not separate the data subjects' submissions related to data protection, instead they made an entry about the otherwise data protection request of the data subject as if it were a consumer protection complaint.

The Authority established that the company – as it did not have any internal rules and procedures – failed to take the appropriate technical and organisational measures to ensure the exercise of data subject's rights related to processing of video devices in accordance with the General Data Protection Regulation. Later, the company adopted rules settling their processing practices carried out in the course of operating the camera system which, inter alia, contained detailed instructions as to how to handle the data subjects' requests related to video recordings. However, the established procedures restricted the rights of data subjects to the issue of copies and to inspect. The interpretation of the right to restrict processing was also restrictive because according to this, the data subject was required to verify his right or legitimate interest when submitting the request for restriction. Furthermore, the rules contained sectoral legal regulations not in force, stating that the restriction of the recording may be requested for max. 30 days.

The Authority established that the company, when developing its data processing rules, brought organisational measures which failed to ensure the data subject's right to restrict processing in accordance with the conditions set forth in GDPR Article 18 whereby the company infringed GDPR Article 25(1). Because of the established infringements, the Authority imposed a data protection fine of twenty million forints on the company. (NAIH/2020/2204)

1.2. Voice recording in a customer service office

A complainant reported that a voice recordings are made in the course of the administration of cases in the customer service office of a telecommunication service provider (hereinafter: service provider), but data subjects do not get (adequate) information about this. It was by chance that the complainant noticed that the microphone was in operation.

In addition, the complainant reported that there was some information in less conspicuous fonts and placed so as to be missed in the second "selector screen" of the "Take a Number system"; he noted, however, that there were cases when he did not have to take a number in the customer service office, but the administrator called him right away, hence he had no way to get this information. The Authority investigated the general data processing practice of the company.

The service provider stated that the voice recording took place based on its legitimate interest as set forth in GDPR Article 6(1)(f) and it enclosed the relevant interest assessment test to its letter. The conclusion of the interest assessment was that as the service provider mapped out and took into account the interests and rights of the data subjects, the processing was necessary and proportionate. In relation to the possible counter-interests of data subjects, the interest assessment only states that "the processing of the data affects the rights of natural persons".

In its decision, the Authority reprimanded the service provider in view of the fact that it was unable to identify the opposing interests and it essentially failed to include the data subject's interests opposed to processing in any form whatsoever; furthermore the test contained a general weighing, it was not a test weighing interests/types of case administration/independently appearing interest/purpose and it follows that the legal basis of legitimate interest does not exist. As the service provider did not refer to any other legal basis and based on all the circumstances, there was no other legal basis, the Authority established that the service provider made voice recordings of the case administration taking place at the personal customer services without the appropriate legal basis during the period under study.

The Authority also reprimanded the service provider, because its practice of making voice recordings of the entire process of personal case administration in every case failed to meet the principle of data minimisation as set forth in GDPR Article 5(1)(c).

Furthermore, the information provided by the service provider in advance was also inadequate, because even though the Privacy Statement was accessible on the company's website, the customer service offices failed to provide information about the existence of these statements or of their accessibility. Prior to commencing recording, the service provider only provided information to the data subject about the fact of data processing, while information on the other essential circumstances of processing was provided in a manner that was not easily accessible, hence this information failed to comply with GDPR Article 12(1).

The Authority also established that none of the Privacy Statements said unambiguously that as a main rule, a voice recording is made of the personal case administration in every instance, irrespective of the type of case that the customer is dealing with.

The only textual information provided in the customer service offices was the information given through the "take a number" system and reaching the customer service window, the data subject did not necessarily notice the microphone put there. Single-level local information can achieve its purpose only if it sufficiently

captures attention. The content of the information provided in the “take a number” system was also inadequate because the statement that the voice recording depended on the consent of the data subject was untrue and misleading.

The information on the purpose of processing provided by the service provider was also inadequate and it failed to provide true information concerning the period of processing either because the Privacy Statement included a one-year retention period even though the voice recordings were in fact stored for five years. In summary, the information provided by the service provider was deficient and misleading, infringing the principle of transparency.

Because of the above, the Authority regarded the imposition of a data protection fine of HUF 60,000,000 as necessary. When imposing the fine, the Authority took the very high number of data subjects into account as an aggravating circumstance. During the period under study, the service provider received 45,000-55,000 persons monthly at its personal customer services altogether in all its shops, thus the calculated number of data subject is in the order of magnitude of a million. It was part of the service provider’s basic activity that for long years, it regularly received a great many customers in the customer service offices, in view of which an appropriate data protection awareness would have been expected from it. The absence of an appropriately, precisely and specifically considered legal basis and purpose and the rough and ready processing of the data indicates a severely negligent behaviour. The service provider initiated the review of the decision in administrative litigation. (NAIH/2020/2758/3)

2. *Outstanding cases from the viewpoint of investigating the processing of special categories of personal data*

2.1. Making copies of pregnancy care booklets for claiming the benefits related to the loan to expectant parents

In the framework of an authority procedure launched ex officio, the Authority investigated data processing by a bank in the course of granting loans to expectant parents and its practice of making copies of pregnancy care booklets.

Married couples who claim the loan to expectant parents are entitled to suspend repayment following the 12th week of pregnancy. In the case of expecting the second or third child, the couples are entitled to a non-repayable child expecting benefit. If a couple claims this benefit prior to the birth of the child, they have to verify that the 12th week of pregnancy is completed, as well as the expected date of delivery with the pregnancy care booklet, of which the bank made copies with

different extents depending on the branch.

The pregnancy care booklet contains a number of health data of the pregnant woman, which are special category personal data, such as blood group, risk rating of the pregnancy, the data of earlier pregnancies and deliveries, medical history, the results of medical tests carried out during the pregnancy. These data are not needed for the couple to verify the completion of the 12th week of pregnancy and the expected date of delivery to the bank, i.e. the additional data processed in the copies of the pregnancy care booklets by the bank are inappropriate for the achievement of the purpose of processing, they are not relevant, they go well beyond the needed data, hence the Authority established that the bank infringed the principle of data minimisation according to GDPR Article 5(1)(c). Beyond this, the Authority also established that the bank had no legal basis according to GDPR Article 6 for processing these health data and none of the circumstances according to GDPR Article 9(2) obtain in relation to their processing.

In its decision, the Authority also established that the requirement of transparent information according to GDPR Article 12(1) was infringed by the information provided on the processing of the data, because the processing purposes indicated in the Privacy Statement were insufficiently specific; moreover, the range of the data processed was not separated according to the type of loan transaction for which the processing was necessary.

Beyond establishing the infringement, the Authority instructed the bank to erase the electronic copies of the pregnancy care booklets still held by it, to annihilate the hard copies and to verify that this was done in a creditworthy manner to the Authority. The Authority also instructed the bank to transform its practice of providing information, so that it complies with the requirement of transparency according to GDPR Article 12(1).

In addition to the above, the Authority regarded the imposition of a data protection fine of HUF 35,000,000 necessary. In imposing the fine, the Authority took into account the fact that the bank after launching the procedure acknowledged the infringement in relation to the personal data processed in the copies of the pregnancy care booklets, transformed its practice and took action to have the unlawfully processed personal data erased as a substantial mitigating circumstance. The Authority took into account the large number of data subjects, the ongoing nature of the infringement and the fact that the unlawful processing primarily concerned health data as aggravated circumstances. (NAIH/2020/2546/15.)

2.2. Data processing carried out in the course of the submission and subsequent evaluation of regular welfare grant applications at a university

The large number of data subjects and the processing of special category personal data warranted that the Authority in its official procedure investigate whether a university complied with the requirements of the general data protection procedure in the course of the submission and the evaluation of regular welfare grant applications.

In its decision closing the procedure, the Authority established that the university determined the circle of data to be processed going substantially beyond the authorisation it was granted by the relevant legal regulations. The university referred to mandatory processing of data requiring the data processing, which the legal regulations it invoked did not specify as criteria to be evaluated. Presumably, in order to definitely ensure the existence of a legal basis, the university also referred to the data subject's consent as a legal basis. The university did not consider that the conditions of the validity of the consent otherwise do not exist, or rather consent in the case of this processing operation cannot even arise because it deemed that if the submission of the grant application is voluntary, it follows that the consent to the processing of all the data provided in the course of filling in the application is also voluntary.

In particular, the Authority found it especially unlawful that the university, going beyond the legal regulations, decided on the processing of additional special category personal data but was unaware that their data in a physician's certificate on handicap/chronic disease/degree of disability qualifies as special category data since the fact that a given person is handicapped, has a chronic disease or has a disability is in itself health data and thereby special category data, hence the university processes special category data even if the data subject covers up all the other data in the certificate.

The Authority established that by specifying the data to be processed, the university infringed GDPR Article 5(1)(a) and (b) and greatly infringed GDPR Article 5(1)(c) because it failed to weigh with sufficient diligence, the submission of what documents and certificates are indispensable, i.e. it did not endeavour to comply with the requirement of data minimisation, it did not appear in its practice, but in order to make sure that all the circumstances requested to be verified are substantiated even if the verification of the given circumstance was concomitant with the processing of unnecessary additional data.

In addition, the Authority imposed a data protection fine of HUF 8,000,000. The point of departure when imposing the fine was to what extent the legislator's failure impacted the infringements carried out by the university, which was taken

into account as a mitigating circumstance. At the legislator failed to accurately specify the range of data to be processed, the university had to bear the responsibility for weighing the processing of what data are needed for taking into account the criteria specified by the legislator. The university should have followed the criteria specified by the legislator and it should not have required new circumstances generating the processing of additional data: the specification of data going beyond GDPR Article 6(1)(e) – lacking the appropriate legal basis – and furthermore, the infringement of the principles of purpose limitation and data minimisation arose not from the legislator's failure. The university failed to provide appropriate information to the data subjects, it did not update its Privacy Statement after the GDPR became applicable from which it follows that its data processing practice lacks transparency.

When imposing the fine, the Authority took the fact into account as aggravating circumstances that the university committed a severe infringement because the general data processing practice it applied greatly violated several provisions of the principles: going substantially beyond the authorisation granted to it by legal regulations, the university determined the range of the data to be processed and through this behaviour it caused the processing of personal data and personal data qualifying as expressly special category data without a legal basis, in some cases without a purpose and in a major part of the cases unnecessary processing all this in a way that in the absence of specifying the specific purposes of data processing, its processing operations totally lacked transparency . In view of the fact that the certificates required to be submitted contained the personal data not only of the applicants, but also other persons living in the same household, the Authority estimated the number of data subjects in the order to tens of thousands. The processing operation concerned special categories of personal data (data concerning the handicaps, disability and chronic diseases of the applicant student and the persons living in the same household). The university invites and evaluates grant applications every half year, which involves the processing of a large number of personal data and special category personal data. In view of all this, the controller was expected to have an adequate data protection awareness, hence the extent of its responsibility is higher. The Authority also established that in the absence of a sufficiently precise and specific definition of purpose and the consequent non-transparent processing operation and the fact that the university was unable to identify that it was processing a large number of special category data, which is subject to more stringent rules allows the Authority to conclude that the university exhibited severely negligent behaviour. The university initiated the review of the decision in administrative litigation. (NAIH/2020/54)

2.3. Access to the health documentation of deceased relatives

Making use of the authorisation granted by GDPR, the Hungarian legislator introduced the provisions according to Section 25 into the Privacy Act, which ensures the enforcement of certain data subject's rights due to the deceased during his lifetime with certain restrictions. The data subject's rights (rectification, erasure, etc.) that may be exercised pursuant to Section 25 of the Privacy Act, may be exercised by the person specified by the legal regulation; this, however, does not mean that such a person would qualify as a "data subject" in procedural law also.

The right that may be deducted from a sectoral legal regulation, which generates a right to a living person to access data concerning a deceased person is logically separate from this. In such a case, the holder of the right may have access to certain data on the deceased in his own right, but through this, he does not exercise data subject rights under GDPR and the Privacy Act. In such a case, therefore, he will exercise his right not on the basis of GDPR and/or the Privacy Act, but on the basis of the sectoral legal regulation, which generates a right directly for him and not for the data subject.

Pursuant to Section 3/A of Act XLVII of 1997 on the Processing and Protection of Health and related Personal Data (hereinafter: Health Data Act), the mandatory rules incorporated in EU legal acts or legal regulations on the processing of personal data incorporated in the health data and health documentation shall be applied to the processing of the circumstances of the death of the deceased person and the cause of death, as well as the personal data included in the health documentation of the deceased person.

Pursuant to Section 7(5) of the Health Data Act, following the death […] of the patient, the spouse of the data subject, […] – based on a written request – is entitled to exercise the right according to paragraph (3), if

a) health data are needed

aa) for the exploration of the cause influencing the life and health of the spouse […], or

ab) for the purpose of the health care of the persons according to point aa)

and

b) it is not possible to have access to the health data in any other way, or to draw conclusions from them.

Interpreting the provisions of the Health Data Act, the intent of the legislator can be established, according to which providing information to the spouse of the deceased person is essentially possible from two directions.

On the one hand, pursuant to Section 7(6) of the Health Data Act, a situation can be envisaged where some health data or copy of the related documents of the deceased is needed to explore causes influencing the life and health of the spouse of the deceased, or for his health care taking into account that that information cannot be obtained in any other way.

On the other hand, Section 7(7) of the Health Data Act leads to the conclusion that there is another right to obtain information due to the spouse with respect to the deceased, which is, however, restricted to health data related or possibly related to the cause of death and the treatment prior to the onset of death. Based on that he/she has a right to access these data to inspect the related documents and to receive copies of them at his/her own cost without giving reasons in the absence of personally being concerned in health care.

GDPR Article 15(3) provides for the right to the issue of copies with respect to "the personal data undergoing processing". In this case, this may only mean health data among the "health data included in the health documentation" taking into account Section 7(5) and Section 3/A of the Health Data Act.

It is the position of the Authority that the Health Data Act laid the foundations for the applicability of GDPR when the spouse enforces his/her rights according to Sections 7(6) or 7(7) of the Health Data Act as his own right, i.e. not in the capacity of being a data subject. If there are health data in the health documentation whose issue the complainant is entitled to request, the controller has to issue a copy to the complainant with the provision that on the first occasion it has to issue the copy free of charge. Failure to do so constitutes an infringement according to GDPR, in relation to which the Authority may take action.

3. *Cases concerning the personal data of minors*

For years, the Authority has regularly received large numbers of complaints initiating investigative procedures or petitions for the Authority's data protection procedure concerning the extent of meeting the right to obtain information and right to access by parents with regard to their minor children. In these cases, parents request documents concerning their children from guardianship authorities, forensic experts assigned in the course of court procedures or authorities' procedures and from education, welfare or health institutions.

3.1. The right to access copies of data

In relation to an investigative procedure, an education institution posed the question to the Authority "*whether all letters, memos, protocols, alerts, information, letters requesting legal opinion should be issued to a parent that apply to him and/ or the child*". The following should be highlighted from the Authority's position on this issue.

According to GDPR, the provision of information on the processing of data is a fundamental data subject's rights, which the controller has to meet in accordance with the provisions of GDPR providing access in the form of a copy of the data, if so requested. This means that the copy of the personal data processed by the controller will have to be provided which, however, is not always identical with a full copy of the document. There may be notes, references, legal provisions, other text segments and information of a technical nature on the document, which do not qualify as the personal data of the data subjects – provided that from them no conclusions can be drawn with respect to the data subject, so a copy may not be requested of them under the right to access according to GDPR and the controller is not under an obligation under GDPR to issue copies of these parts of the document.

The data concerning the interpretation of the law, professional provisions, internal memos *not including personal data,* correspondence, etc. generated in the course of the activities of an agency discharging public duties may be accessed by requesting access to data in the public interest provided that the conditions set forth in the Privacy Act obtain. Following the provisions of Chapter III of the Privacy Act, the possibility to grant the data request must be evaluated under the request for data in the public interest. (NAIH/2020/2618)

3.2. Right of access exercised by the legal representative of a minor

Frequently, one of the parents, acting as legal representative, wishes to exercise data subject's rights on behalf of his/her minor child, thus acting on behalf of the minor child as data subject, he wishes to have access to the data or get copies of voice recordings on which the opinions of the forensic experts appointed in litigation concerning the placement of the child, maintaining parental contact, or the settlement of parental right of supervision. In one such data protection authority procedure, initiated at the request of a parent, the parent requested that the appointed expert be instructed to issue the data and audio recordings of the examination of his or her child. . The Authority rejected the parent's request

because the issue of such data and voice recordings may give rise to concern if what the child had said concerning the parent requesting the data may include information, access to which by the petitioner could violate the legitimate interests of the child. According to the Authority's position, the confidentiality obligation of the expert with respect to whatever was said by the minor, prevails vis-a-vis both parents. With respect to the data generated in the course of the expert's examination in the case of a minor, the person of the data subject (child) is not identical with the person who exercises the right to access due to the data subject (legal representative). In this way, the exemption from the expert's confidentiality obligation cannot be regarded as automatic.

According to the position of the Authority, it is desirable, if the expert evaluates whatever was said by the minor, following the child's examination from the viewpoint whether there was a conflict of interests between the child and either of his or her parents in view of the subject matter of the given procedure and the provisions of the assignment. He has to assess whether access to whatever was said by the child by either or both parents would have detrimental consequences with respect to the child. According to the Civil Code, the parent shall not represent the child in cases, in which he/she is a party with interest opposed to those of the child, thus the right of access may not be exercised in such a case by the legal representative pursuant to the Civil Code.

The Authority called the attention of the assigned expert and in general experts to the fact that in the event of exercising the right to access by a legal representative concerning a minor child, they should always examine the possibility to grant the request from the viewpoint of a possible conflict of interests, if they note any circumstance giving reason for refusal, they should always obtain the instruction from the assigning court/authority concerning the refusal to grant the access request by amending the assignment order. In such cases, the experiences of the examination laid the foundations for the restriction of the right as the expert notes that access to what was said by the child is contrary to the child's interest in the course of the examination, this cannot be stipulated in advance in every case in the assignment order. (NAIH/2020/593)

4. *Outstanding cases because of the novel nature of the legal issue to be decided and the significance of the issue of the interpretation of the law*

4.1. Data processing by independent judicial officers

Upon request the Authority also conducts its data protection procedures against

independent judicial officers. In the course of these procedures, the Authority investigated whether the judicial officers evaluated the access request of petitioners in accordance with the provisions of GDPR.

In the course of one of these procedures, the independent judicial officers disputed the powers of the Authority and in this context he invoked the prohibition of the withdrawal of powers according to the Administrative Procedures Act and the legal institution of data protection objection according to Chapter VI/A of the Privacy Act, on the basis of which data processing in the course of a distraint procedure may be investigated by the district court based on a petition submitted to the competent district court having the relevant powers. In his view, the procedure of the Authority infringes the right to a lawful court procedure according to Article XXVIII(1) of the Fundamental Law and it negatively implements the prohibition of the withdrawal of powers already referred to.

He also referred to GDPR Article 23(1)(j), which allows Member States to introduce restrictions by way of legislation with regard to the application of the enforcement of data subject's rights with a view to enforcing claims according to the Civil Code. In his view, the Member State legislator allowed the restriction of the right in a Member State in the field of the law governing distraint. Thus, if the Authority disregarding the rules governing powers still investigates his data processing, then it should investigate the enforcement not of the rules of GDPR, but of the provisions of Act LIII of 1994 on Distraint (hereinafter: Distraint Act). According to his statement, a provision of information in a distraint procedure is affected primarily not in writing, but in person or by phone, whose rules are regulated by Section 40 of Ministry of Justice Decree 1/2002. (I.17.) on the administration and the management of funds by judicial officers. According to his statement, he granted the petitioners' "request for data" and in his view, "an objection to the extent is ab ovo not a data protection issue".

Upon receipt of the request, the Authority ex officio examined its powers and competence and in the course of this, it also took into account that according to GDPR Article 55(3), the powers of the supervisory authorities do not extend to the supervision of data processing operations carried out in the course of the discharge of the judicial tasks of courts. Pursuant to Section 38(2b) of the Privacy Act, the responsibilities of the Authority do not extend to litigious and non-litigious proceedings aimed at bringing a court decision with regard to the data processing operations carried out by the court.

The above legal regulations exclude the powers of the Authority only with regard to the data processing activities of the courts carried out in the course of the

discharge of their judicial tasks, but as the independent judicial officers cannot be regarded as part of the judiciary pursuant to Article 25 of the Fundamental Law and Act CLXI of 2011 on the Organisation and Administration of the Courts and he does not carry out judicial activities administering judgment, hence the data processing activities of the independent judicial officers carried out in the course of the discharge of his duties is subject to the Authority's supervisory powers. It follows that Section 225(2) of the Distraint Act referred to by the independent judicial officers, according to which the procedure of the bailiff as civil non-litigious proceedings is the same and the proceedings of the court does not mean that the supervisory powers of the Authority would not extend to the supervision of the data processing activities carried out by the independent judicial officers.

The above is substantiated by the fact that as this is a rule of exception related to the powers of the supervisory authorities, it may not be interpreted ampliatively, i.e. the solution which would include the judicial officers in this circle only by reference and analogy is not possible because that would require itemised legal regulation.

In terms of its legal standing, the bailiff is not a judge, he does not meet the requirements for judges, nor does he have to do so. The conditions of appointment and applications are different for judges and judicial officers. Their separation from the judiciary is also indicated by the fact that the judicial officers are in a service relationship not with the court, but their activities are supervised by the Magyar Bírósági Végrehajtói Kar (Hungarian Chamber of Judicial Officers). In addition, it is necessary to underline Section 71/B(1) of the Privacy Act, which regards the data processing activities of "the judge, lay judge or judicial employee taking action" as testable in an objection procedure. The same thing holds for this, as explained above in relation to GDPR, namely that as this is an exception rule, it is not possible to mean "judicial officer" by "judge" through the interpretation of the law.

In terms of the relationship between sectoral legal regulations and GDPR, it should be highlighted that in addition to the provisions of the sectoral rules, the rules of GDPR are also to be complied with, because as a result of the primacy of Union law, GDPR is to be applied over Hungarian law. The Court of Justice of the European Union[5] declared on several occasions that the obligation to waive

5 Costanzo judgment of 22 June 1989, 103/88, EU:C:1989:256, Section 31; CIF judgment of 9 September 2003, C198/01, EU:C:2003:430, Section 49; Petersen judgment of 12 January 2010, C341/08, EU:C:2010:4, Section 80; The Trustees of the BT Pension Scheme judgment of 14 September 2017, C628/15, EU:C:2017:687, Section 54

the application of national legal regulations over Union law is an obligation not only for national courts, but of all state agencies called to apply Union law within their powers, including the administrative authorities, i.e. the Authority as well. In the present case, this means that while applying the sectoral rules on distraint, the rules of GDPR need also to be complied with, so that if there is a clash of laws between GDPR and the sectoral rules, then the application of GDPR is mandatory notwithstanding any national law that may conflict with it, in this case even implementing sectoral legislation.

Consistently with the above, in its decision the Authority established that in contrast to the argumentation of the independent judicial officer, the Distraint Act and Ministry of Justice Decree 1/2002. (I.17.) on the administration of court distraint and the management of funds (hereinafter: Distraint Administration Decree) does not contain any provision that would put any restriction of the application of any provision of GDPR. In this respect, Hungarian legislation corresponding to GDPR Article 23(2) could not be identified. The Authority reprimanded the independent judicial officer as the controller of personal data because according to the rules of Section 40 of the Distraint Administration Decree, he has to provide information personally and by phone, but he also has to comply with the principles of GDPR, as well as the provisions of GDPR Articles 12 and 15 and has to answer the access request of the data subject appropriately, hence it instructed him to provide full information with the content corresponding to GDPR Article 15(1) to the petitioner. (NAIH/2020/4637)

In the course of the other procedure, another independent judicial officer disputed his capacity as controller beyond the above, invoking that the “IT application ensuring the processing of the data is not the property of judicial officers, nor is the documentation of the distraint case”.

In spite of this argument, it was established that the independent judicial officer was a controller with respect to the personal data of the petitioner because he was pursuing data processing within the framework of legal regulation based on the authorisation granted in legal regulations. As against the argumentation of the independent judicial officer, pursuant to GDPR Article 4(7) it is not necessary for the determination of the controller status that the documents containing the personal data be in his ownership because through the fact that he carries out data processing with regard to the personal data in these documents, he becomes a controller. (NAIH/2020/6088)

5. *Cross-border processing of personal data*

5.1. Pursuant to GDPR, the Authority cooperates with the data protection authorities in the other Member States of the European Union. In the case of cross-border processing of personal data, the data protection supervisory authority according to the centre of activities or single place of activity of the controller (processor) within the meaning of EU law is entitled to take action as the lead supervisory authority. The supervisory authorities of the Member States other than the Member State according to the centre of activities (single place of activity) of the controller (processor) concerned in the data processing activity are entitled to participate in the administration of the case as concerned supervisory authority.

Acting as the lead supervisory authority means that the lead supervisory authority conducts the investigation of merit pursuant to EU norms, primarily the provisions of GDPR Article 60 and the procedural law of its own Member State and at the end of the procedure produces a draft decision, which it makes available to the concerned supervisory authorities involved in the proceedings in a specific procedure for obtaining their opinions prior to issuing the decision. The decision may be issued only if the concerned supervisory authorities agree with it, or if it was not possible to achieve a consensus, a dispute settlement procedure is launched. In the former case, the lead supervisory authority communicates the adopted decision with the centre of activities (single place of activity) of the controller (processor) and the lead supervisory authority monitors the implementation of the decision according to the procedural law of its own Member State.

The procedure of the Authority outlined above differs from the purely national Member State data protection investigation and the Authority's data protection investigation fundamentally with respect to the receipt of the case and the preparation of the draft decision. In procedures launched on the basis of a data subject's complaint, another EU supervisory authority receives the complaint, then if it deems it admissible based on the law of the Member State, it forwards the case together with its eventual annexes translated into English to the assumed lead supervisory authority through the Internal Market System, which enables communication among the supervisory authorities. The same channel of communication is to be used for the management of cross-border cases, not launched on the basis of a complaint. The other substantial difference is in the drafting and finalisation of the decision: the lead supervisory authority prepares the first draft based on the explored facts of the case, but finalisation may take place only in the case of a consensus acceptable to all the concerned supervisory authorities. The procedure between the two endpoints is conducted by the lead

supervisory authority in accordance with the provisions of its national procedural law; a specific feature of this type of procedure is that there may be an exchange of information, informal consultation and joint operation among the supervisory authorities involved in the case.

It is important that there can be no cooperative procedure, if the processing activity under study is carried out by official authorities or other organisations established according to the rules of civil law – in GDPR terminology "private party organisations" – pursuant to GDPR Article 6(1)(c) or (e) because then the procedure may only be conducted by the competent Member State supervisory authority according to the provisions referred to. It should also be noted that not even the Member State supervisory authority competent according to the seat of the given court has the power to supervise the data processing operations of courts carried out discharging their judicial duties; this is done by an agency(agencies) dedicated for this purpose by the given Member State within the judicial system of the Member State concerned.

5.2. In the cases where the Authority acted as lead supervisory authority in 2020, following reconciliation with the concerned supervisory authorities, five cases were closed finally and the administration of an additional thirteen cases is currently in progress at the Data Protection Department of the Authority. Of the 13 cases in progress, currently the Authority is working on the preparation of the draft decision in 6 cases, the others have progressed to the next phase and the reconciliation of the draft decision is in progress among the EU supervisory authorities. Of the cases received until the end of 2020, there were 2 cases in which investigation by the Authority led to the conclusion that it does not qualify as the lead supervisory authority because in contrast to the preliminary evaluation of the sending authority, it could not identify a controller with a centre of activities in Hungary and in another case, the Authority established lack of competence and transferred the complaint to the Hungarian National Authority for Media and Communications. Of the altogether 18 cases dealt with by the Data Protection Department 3 were received in 2018, 8 in 2019 and altogether 7 new cases were received in 2020.

5.2.1. During the period since the commencement of the application of GDPR, several complaints were lodged with the Authority concerning the sending of newsletters, data processing related to the customer accounts and the handling of data subject requests associated with these processing operations, of a business organisation providing passenger transportation services all over Europe, whose centre of activities is in Hungary.

In one case against the controller referred to above, the complainant lodged

a complaint with the Information Commissioner's Office, the data protection authority of the United Kingdom, in which he complained that although he had requested the controller in writing to terminate the user account registered with his e-mail address, but not created by him, the company failed to grant his request. (NAIH/2020/4204, NAIH/2019/405)

According to the position of the Authority, although the e-mail address registered with the user account is doubtless the personal data of the complainant, but the additional data registered with the account cannot be associated with the complainant, on their basis the complainant cannot be identified or, to be more precise, it is not the complainant that is identifiable. It follows that the complainant could have asked only for the erasure of its e-mail address and not that of the entire account. Because of this, the legal basis of being in contract invoked as the legal basis of processing cannot be applied because the contractual legal basis can be lawfully applied only if the data subject is one of the parties to the contract. According to the Authority's position, the complainant was entitled to request the erasure of his e-mail address from the company.

The Authority established that the controller carried out an infringement when it failed to take measures based on the erasure request of the complainant within a month, when it failed to notify the complainant of the fact of erasure and it also infringed the provisions of GDPR because it only met the erasure request with a substantial delay. However, in view of the fact that the company erased the complainant's user account and notified the complainant of this in a verified manner, the Authority did not apply additional legal consequences and closed the investigation with the agreement of the concerned supervisory authorities.

In the other case, the complainant lodged the complaint with the Data Protection Authority of Baden-Württemberg, in which he stated that he requested the erasure of his personal data and his e-mail address processed for the purpose of direct acquisition from the controller and also requested not to be sent any newsletters in the future, but the controller company did not comply with his requests. (NAIH/2020/5815, NAIH/2019/546)

In the course of its investigation, the Authority established that the complainant indicated his erasure requests through several channels of communication – in an e-mail addressed to the data protection officer of the controller and through the complaint management form accessible on the website of the company – in reaction to which the customer service of the controller informed the complainant of having received his erasure request and that it would investigate it as soon as possible but requested an additional eight weeks to take measures on the basis of the request in view of the fact that they received a large number of similar requests.

As the erasure request of the complainant was aimed in actual fact only at the erasure of a single e-mail address, it cannot be regarded either as complex or of a large number, i.e. the conditions on the basis of which the deadline for performance could have been lawfully extended did not exist with respect to the complainant's request, hence the company violated GDPR Article 12(3) when they failed to meet the complainant's erasure request within a month.

In relation to the Authority's draft decision, the Berlin and the Portuguese supervisory authorities submitted a relevant and reasoned objection in accordance with GDPR Article 4(24); these, however, did not concern the above interpretation of the law by the Authority and subsequently consensus was reached with respect to the content of the decision.

5.2.2. In his complainant lodged with the Berlin data protection authority, a complainant objected to the fact that he could not find a Privacy Statement on the website of the landlord of a Budapest apartment rented by him and a co-traveller, which is a business organisation with its registered offices in Hungary, and that he did not receive an answer to his access request sent to the contact e-mail address of the landlord. He also objected to the fact that the employee of the landlord wished to make a photo of his identification document and that the employee of the landlord uploaded the photo of the identification document of his companion to the landlord's WhatsApp group, which includes only a few employees of the landlord. (NAIH/2020/2305., NAIH/2019/3239)

In view of the fact that the landlord took action to meet the complainant's access request only after learning of the procedure of the Authority, and the complainant did not receive any information on the processing of his personal data for more than seven months from the submission of his access request, the Authority established the infringement of the GDPR provisions concerning transparency and an infringement of the complainant's right to access. It was also established that the controller failed to provide information about all the circumstances of data processing in accordance with the provisions of GDPR and through this, it infringed the complainant's right to access also in this respect.

As far as photocopying the ID card is concerned, the Authority established that the controller infringed one of the GDPR principles, that of data minimisation, by photocopying the identification document of the complainant's travel companion with the purpose of checking the correctness of the data given upon registration.

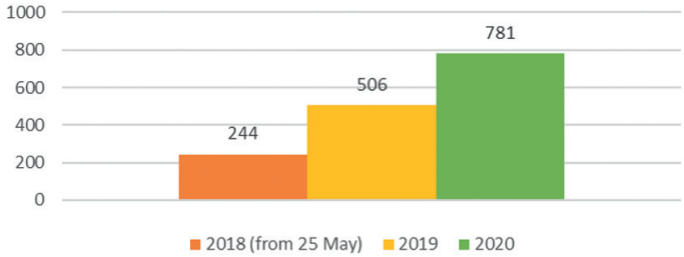
The employee of the controller did not have any of the legal basis under GDPR for uploading the photo made of the identification document to the WhatsApp group because the data subject did not grant his consent for that, it was not necessary for performing a contract, no legal regulation required him to do so, nor

did he have any legitimate interest in doing so that could override the interests and fundamental rights and freedoms of the data subject and the use of any other legal basis according to GDPR was excluded on principle. It follows that the Authority established that the employee of the controller provided access to the personal data of the complainant's companion to the other employees of the controller unlawfully without any legal basis.

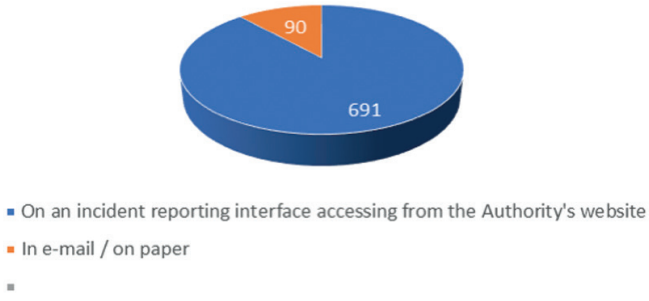
II.2. Reporting data protection incidents

In 2020, the Authority received altogether 781 data protection incident notifications, which is more than one-and-a-half times that of the number of notifications in the preceding year.

The number of data protection incidents reported to the Authority in an anual breakdown



Mode of notifing data protection incidents in 2020



II.2.1. Guidelines on data breach notification

The Authority was the lead rapporteur in drafting the guidelines regarding data breach notifications published by EDPB[6], which intends to provide assistance to controllers through fictitious but real-life data breaches cases so that they know what criteria to take into account when different types of incidents are detected to determine whether it is necessary to notify the supervisory authority about the data breach, or to inform the data subjects thereof, or whether it suffices just to record the data breach.

Article 33(1) of the General Data Protection Regulation states that it is not necessary to notify the data breach to the supervisory authority when "*it is unlikely to result in a risk to the rights and freedoms of natural persons*". Below, we present as few examples of frequent data breach types from the above guidelines, which are not required to be notified to the Authority provided that all the individual circumstances of the case correspond to those described in the guidelines.

An incident not requiring notification to the Authority may include, where appropriate, a ransomware attack of the controller's IT system provided that in the course of the investigation of the data breach, an independent IT expert concluded that there was no data loss or third party data copying and the controller had adequate security backups to fully restore the data encrypted by the virus within a short period of time. The situation is similar when there is unauthorised access to a database containing personal data protected by industry-standard (state-of-the-art) encryption and the encryption key has not been exposed or compromised. It is also not necessary to notify the cases when personal data are accidentally forwarded to a "reliable" third party, the wrong addressee himself notifies the incident to the controller and there is a binding relationship between the controller and the third party, on the basis of which the controller can require the third party to erase the personal data of which it has become aware, which can be shown to be irretrievable.

6 https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf

II.2.2. Significant data breaches

1. The data breach at the Health Centre of the Hungarian Army

A Member of Parliament lodged a complaint with the Authority in which he described that two articles were published on an Internet portal on 12 February and then on 13 February 2019 , in which it was disclosed that the Member of Parliament had earlier requested an entrance permit to the Health Centre of the Hungarian Army (hereinafter: MH EK). The portal published the scanned version of the request sheet submitted by the Member of Parliament. According to the complaint, the Member of Parliament had not disclosed the request sheet anywhere, he only sent it to MH EK scanned electronically.

Based on the complaint, the Authority held an official supervision on 25 March 2019 and then in view of the findings of the supervision, it launched its data protection procedure against MH EK on 24 May 2019. The Authority closed its data protection procedure with its decision NAIH/2019/2485/20 on 24 October 2019. In its decision, the Authority established an infringement in relation to the data processing operations of MH EK, because it did not have breach management rules during the period of the onset of the data breach which, based on GDPR Article 32(1) and Article 24(1) and (2), would have been expected of it in the case of an institution processing a large number of special category (health) data. In addition, the controller failed to meet its obligation according Article 33(1) of the Regulation on notifying breaches to the Authority without undue delay, not later than 72 hours after having become aware of it and it also failed to meet its obligation of documentation according to GDPR Article 33(5). Based on the infringements, the Authority imposed a data protection fine of HUF 2,500,000 on MH EK.

In the administrative litigation in progress in 2020, both the Fővárosi Törvényszék (Budapest Court of Appeal) and the Kúria (Supreme Court) upheld the decision of the Authority without any modification.

2. Data breach at DIGI Távközlési és Szolgáltató Kft.

DIGI Távközlési és Szolgáltató Kft. (hereinafter: DIGI) notified a personal data breach to the Authority on 25 September 2019, according to which an attacker making use of a vulnerability accessible through the www.digi.hu website accessed the personal data of some 322,000 data subjects, most of whom

(roughly 297,000) were its customers and subscribers, a smaller part (appr. 25,000) were subscribers to its newsletter. The personal data of the subscribers included the data subjects' name, their mother's name, place and date of birth, address, ID card No. (in some cases the personal number), e-mail address, landline and mobile phone numbers.

The greater part of the data of the data subjects concerned in the breach (appr. 297,000) constituted part of a database created for testing purposes on 21 April 2018. According to DIGI's assumption, the data were uploaded to the test database in order to temporarily debug the system to ensure the accessibility of subscriber data. The source of the data uploaded to the test database created in the course of the debugging process was the customers who provided their personal data online or through other sales channels for the purpose of entering into a contract of subscription with them.

After debugging and the re-establishment of access, the data uploaded to the test database should have been erased; this, however, was omitted. DIGI had no knowledge of the accessibility of these data through the above vulnerability until the notification of the attacker. They have not been able to detect the access to the data by the attacker (for instance based on the alert of a network security device), until the attacker himself called attention to it.

In its decision, the Authority established that DIGI infringed Article 5(1)(b) ("purpose limitation") and (e) ("limited storability") of the General Data Protection Regulation when it failed to erase the test database originally created for the purpose of debugging after running the necessary tests and debugging, so the large number of customer data in it were stored without a purpose and in a manner suitable for identification in the systems used for the next almost one-and-a-half year period. The absence of this measure directly enabled the data breach and the accessibility of the personal data.

In addition, DIGI infringed Article 32(1)-(2) of the General Data Protection Regulation when it failed to implement appropriate technical and organisational measures to ensure a level of security, appropriate to the risk through the fact that by exploiting a vulnerability of the content manager it used, which was otherwise known for more than 9 years and could be detected and debugged using the appropriate instruments, enabled access to the databases affected by the breach through the publicly accessible digi.hu website.

In view of the above, the Authority imposed a data protection fine of HUF 100,000,000 on DIGI. An administrative litigation is in progress in relation to the Authority's decision.

3. Data breach at Hungária Med-M Kft.

The Authority received notification in the public interest, according to which the medical findings and referrals processed in the appointment scheduling system of the website operated by the controller were accessible to the public and unauthorised users could download them. The Authority carried out an official supervision after which it launched its data protection procedure concerning the case.

The Authority has concluded that there is a genuine information leakage (directory browsing) vulnerability. The vulnerability affected two websites, where the .pdf documents were stored containing the medical findings of the patients. By calling the URLs, the web server listed all the content on the web server to the screen instead of displaying the requested interface. This allowed anyone with knowledge of the links to access the documents stored on the online interface without registering on the site. The vulnerability may have been the result of the fact that the controller used inappropriate configuration settings on its server, as a result of which the server displayed the director structure of the website by calling the URLs affected.

The controller was unable to accurately specify since when that vulnerability existed, it only learned of it from the NAIH decision. Based on the log files, it was unable to establish unauthorized access, hence in the course of the risk analysis carried out in relation to the breach, it established that it was unlikely to carry any risk with respect to the rights and freedoms of the data subjects, so it did not find the notification of the breach and the provision of information to the data subjects warranted.

In its decision the Authority established that owing to the inability of the client to demonstrate external accesses, it infringed the provisions of GDPR concerning the security of data processing, as well as its obligation to notify data breaches, because it failed to notify the Authority of the fundamentally high-risk data breach without undue delay after it became aware of it and also failed to inform the data subjects of it. The Authority imposed a data protection fine of HUF 7,500,000 on the controller.

4. Data breach at ROBINSON TOURS Kft.

The Authority received notification in the public interest, according to which the personal data of the customers using the travel services of the company could be accessed by anyone through the website operated by ROBINSON TOURS Kft., which included the names of passengers, their access data, address data, ID card and passport numbers, data related to reservations and travelling, dates and destinations, contracting and the specific travel contracts that could be downloaded in .pdf format According to the notification, the person who submitted it realised this when he entered his father's name in Google's search engine and through one of the hits he was able to open the database without any kind of access control. This means that Google's search engine detected the database and made the data stored in it searchable.

The Authority also checked and documented the accessibility of the database and the downloadability of the contracts, then it launched an official supervision followed by its data protection procedure against the travel agency as controller and the undertaking entrusted with the development of the website as processor.

In the course of its data protection procedure, the Authority established that because of omitting to take certain IT security measures (e.g. testing, testing for vulnerability) in the course of developing the website of the travel agency and the negligent design of the website, a security gap remained enabling access to the database by the public. The origin of the problem was that the customer data continuously uploaded to the live database of the travel agency containing the contract data were transferred through a "forgotten" connection point to the test database created earlier by the website developer. However, as the test database was inadequately protected, it became accessible to anyone through the website, thus practically anyone could monitor through the Internet the updating and processing of the data of the customers wishing to travel. Neither the controller, nor the processor were aware of the accessibility of the database by the public, they only learned of it from the Authority's order clarifying the facts of the case.

Through this vulnerability, altogether 309 travel contracts could be accessed, containing roughly 2,500 personal data of 781 data subjects until the vulnerability was terminated. The data subjects included children. The vulnerability existed for about three months.

In its decision, the Authority established that the controller travel agency infringed Articles 25, 32 and 34 of the General Data Protection Regulation because it

entrusted an unsuitable processor with the design of the website, it was unable to guarantee the security of the personal data processed and failed to inform the data subjects of the high-risk data breach. The Authority also established that the processor entrusted with the development and operation of the website also infringed Article 32 of the General Data Protection Regulation as it failed to subject the website to the appropriate security testing and vulnerability testing and it acted with a highly degree of negligence when developing the website. Based on the above, the Authority imposed a data protection fine of HUF 20,000,000 on the travel agency and HUF 500,000 on the website developer.

5. Data breach at a controller providing financial services

A financial service provider controller notified the Authority of a data breach, in the course of which business documents (contracts, statements of portfolio) prepared and printed for the individual customers for ad hoc use (in .pdf format) became accessible to the public from one of the websites of the controller from the business systems via an Internet interface created by it for sharing data because of a faulty setting. Of the data of about 200 customers stored on the website affected by the breach, the personal data of 50 customers were affected: data related to identity (name, place and date of birth, ID card number, tax identifier, citizenship), identification data, contact data (address, e-mail address, phone number) and economic and financial data (portfolio value).

The incident was caused by a misconfiguration on web servers providing content towards the Internet, which caused the default setting to be in effect, making the directories and files on the mounted drive accessible. Another consequence of the default configuration was that personal data could be accessed without any authentication through the URLs affected by the breach and it was also possible to list the directory.

The procedure of the Authority extended to investigating the performance of the controller obligations related to the breach and the data security measures taken by the controller. The Authority did not find any infringement in relation to the obligations according to GDPR Articles 33-34. However, the Authority investigated the enforcement of the requirement of data security according to GDPR Article 32 in relation to the processing concerned in the breach. The Authority found that there were measures taken to guarantee the security of the personal data processed by the controller; these, however, were inadequate and insufficient to actually guarantee the security of personal data, that is why the data breach could take place.For example, the controller could have been expected to have the

vulnerability test, otherwise carried out regularly by internal and external experts, extended to checking the misconfigured system. Applications are available to test for vulnerabilities, which can screen for this type of misconfiguration that led to the breach of confidentiality in the case of the specific incident The controller could also have been expected to disable the search bots of the search engines in the case of the processing under study, that is banned the listing of the data stored in the web server, i.e. to prohibit the listing of data stored on the web server.

In view of the inadequate security measures, the Authority established infringement of GDPR Article 32(1)(b) and (d), for which it imposed a data protection fine of HUF 2,000,000 on the controller.

II.2.3. Data breaches notified based on the Privacy Act

With regard to data processing for law enforcement, defence and national security purposes subject to the Privacy Act, the Authority received several notifications from the police and – presumably because of a higher level of data protection awareness – from the National Tax and Customs Administration and penitentiary institutions in 2020. Last year, controllers subject to the Privacy Act generally met their obligations to notify breaches on time.

The reasons for the onset of the data breaches continue to be characteristically negligent actions within the organisation that do not qualify as mala fide, for instance document sent to the wrong addressee or lost data medium. Unauthorised queries and inspections, however, also took place.

The case when a data breach did not remain latent can be highlighted as good practice because the exploration of the breach was the result of comprehensive internal data protection checks by the police acting as controller.

Taking disciplinary action against the person to whom the breach can be attributed remains very frequent among the measures taken to handle the breach. The Authority emphasised also in the previous year that, from a data protection perspective, measures to mitigate the potential negative consequences of the incident and other measures are relevant. In this context it can be established that in order to avoid similar breaches in the future and to improve data protection awareness, controllers should provide data protection training to their staff and review the work processes affected in the breach and modify them or incorporate additional checks (for instance to avoid sending documents to the wrong addressee) after such breaches.

The Authority found that when notifying breaches controllers typically do not place sufficient emphasis on presenting the data security measures preceding the breach, even though the Authority when investigating the breach notification takes into account whether the controller took the necessary measures to avoid the breach in order to exclude or at least minimise the breach or its detrimental consequences.

On several occasions, the controllers explained the absence of notification to the data subjects by stating that they carried out the appropriate technical and organisational protective measures, applying them to the data affected by the data breach, in particular, measures that would render the data incomprehensible to persons unauthorised to access the personal data.

There was a case, however, when following notification the official supervision revealed that the measure to which the controller referred to under the relevant point of the notification (training of the staff) would not result in the improbability of detrimental consequences from the data breach – i.e. the controller had no grounds to refer to it as a reason for waiving the notification of data subjects.

II.3. Cases of litigation for the Authority

In 2020, the Authority had altogether 25 finally closed cases of litigation before the Budapest Court of Appeal and the Supreme Court.

Of these, the Authority won the case in 20 litigations[7], partially won the case in 2 litigations[8] and lost the case in 2 litigations[9], 1 procedure was terminated by the court[10] because of the *nolle-pros* of the petitioner.

Below, we present a few interesting cases, as well as some of the cases fundamentally affecting a wide range of debt collectors and their customers as data subjects.

7 NAIH/2017/148/98.; NAIH/2019/3620/5., NAIH/2018/3102601/H., NAIH/2018/1031/H., NAIH/2019/3633/10., NAIH/2019/2485/20., NAI/2019/2566/8., NAIH/2019/167/13., NAIH/2019/2485/17., NAIH/2019/2668/2., NAIH/2019/214/23., NAIH/2019/5630/30., NAIH/2019/3990/25., NAIH/2020/610/4, NAIH/2020/146/5., NAIH/2020/186/4., NAIH/2019/3107/7., NAIH/2019/1189/11., NAIH/2019/56/6. NAIH/2018/21/34/H.

8 NAIH/2018/698/5/H., NAIH/2020/974/4.

9 NAIH/2020/306/8., NAIH/2019/7223/7. – In these cases, the court did not rule on the substantive issue, but only ordered further clarification of the facts of the case.

10 NAIH/2020/5552.

1. Data breach at a political party

In its decision NAIH/2019/2668/2 of 21 March 2019 the Authority established that a political party acting as controller failed to meet its obligations of data breach notification, documentation and providing information to the data subjects as set forth in GDPR Articles 33-34 with respect to a data breach affecting a database comprising the data of more than 6,000 data subjects it processed. Because of this, the Authority imposed a data protection fine of HUF 11,000,000 on the party.

Based on a report in the public interest in August 2018 related to the data breach, the Authority first carried out an official supervision and subsequently launched its data protection procedure. According to the report in the public interest, there was a comment in a hacker forum calling attention to an IT security vulnerability (SQLi) on the website operated by the party. Exploiting the vulnerability, the hacker writing the comment was able to access a database, which contained several personal data of the members and sympathisers of the party (name, e-mail address, user name, function in the party, weakly encrypted password). The hacker published the database in the forum and, as he said, he also called the attention of the controller to it. However, the controller failed to notify the Authority of the breach and also failed to inform the data subjects.

In the course of the Authority's procedure, the party adopted the position that as the stored data have not been updated for years, they were therefore outdated and an incident resulting from the disclosure of such a database did not need be notified to the supervisory authority and they did not need to inform the data subjects of it either. In its decision, the Authority argued for the high risk to the rights of data subjects because sensitive conclusions could be drawn as to political opinions and party affiliations even from the data that have not been updated for years. Also, the use of the weak password encryption (MD5 algorithm) could jeopardise the privacy of the data subjects. Because of this, the Authority therefore considered the provisions of GDPR for the management of data breaches applicable to the above case.

The party requested the review of the lawfulness of the decision. In its petition, it invoked the fact that as the vulnerability giving rise to the data breach existed even prior to 25 May 2018 when GDPR became applicable (since April 2018), it did not need to apply the provisions of the regulation concerning the management of data breaches. In addition, it also disputed the equitableness of the fine because of its proportionality and the disregard for the party sources of revenue. The Authority requested dismissal of the petition.

In the judgment of the first instance, the court shared the position of the Authority and pointed out that the GDPR provisions concerning the management of data breaches has to be applied to this data breach, because the vulnerability continued to exist even after the regulation became applicable and the controller became aware of it. In terms of a reassessment of the criteria concerning the extent of the fine, the court of the first instance instructed the Authority to pursue a new procedure. Both the petitioner and the Authority submitted an appeal against the judgment of the first instance not yet final to the Supreme Court as court of the second instance.

According to the judgment of the Supreme Court, the part of the Authority's decision concerning the imposition of the fine complied with the requirements set forth in Section 85(5) of the Administrative Litigation Procedures Act. The Supreme Court underlined that, among the criteria listed in GDPR Article 83(2), the Authority had to assess the circumstances that were relevant to the given case. The criteria not mentioned in the decision have to be regarded as not having been considered by the Authority as significant for the purposes of imposing the fine and they could not be taken into account either positively or negatively.

A decision brought within the powers of weighing is in violation of the law, if the process of consideration and the weighing of the criteria taken into account cannot be established from the justification of the decision, individual criteria were considered contrary to causality or documentary evidence and if elements significant from the viewpoint of all the circumstances of the case were disregarded, or if circumstances were evaluated that have no actual legal significance in the context of the infringement giving rise to the legal consequence.

The Supreme Court decision underlined that a decision brought within the powers of weighing does not violate the law merely on the basis that it presents only those of the weighing criteria specified in the legal regulations which were regarded relevant for the given case by the Authority and it did not list the elements, which had no significance, which were not evaluated or which could not be interpreted in the given case *(Kúria Kf.III.37.998/2019/10.).*

2. "Let us join the European Prosecutor's Office" initiative

In the course of the initiative entitled "Let us join the European Prosecutor's Office" (hereinafter: initiative) the petitioner, a Member of Parliament, collected the names, addresses, e-mail addresses, phone numbers and signatures (hereinafter

jointly: personal data) of the data subjects on the sheet for expressing support for the initiative, according to the Privacy Statement printed on the back of the sheet (hereinafter: Privacy Statement) in order to be able to provide information concerning his parliamentary activities.

Information on the primary purpose of data processing was provided on the front of the sheet and there was no indication at the individual data whether providing them was mandatory or optional for supporting the initiative. Below the table for filling in the data, there was the following caption: "I support Hungary's joining the Institution of the European Prosecution with my signature", there was information of the mode of returning the sheet and the following text: "Privacy Statement – I accept the Privacy Statement with my signature […] Privacy Statement on the personal data processed by the staff of […] and his colleagues." The information on the back of the sheet states that "The legal basis of processing is your express consent given after reading this Privacy Statement".

According to the information provided the petitioner would submit the sheets at the latest on 31 May 2019 to the public notary, irrespective of the number of signatures collected. There was, however, no information about what was going to happen to the sheets and the data following their submission to the public notary, or if the number of signatures is collected was not sufficient.

During the period of signature collection, there was a possibility to upload the completed sheets online, for which it was necessary to provide the name, e-mail address, county, settlement and phone number and the Privacy Statement had to be accepted according to which the purpose of processing was taking up and maintaining contact with those supporting the European Prosecution and informing data subjects of the activities supporting the European Prosecution related events, movements and signature collections.

In the course of the online uploading, the data subjects gave their consent to the processing of the data by providing their personal data in the fields whose completion was mandatory and ticking the box beside the Privacy Statement. Without this, it was not possible to upload the sheets. Anyone was able to upload the form online. In the case of online uploading, there was no separate opportunity to subscribe to the newsletter in the form whose completion was mandatory and there was no information on the period of processing of the data uploaded online.

Because of non-compliance with the repeated calls for the erasure of personal data in the course of its investigative procedure launched ex officio, the Authority launched its data protection procedure ex officio.

In its decision NAIH/2020/974/4 of 9 July 2020, the Authority

- established that the controller collected the personal data of the data subjects without a legal basis for the purpose of maintaining contact related to the initiative called “Let us join the European Prosecution” in the period between 19 July 2018 and 30 May 2019 and infringed GDPR Article 6(1) and Article 9(1)

- established that by not providing appropriate information on all the essential circumstances of processing, the controller infringed GDPR Article 5(1)(a), Article 5(2) and Article 13

- instructed the controller to erase all the personal data collected from the data subjects for the purpose of maintaining contact in relation to the initiative called “Let us join the European Prosecution” between 19 July 2018 and 30 May 2019 within 30 days from the decision becoming final; an

- imposed a data protection fine of HUF 1,000,000 on the controller.

The petitioner requested the review of the lawfulness of the decision from the Budapest Court of Appeal. According to his position, the qualification of contact data as special category personal data is excluded, so there is no need for an express consent for the processing of these data. With respect to informed consent, he explained that it is sufficient to provide the identity and the purpose of the controller, and other deficiencies of the information provided do not affect the legal basis. He declared that the information provided complied with the provisions of GDPR Article 13(2)(a).

Concerning the part of the decision ordering erasure, he declared that the Authority may order the rectification or erasure of personal data or the restriction of data processing only in accordance with the provisions of GDPR Articles 16, 17 and 18 and the power of rectification according to Article 17 may be used if the data subject requests the erasure of his personal data making use of his rights according to this Article, hence the Authority exceeded its powers when requiring erasure in its decision.

In its judgment, the Budapest Court of Appeal annulled the point of decision NAIH/2020/974/4 concerning the instruction to erase personal data, beyond this, however, it rejected the petition of the petitioner.

According to the justification of the judgment, the petitioner processed personal data for the purpose of providing information on his public activities pursued as

a Member of Parliament and they constitute data reflecting political opinion by virtue of a political viewpoint that can be identified by deduction on the basis of the need to inform about or maintain contact with a politician, taking into account the purpose of the initiative and the need to provide information about the petitioner's political activities in support of the initiative. Because of this, the personal data were special category personal data, whose processing required more than just consent according to GDPR Article 6(1)(a), it required express consent by the data subject according to GDPR Article 9(2)(a). The absence of express consent was substantiated by the circumstance that the signature of the data subject did not apply to processing the data but to supporting the initiative and that he accepted the Privacy Statement with his signature. Providing the requested data in the sheet and accepting the Privacy Statement by signature in themselves does not constitute an unambiguous act of confirmation of consent to the use of special category personal data.

In accordance with the position of the Authority, the Budapest Court of Appeal underlined that the data subjects' consent may not be extended to additional purposes other than the original purpose of data processing affected by the consent. The signatures were collected not only to support the initiative because for this purpose, the petitioner only collected the data of name, address and signature. When the phone number and/or e-mail address were also provided, all the data have become the subject to data processing for an additional purpose, that of maintaining political contact.

According to the position of the court, the Authority lawfully imposed the data protection fine on the petitioner. In this respect, it declared that the Authority appropriately assessed the relevant facts of the case when imposing the fine, the amount of the fine was not excessive relative to the amount of the remuneration the petitioner received as a Member of Parliament.

According to the justification of the order requiring the annihilation of the part concerning the erasure of the personal data, ordering the erasure of personal data is only possible based on the request of the data subject, the Authority made its decision by infringing his powers and was not authorised to instruct the petitioner to erase the personal data as a legal consequence of the established infringement. *(Fővárosi Törvényszék 105.K.706.125/2020/12.).* In this context, the Authority launched a review procedure before the Supreme Court, the Supreme Court accepted the petition for review and the procedure is in progress.

3. Judgment concerning the legal basis of transfer

The facts of the case

On 18 May 2000, a complainant concluded a loan contract with a bank. The bank terminated the loan contract with immediate effect on 8 May 2002, then it sold its claim arising from the contract, which was eventually transferred to the petitioner debt collector after several transfers.

In his complaint lodged with the Authority, the complainant requested the Authority to order the erasure of his personal data, in view of the fact that, as he stated, the above loan has already been repaid, hence the debt collector should not process his personal data.

According to the statement of the debt collector made in the course of the data protection procedure, it processed the data of the complainant for three purposes: pursuant to GDPR Article 6(1)(b) it processed the data obtained through the contract of transfer for the purpose of collecting the claim, pursuant to GDPR Article 6(1)(c) it processed certain personal data for the purpose of complaint management, and pursuant to GDPR Article 6(1)(c) it processes additional data for transferring reference data to the central credit information system (hereinafter: KHR).

It its decision NAIH/2019/2566/8 of 8 August 2019, the Authority established that the debt collector cannot lawfully process the personal data of the complainant with reference to the legal basis of a contract according to GDPR Article 6(1)(b). The Authority instructed the debt collector to demonstrate to the complainant, if it has a legitimate interest in processing the personal data of the complainant for the purpose of collecting the claim and this interest overrides the fundamental rights of the complainant and pursuant to GDPR Article 14(2)(b) to inform the complainant based on what legitimate interest it is necessary to process his personal data for collecting the claim and whether this interest overrides the fundamental rights of the complainant and to inform the complainant of his right to objection and about how he can exercise that right. If it is unable to demonstrate the legitimate interest, it should erase the data.

The court procedure of the first instance

The petitioner debt collector submitted a petition against the decision of the

Authority. In its petition, it requested the alteration of the decision and the establishment of the fact that the decision was in violation of the law and the declaration of the fact that the petitioner debt collector may process the personal data of the complainant on the legal basis of performing a contract according to GDPR Article 6(1)(b) in order to be able to perform the contract, which means that it has no obligation to verify its legitimate interest in processing the personal data for the purpose of collecting the claim. It also requested the establishment of the fact that because of the lawful processing of the data, there is no need for restricting data processing or to erase the personal data.

According to the position of the petitioner, the underlying civil legal relationships have also to be analysed in relation to this case. As presented by it, a contract – when terminated –is terminated with respect to the future pursuant to Section 525(1) of Act IV of 1952 on the Civil Code (hereinafter: old Civil Code), its Section 321(1) and the explanation of the old Civil Code, and this provision means that the services provided on the basis of the contract are due back – i.e. a contract is fully terminated when the parties have fully met their obligation of settlement set forth in the legal regulation and otherwise in the loan contract. It follows with respect to the present case that the personal data of the complainant have to be processed with a view performing the remaining provisions of the contract in relation to that. According to the point of the petitioner's argumentation, the claim is not separated from the basic legal relationship through the transfer.

In relation to processing data for the purpose of collecting the claim it explained that the purpose of processing is the enforcement of the obligation to settle, which survives the termination of the loan contract, in particular the enforcement and collection of the claim, or in other words, forcing the obligation according to the contract outstanding between the creditor and the debtor, hence, according to its position, the contract as a legal basis according to GDPR Article 6(1)(b) can be applied.

With respect to the interpretation of the civil law by the petitioner, the Authority expounded that if a contract is terminated, data processing is not possible on the legal basis of performing the contract and although it is not disputed that a settlement obligation remains, this, however, does not mean that the contract as legal basis could be applied.

From the viewpoint of data protection, the contract and the obligation to settle following termination are separated from one another and in contrast to the

petitioner's argumentation, the issue of statutory limitation is relevant only in so far as in the event of a claim that cannot be enforced through a court, the petitioner as controller has, in particular, to take into account the reality of voluntary performance and to carry out the interest assessment in view of this.

The Authority also mentioned the unbroken practice that the legal basis of performing a contract is to be taken stricto sensu, which is reinforced by the opinion according to the Recommendation of the Working Party[11] ("Article 7(b) applies only to what is necessary for the performance of the contract, it does not apply to additional steps caused by non-performance, or to other events arising upon the execution of the contract. The more sophisticated data processing, in which third parties are also involved, such as debt collection or bringing a customer who fails to pay for a service to justice, is carried out not in the course of the ordinary performance of the contract, hence they are not subject to Article 7(b).")

Judgment of the court of the first instance

The Budapest Court of Appeal rejected the petition of the petitioner and found the references in the petition to legal issues, thus the infringement of substantive law unfounded. The Budapest Court of Appeal explained that the Authority took the correct position with regard to the fact that the legal ground of the contract according to GDPR Article 6(1)(b) may only be applied when it is necessary for the performance of the contract and this legal ground may not be extended to data processing operations, which become necessary to remedy the situation created because of the non-performance of the contract by the data subject; this legal ground cannot be applied to the case when the controller transfers its claim against the data subject because of failure to perform to an undertaking pursuing debt collection. The precondition of data processing on this legal ground is that the contract exists, that it is valid and in force when data processing is carried out with reference to its performance.

The Budapest Court of Appeal agreed with the legal interpretation of the Authority, according to which the transfer is the transfer of the ownership right to the claim, through the transfer the claim becomes separated from the original legal relationship, from which it stems and the transferor is replaced via the transfer only in respect of the claim and not the underlying legal relationship. However, by separating the claim from the underlying legal relationship and making the transferee the obligor of the claim, the enforcement of the claim by the transferee

11 Opinion 06/2014 on the notion of legitimate interest of the data controller under Article 7 of Directive 95/46/EC

and the related data processing no longer takes place with a view to the performance of the contract, from which the claim originally stemmed.

With respect to the situation of the petitioner, the court of the first instance stated that as transferee it takes action for the purpose of collecting the claim in his own interest and on his own behalf because getting the obligee to perform and processing the data to that end serves the legitimate interest of the petitioner and not the performance of the contract on which it was based (as the claim has become independent of the contract through the transfer). The court underlined that there was no contractual legal relationship between the petitioner and the complainant, which from the viewpoint of data processing means that based on the receipt of the data as part of the transfer, it can only have other legitimate interests, typically the transferee's legitimate interest in enforcing the claim for its own benefit.

It follows that the petitioner processed the personal data with reference to the performance of a contract, which was terminated, i.e. it was unsuitable to have a legal impact, thus it could not lawfully invoke GDPR Article 6(1)(b) as the legal basis of processing.

The Budapest Court of Appeal highlighted that it regarded the interpretation in the Guidelines of the Board[12] as governing, according to which performance of the contract as legal grounds is to be taken *stricto sensu* and it does not automatically extend to data processing arising from non-performance and the performance of the contract as legal basis covers only the sending of a payment reminder or data processing related to returning to the ordinary course of the contract but not the data processing for the purpose of claims management following the termination of the original contract *(Fővárosi Törvényszék 105.K.700.451/2019/9.).*

12 Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) of the General Data Protection Regulation in the context of the provision of on-line services to data subjects

The judgment of the Supreme Court

The Supreme Court upheld the judgement of the first instance.

The Supreme Court underlined that the petitioner became the obligor of the claim not directly through transfer by the original obligor and not before the termination of the loan contract. The Supreme Court's position was that the settlement obligation outstanding after the termination existed only in the interest of settling the claim through an extraordinary procedure. The legal relationship of settlement does not mean a contractual legal relationship, the petitioner does not take action directly on the basis of the loan contract, which had incidentally been terminated earlier with a view to managing and collecting the claim, it enforces its own claim on its own behalf and for its own benefit. Which means that this is taking place not in order to force the complainant debtor "to perform according to contract" – performance according to contract (according to the loan contract) in this phase is notionally excluded – instead the purpose of the petitioner is to collect the independently transferred claim.

According to the Supreme Court, the court of the first instance correctly invoked the provisions of the Board Guidelines and the Working Party Opinion, which were also referred to by the Authority for the interpretation, because they allow the conclusion that only a payment reminder and administration directly related to the underlying contract or directly following its termination allow for the reference to the legal ground necessary for the performance of the contract for the processing of personal data. In the case under litigation, the loan contract was terminated by cancelling it, the transfer of the claim does not change this, the legal relationship of settlement does not correspond to the contractual relationship *(Kúria Kf.V.39.291/2020/5.)*.

4. Data processing by the Hungarian Church of Scientology and the Central Organisation of the Church of Scientology

The Authority presented its data protection procedures launched against the Hungarian Church of Scientology (hereinafter: MSZE) and the Central Organisation of the Church of Scientology (hereinafter: MSZE Central Organisation) investigating the lawfulness of their data processing in detail in the 2017 and 2018 annual reports. It is necessary to outline the case in this report in view of the judgment of the Supreme Court made in a review procedure.

In its data protection procedure launched ex officio, the Authority investigated the electronically managed records of MSZE and MSZE Central Organisation, the

processing of personal data contained in the various types of folders processed in relation to the services of the Church [PC folder (notes, protocols, worksheets, reports generated in the course of auditing and detoxification service), Ethics folder, Correspondence folder, Staff folder], the various data processing purposes and data processing with the purpose of direct marketing.

In the case of PC folders, the Authority established that in the information in the statements signed by clients prior to the commencement of the services, the Church does not provide sufficient information as they do not indicate unambiguously the identity of the controller and there is a very brief presentation of the purpose of processing. In the case of such complex data processing, when a very large amount of personal data is processed as in the processing operation under study, the purpose of processing must be indicated much more accurately and much more comprehensively. Also, there must be an accurate description of the kind of data that need to be processed and in what way they are used to achieve the purpose indicated, because it is only in this way that a data subject can decide whether or not to consent to the processing. Information provided does not accurately identify which Church personalities, officers, staff members are authorised to access the data, it does not provide full information on data subjects' rights and the available possibilities of legal remedy and they do not obtain a separate consent for data transfers.

In the case of the detoxification programme, the Authority established that only the examining physician or health care service provider may process the recorded health data, condition assessment and findings based on consent and they could only forward the information on whether the data subject meets the conditions of participating in the programme; however according to the position of the Authority, the entire content of the statement including the detailed health condition assessment and medical findings of the data subject may not be handed over to a religious organisation.

It follows that the Church infringed Section 20(2) of the Privacy Act and because of the insufficient prior information it also infringed the requirements concerning consent according to Section 3(7) of the Privacy Act.

The Authority also established that in the course of auditing and detoxification, the Church processes special category data with respect to which Section 5(2) (a) of the Privacy Act may not be applied as the legal ground for processing special category data; furthermore, the legal ground according to Section 5(2) (c) of the Privacy Act cannot be established either in the course of processing by the Church, in view of the fact that the Church indicated religious services as the

purpose of processing and this purpose is not in line with Section 4(1) of Act XLVII of 1997 on the Processing and Protection of Health and related Personal Data (hereinafter: Health Data Act), which applies to data processing within the health care network, nor can the other purposes indicated in Section 4(2) of the Health Data Act. As detailed above, the consent as legal grounds indicated in Section 4(3) of the Health Data Act cannot be substantiated.

The processing of third persons' data was an infringement of outstanding weight as established in the decision. Pursuant to the definition of the Privacy Act, all the data that relate to a person other than the PC in the documents found in the folders qualify as third persons or rather personal data related to third persons. This includes, for instance, all the data related to the PC's relatives, friends, acquaintances and relationships. In several cases, the Church processed special category data of third persons in some documents, despite the fact that it had no authorisation to process them from the data subjects.

By processing the personal data of third persons, the Church infringed the principle of purpose limitation according to Section 4(1) of the Privacy Act. According to the Authority's position, the MSZE processes the personal data of third persons, while processing the documents stored in the folders without a specified purpose and appropriate information provided in advance.

On account of the above, the Authority prohibited the continued unlawful data processing by the obligees and called upon them to transform their practice of providing information in advance in accordance with the provisions of the Privacy Act and to request the consent to the data processing of all the data subjects or the confirmation of their consent. In the absence of confirmed consent, the Authority called upon the obligees to erase the data of the data subject in a documented manner. The Authority banned their practice concerning the collection of the personal data of third persons who do not qualify as staff members, applicants to staff position or believers and ordered the erasure of these personal data. It also called upon the obligees to terminate data transfers abroad and to comply with expectations on data security with regard to the transmission of personal data abroad.

In addition, the Authority imposed a data protection fine of HUF 20 million each on the controllers. When determining the amount of the fine imposed, the Authority took into account all the circumstances of the case, in particular the number of data subjects, the weight of the infringement and the recurrent nature of the infringement.

The controllers submitted a petition against decision NAIH/2017/148/98/H. The Budapest Court of Appeal rejected the petition *(Fővárosi Törvényszék 13. K.700.014/2018/60.).*

The petitioners requested a review of the judgment.

The judgment of the Supreme Court

The Supreme Court annulled the judgment of the Budapest Court of Appeal; it annulled points 159-170 of the Authority's decision containing the findings of the psychologist expert; beyond this, it fully rejected the petitioner's petition.

According to the justification of the judgment, no direct infringement could be established against the petitioners based on the psychological expert opinion obtained by the defendant Authority. According to the Supreme Court, the presentation of evidence, which does not constitute underlying evidence of the case within the facts of the case had an impact on the merit of the case because in addition to giving rise to misunderstanding on the part of clients, it gives rise to uncertainty in the course of the implementation of the decision; also, in view of the formulation of the operative part of the decision, it is not unambiguous whether the expert assessment carried out in relation to the statements of consent included in the justification of the decision should be taken into account in the course of the implementation of the decision.

In this context, petitioners had good grounds to plead infringement of the law in that the Authority did not disregard the findings of the psychology expert in the decision in spite of the fact that the Authority itself found that the expert opinion in question was not the basis for the decision.

Beyond this, the Supreme Court found the findings of the court of the first instance and of the Authority correct in all respect and pointed out that:

- in the event of ongoing data processing, data must be processed in accordance with the data protection provisions in force at all times, hence data collected under the former Privacy Act can be processed under the new Privacy Act if the controller guarantees compliance of processing with the provisions of the new Privacy Act;

- Section 6(4)(n) of the Church Act merely stipulates that data processing activity beyond what is necessary for activities related to religious life cannot in itself be regarded as religious activity and, furthermore, the conclusion that data

processing carried out in the course of religious activity may not be investigated by the data protection authority cannot be inferred from this provision by any method of interpretation;

- Section 71 of the Privacy Act grants clear authorisation to the data protection authority to process data, which qualify as confidential subject to professional secrecy to the extent necessary for the successful conduct of its procedure;

- the petitioners failed to verify the lawful purpose and need to process the data of third persons.

A Supreme Court highlighted that data processing for a religious purpose does not mean exemption from the objective scope of the Privacy Act and data processing for religious purposes must also meet the requirements specified by the Privacy Act *(Kúria Kfv.II.37.743/2019/21.).*

5. Accessibility of archive data

The Constitutional Court in its adjudication IV/584/2020 ABH rejected a constitutional complaint in a case concerning the accessibility of archive data, in which the Authority was also affected as defendant.

According to the facts of the case, in March 2016 a researcher registered with the proponent (the public archive) and completed a researcher data sheet for documents generated in the years 1959-1960-1961 for research into "contemporary crime" indicating that the research was "scientific" research. The public archive issued a visitor's pass to the researcher. On the same day, the visitor sheet received by the public archive referred to the following indicating specific surnames and given names: "XY, (and) associate – 1960". The public archive made ten pages of the forty-eight-page judgment of the first instance and three pages of the thirteen-page judgment of the second instance available to the researcher, all pages anonymised. After this, articles appeared on a website and they were taken over on several media platforms in April 2016 that XY was sentenced in the 1960s because of gang rape. The data subject then lodged a complaint with the Authority objecting to the publication of his personal data involved in a criminal case by an online crime magazine and an Internet portal without his consent.

In 2016, the Authority launched its data protection procedure ex officio on account of data processing activities related to the "judgment of the Budapest Court of Justice of 17 February 1962" (the Authority investigated the data transfer by the

researcher and the publication of personal data involved in a criminal case in a separate procedure). As a result of the procedure, the Authority established that the public archive unlawfully provided access to the 1962 judgment to a third person; because of this, it imposed a data protection fine of three million forints and instructed it to abide by the provisions of the decision when providing access to the 1962 judgment in the future and develop procedural rules, which ensure the appropriate application of Section 24(1) and (2)(a) of Act LXVI of 1995 on Public Documents, Public Archives and the Protection of the Materials of Private Archives.

In its petition, the public archive initiated the review of the decision, upon which the Budapest Administrative and Labour Court annulled the decision, but did not order a new procedure because an actual investigation of anonymisation carried out on the documents affected in the research was not the subject matter of the administrative procedure. The Authority submitted a petition for review against the judgment. The Supreme Court annulled the judgment of the court of the first instance, as well as the decision of the Authority and ordered the Authority to conduct a new procedure. After this, the public archive submitted a constitutional complaint to the Constitutional Court and requested the annulment of the judgment of the Supreme Court.

Having examined the constitutional complaint, the Constitutional Court arrived at the conclusion that it is not admissible. The condition of submitting a constitutional complaint is that the proponent could invoke the infringement of a right guaranteed by the Fundamental Law, but this submission fails to satisfy this condition. The public archive based the infringement of fundamental rights on the freedom of scientific research as set forth in Article X(1) and (2) of the Fundamental Law. In relation to this, the Constitutional Court underlined that right to the freedom of scientific life is due to everyone, but the actual beneficiaries of this freedom are the scientists. With regard to the specific case, it established that although the public archive referred to the fact that its responsibilities include pursuing archival and historic research, however, in the litigation on which the constitutional complaint was based it acted not as a researcher but as a controller.

Furthermore, the Constitutional Court mentioned that one can turn to the Constitutional Court against the decision of a court held to be anti-constitutional, if the decision made on the merits of the case or another decision concluding the court procedure infringes the proponent's rights set forth in the Fundamental Law and the proponent has already exhausted the possibilities of legal remedy. According to the practice of the Constitutional Court, the decision of the Supreme Court ordering the defendant to conduct a new procedure beside annulling the

decision of the court does not meet this condition because the procedure will then be continued and a possibility to submit a constitutional complaint will open at the end of the procedure, after the final judgment has been delivered.

III. Procedures related to the processing of personal data for the purposes of law enforcement, defence and national security

III.1. Data processing by penitentiary institutions

In 2020, the Authority received several requests and data subjects' complaints with respect to data processing by penitentiary institutions, of which the complainants objected to the processing of their health data generated during the enforcement of their sentence in numerous cases, but there was also a case when the penitentiary institute wished to use the personal data generated in the course of the enforcement of the sentence or those obtained in a civil litigation for damages, which the complainant objected to. The following has to be declared in relation to data processing by penitentiary institutions.

Pursuant to Article 2(2)(d) of the General Data Protection Regulation of the European Union, the Regulation does not apply 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, including the safeguarding against and the prevention of threats to public security.

Pursuant to Article 1(1) of (EU) 2016/680 of the European Parliament and of the Council 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 (Law Enforcement Directive), this Directive lays down the rules relating to the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection, prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

The General Data Protection Regulation is a legal act of the European Union, which is directly applicable, its provisions are in force in national law even without being transposed. The transposition of the Law Enforcement Directive was carried out by the Privacy Act, in addition to containing provisions for data processing operations subject to the General Data Protection Regulation. When

interpreting the provisions concerning data processing activities subject to the Law Enforcement Directive and regulated in the Privacy Act, the rules of the Law Enforcement Directive must be borne in mind as they provide a framework of interpretation for the assessment of the data processing operations.

In order to be subject to the scope of the Law Enforcement Directive, data processing operations have to meet two conditions:

- the purpose of data processing may be the following: prevention, investigation, detection, prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, and

- the controller is the competent authority defined in the Directive.

Pursuant to Article 3(7) “competent authority” means:

a) any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; or

a) any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

Pursuant to Article 9(1) and (2) of the Law Enforcement Directive, if competent authorities process personal data for purposes other than those of the Directive, the General Data Protection Regulation shall apply. So, there may be data processing when the competent authority is the controller, yet the data processing activity is subject to the scope not of the Directive but of the General Data Protection Regulation, in view of the fact that the purpose of processing does not correspond to the purposes of the Directive.

Pursuant to Section 1(1) of Act CCXL of 2013 on the Enforcement of Penalties, Certain Coercive Measures and Detention for Misdemeanours, the responsibility of the penitentiary institutions is to enforce the purposes of punishment through the execution of a sentence or a measure with a view to ensuring the criteria of individualisation in the course of enforcement, so that the punishment should appropriately serve the achievement of individual prevention goals. The purpose of punishment is defined by Act C of 2012 on the Criminal Code (hereinafter: Criminal Code). According to Section 79 of the Criminal Code, the purpose of

punishment is no other than the prevention of the committing of criminal acts by the perpetrator or by anybody else in order to protect society.

By virtue of its responsibilities and public powers, the penitentiary institution meets the notion of competent authority according to the Law Enforcement Directive. In view of the fact that its task is the enforcement of penalties, data processing operations carried out as part of this basic duty are subject to the Directive and the Privacy Act, which transposed the Directive into national law. At the same time, penitentiary institutions also carry out data processing operations, which are subject to the General Data Protection Regulation, but such processing of data is envisaged not in relation to the inmates, but in its role as employer or in some other role, i.e. not in the course of discharging its basic duty.

In addition to the Privacy Act and the Directive, the provisions of Act XLVII of 1997 on the Processing and Protection of Health and Related Personal Data (Health Data Act) govern the processing of health data generated in the correctional system.

When an inmate receives health care in the prison, that health care is part of the enforcement of the penalty, it is carried out within its framework and under its legal conditions, and the processing of the data generated in its course is subject to the Directive. However, when processing health data the provisions of the Health Data Act must always be borne in mind, as well as the fact that it is data processing subject to the Directive, which may not lead to a restriction of the exercise of the data subject's rights as far as his health data are concerned. If the inmate is treated in an institution outside the system of the penitentiaries in a hospital, i.e. he needs health care that the penitentiary institution cannot provide and because of this, the services of a health care institution are used, the processing of the data generated in the course of this type of care, which are processed not by the penitentiary institution but by the hospital, which does not qualify as competent authority, is not subject to the Directive. This data processing operation is governed by the rules of the General Data Protection Regulation (GDPR).

A case mentioned in the introduction and the penitentiary institution used the personal data generated in the course of the enforcement of the penalty or those obtained during that period, in a civil litigation for damages, is not a data processing operation subject to the Directive and the Privacy Act. This holds even if the personal data used were subject to the Directive in the course of an earlier processing operation because then the purpose of processing was truly related to the enforcement of the penalty and the inmate was the on other

side in the litigation. The enforcement of rights in a civil litigation as a processing purpose, however, is not closely related to the enforcement of the penalty, i.e. the enforcement of the purposes of punishment. That relates to the compensation for the eventual damage arising from what is going beyond the enforcement of the penalty, so it qualifies as a data processing relationship subject to GDPR.

III.2. The processing of personal data in decisions brought in infraction proceedings

Based on a citizen's report, the Authority investigated the lawfulness of processing personal data in a decision brought by BRFK District VII Police Station as infraction authority (hereinafter: Police Station) in an infraction procedure.

Based on the relevant legal regulations, the Police Station adjudicated several cases in a single procedure and issued a single decision against the persons subject to the proceedings. The decision contained the personal data of all the persons subject to the procedure. The Police Station communicated the decision to all the persons concerned, thus the persons subject to the procedure learned one another's personal data because of the communication of the decision.

Section 4(1) and (2) of the Privacy Act stipulated the principles of purpose limitation and data minimisation. Compliance with the principle of data minimisation guarantees that only the narrowest justified range of data are processed in view of the purpose of processing. The requirements of purpose limitation and data minimisation extend to all the stages of data processing, including the transfer of data.

The requirements of data protection by design and by default set forth in Article 20 of the Law Enforcement Directive, which sets forth obligations for the controller was transposed into Hungarian law by Section 25/A of the Privacy Act. Pursuant to Section 25/A(1) of the Privacy Act, it is the controller's responsibility to take technical and organisational measures appropriate to all the circumstances of processing, in particular its purpose and the risks to the fundamental rights of data subjects posed by processing, in order to ensure the lawfulness of processing. Such a measure may be anonymisation.

The right to the protection of personal data is a fundamental right guaranteed in Article VI of the Fundamental Law. In its decision 15/1991, the Constitutional Court pointed out that it interprets the right to the protection of personal data as a

non-traditional right of protection, but as a right to informational self-determination taking its active side into account as well. Accordingly, the content of the right to informational self-determination is that everyone shall provide for the disclosure and use of his personal data. The Constitutional Court decision referred to states that the fundamental guarantee of the exercise of the right to informational self-determination is the restriction of data transfer. The narrower meaning of data transfer is that the controller makes the data accessible to a specified third person. Personal data may be made accessible to a third person other than the data subject and the original controller only if all the conditions allowing for data transfer are met with respect to every single data.

The Authority's investigation established that via disclosing its decision brought in an infraction procedure, an infringement took place at the Police Station with regard to the processing of personal data, because as a result of the communication of the decision, the persons subject to the procedure learned about one another's personal data without legal authorisation or in the absence of the data subjects' consents, which meant that a data transfer to a circle greater than necessary was implemented.

The Authority called upon the Police Station as controller that in the event of cases adjudged in a single procedure with regard to a decision made against several persons subject to the procedure to take the necessary technical and organisational measures (for instance, sending an abstract of the decision) to prevent that the persons subject to the procedure to whom the decision is disclosed should learn one another's personal data as a result of the communication of the decision. Furthermore, pursuant to Section 96(1) of Act II of 2012 on Misdemeanours, Misdemeanour Proceedings and the Registration System of Misdemeanours, the Authority also called the attention of the Police Station to the fact that the decisions brought in infraction procedures must contain only the natural person's identification data of the person subject to the procedure, not the address.

In his response, the Budapest Police Superintendent informed the Authority that he agreed with the terms of the call and he ordered the provision of documented training on the data protection rules in order to avoid possible future breaches of rights in relation to the processing of personal data and the full application of the rules in infraction procedures and also sent a communication to the National Police Headquarters followed by action to update the Robotzsaru (Robocop) integrated administrative processing and electronic file management system to delete address data from the process-driven document templates. (NAIH/2020/4266)

III.3. Visit to the Headquarters of the Traffic Security Automated Processing Information System

As early as in 2019, the Authority commenced a dialogue with the Ministry of the Interior with a view to jointly review the legal regulations necessary for the operation of the VÉDA system and to discuss their eventual amendment, if necessary. As part of this, the staff members of the Authority paid a visit to Vásárosnamény, the Headquarters of the Traffic Security Automated Processing Information System (KAFIR) invited by the Ministry of the Interior and the National Police Headquarters, where they gained additional knowledge about the operation of the system, its IT background and the handling of cases by the Administrative Official Service. The primary purpose of the VÉDA system operated by the Police is to provide technical support for monitoring compliance with the rules of road traffic by the Police. The continuously operating video devices of the system were placed along the public roads of the country. Based on the images recorded by the VÉDA system, the recognition of the registration numbers of vehicles and their other individual characteristics and the filtering out of road traffic infractions are done in an automated manner. The system stores the data for thirty days.

The staff members of the Authority inspected a fixed location and a variable location complex traffic checkpoint on-site in operation, they understood the responsibilities of the police officer in their operation and what happens to the recorded data until the end of the process.

The Authority continues to maintain its earlier position even in the light of the information received in the course of the visit, according to which the legal regulation concerning the recording of images in force, i.e. the Act on the Police, requires a review. The rules on image capture cannot be properly applied to an automated monitoring system In spite of this, the rules in force are extended to the VÉDA system, whereby automated image recording also regarded as a measure, which is not in line with other legal provisions.

The nature and content of the legal regulations governing the system is essential because it is the legislation that can set the framework for the application of the technology. Until the problem is resolved in a reassuring way, an amendment of the legal regulation would be necessary on the part of the legislator.

III.4. Drone regulation

In November 2014, the Authority issued a recommendation concerning data processing by drones[13]. The recommendation includes proposals for the legislator with regard to the need to deal with certain rules in the context of data processing through drones at the level of a law. In the meantime, substantial changes took place with respect to the legal environment.

In addition to the General Data Protection Regulation, it is necessary to mention Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency and amending Regulations (EC) 2111/2005, (EC) 1008/2008, (EU) 996/2010, (EU) 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council and repealing Regulations (EC) 552/2004 and (EC) 216/2008 of the European Parliament and of the Council and Council and Council Regulation (EEC) 3922/91; and Commission delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third country operators of unmanned aircraft systems, as well as Commission implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft.

The development of a set of rules for the use of drones bearing in mind the criteria of air traffic safety, public order and public security and at the same time ensuring the protection of privacy is still awaiting the Hungarian legislator.

Parliament adopted Act CLXXIX of 2020 on the amendment of certain acts related to the operation of unmanned aircraft on 15 December 2020. As revealed by the justification of the act, a rule at law level had to be enacted with regard to the registration of unmanned aircraft and the operators of unmanned aircraft in order to stipulate roles and responsibilities, the granting of data processing authorisations and the specification of obligations on the owners and operators of unmanned aircraft. The justification also extends to the fact that the EU legislation leaves it up to Member States to designate geographical areas over which drones can be banned or restricted, and allows them to define areas where the use of drones is subject to different conditions.

Domestic regulation – the designation of air space, permits from the authorities, registration – enables those applying the law to keep drone traffic under control, check it and take action upon the onset of an infringement. The Criminal Code

13 https://www.naih.hu/files/ajanlas_dronok_vegleges_www1.pdf

establishes the possibility for the state to take action – as an *ultima ratio* – in the event of unlawful and flagrant interference with privacy by drones, the regulation in. Enforcement of the rules is the responsibility of the authorities and and monitoring of the emergint practice will help to determine to what extent these legal regulations serve the needs and expectations of society, and whether any correction is necessary in the area of creating a legal environment.

IV. Freedom of information

IV.1. Introduction

2020 was a hectic year from the viewpoint of the freedom of information, the primary reason of which was the emergency or health crisis due to the COVID pandemic.

The power drafting the bill or rather the constitutional amendment chose not to invite NAIH's opinion in the course of the constitutional amendment related to the notion of public funds in December. Bill T/13647 was the ninth amendment to Hungary's Fundamental Law, whereby Article 39 of the Fundamental Law was supplemented with the following paragraph (3): *"Public funds mean the state's revenues, expenditures and receivables*."

According to the justification of the amendment: *"The Bill defines the notion of public funds, so as to allow the evolution of a uniform practice instead of the current different practice of the constitutional bodies. The Bill clearly and unambiguously defines the notion of public funds covering the entire operation of the state, which is a guarantee to the transparent use of public funds. With this definition, the notion extends to all the constitutional, state and municipal bodies, state and municipal institutions."*

According to the Authority's position, the new definition of "public funds" will not be suitable for terminating or mitigating the deficiencies and inconsistencies in the interpretation of the law to be remedied, but it may lead to additional confusion in the interpretation of the law. In our view, it would be more appropriate to include some kind of differentiation also in legislation in the case of participation in public funds and state assets. By including the notion of data accessible on public interest grounds, in addition to data in the public interest, in the Fundamental Law, it would be possible to settle at the level of the law exactly which data sets, data types must be made public, to substantially improve the competitiveness of the state and business organisations subject to market conditions, while at the same time, creating a clear and unambiguous situation for those applying the law in the field of rights and obligations.

NAIH continues to maintain, and intends to apply also in the future, its statements related to the accessibility of the use of public funds.

The Authority received more complaints and other submissions related to data in the public interest than in the preceding year: the investigation and administration of over 900 cases was in progress at the Department for Freedom of Information, which shows a substantial increase in case numbers by about a quarter.

In addition to the submissions directly affecting the fundamental right to access data in the public interest and data accessible on the grounds of public interest, this department is responsible for the investigative procedures and the Authority's data protection procedures conducted on the basis of complaints related to other fundamental rights affecting public access. In relation to the effectiveness of investigative procedures, it should be noted that, unfortunately, it does happen albeit rarely, that the controller sought – whether it is a small municipality or a ministry – fails to respond to our call. In such cases, the Authority may issue public reports naming the controller (see for instance: https://www.naih.hu/files/Infoszab_jelentes_NAIH_2020_4801.pdf) and there are examples of the Authority launching a data protection procedure imposing a fine.

The entry into force of Council of Europe Convention on access to official documents (CETS No. 205., promulgated in Hungary by Act CXXXI of 2009) on 1 December 2020 was an event of major international significance; this could take place following the tenth ratification (Ukraine). The document was signed by 8 countries, including Hungary, in Tromsø, Norway in 2009 and we were the second country after Norway to ratify it in 2010. This Convention is the first international legal document imposing obligations in the field of the freedom of information, it is open to countries that are not members of the Council of Europe as well as to international organisations, and it has an expressly practical approach (for instance, the term "public authority" includes everybody, natural or legal person discharging public duties, the objective of the person requesting data is irrelevant, the accurate description of the requested document is not expected, personal inspection is free of charge, etc.). The independent expert group consisting of 10-15 members responsible for monitoring the implementation of the Convention will begin its work early in 2021.

IV.2. Important decisions of the Constitutional Court

Constitutional Court Decision 7/2020. (V. 13.) AB: the Fővárosi Ítélőtábla (Budapest Court of Appeal) initiated the annulment of Section 27(3b) of the Privacy Act in the case of the judicial initiative against this provision. In the initial case, the issue of the construction documents of a motorway construction

financed by public funds (with EU support, procured through a public procurement procedure) was requested. The court of the first instance rejected the case on the grounds that pursuant to Section 27(3b), the trade court is responsible to legal oversight over the defendant as a business organisation, hence the court has to terminate the lawsuit. According to NAIH's position[14]. the specific provision of the law provides an opportunity only for the person exercising his rights to turn to the body in charge of legal oversight which however may not impair his constitutional right to turn to the Authority or directly to the court requesting legal remedy in the event of noncompliance or inappropriate compliance with the obligation to provide information in relation to data in the public interest with a view to investigating the infringement. The Constitutional Court rejected the motion as the opportunity to initiate the procedure by the body responsible for legal oversight in itself cannot be regarded as a requirement restricting a fundamental right; at the same time, it established that Parliament created an anti-constitutional situation by way of an omission infringing the Fundamental Law because it failed to provide efficient legal defence for the person requesting the data in the event of non-compliance with the obligation to provide information as set forth in Privacy Act Section 27(3)(a). As Section 31(3) and (5) of the Privacy Act expressly mentions "body discharging public duties" as the defendant in a litigation that may be launched in the event of noncompliance with a data request, starting litigation concerning a request for data in the public interest as set forth in Sections 28-31 of the Privacy Act is not admissible against persons and entities subject to the obligation to provide information according to Section 27(3a). Privacy Act Section 27(3b) allows only to turn to the body exercising legal oversight, which is however not authorised to order compliance with the request for data. Defending the right to access and disseminate data in the public interest requires that the request for data could be enforced in front of a court with respect to all those subject to the obligation to provide information.

Decisions 3209/2020. (VI. 19.), 3210/2020. (VI. 19.) and 3211/2020. (VI. 19.) AB concerning constitutional complaints related to lawsuits launched because of the infringement of goodwill through reports and articles published in relation to the so-called "Questor case": the disputed articles published the names of the data subjects, the names of their earlier workplaces, the fact of their civil partnerships, the names of their life companions, their family relations and through that, data related to the family of the petitioners taken in the wider sense without the consent of the data subjects and the petitioners launched litigation against various news portals and newspapers on the grounds of infringement of privacy and the right to the protection of personal data. The courts taking action had to resolve the conflict

14 NAIH/2019/2996

of law concerning the freedom of expression, freedom of the press, the right to provide information about the case presented and the right to the protection of personal data. The Questor case was of outstanding public interest, given the large number of the people sustaining losses, its nationwide scope and the extent of the damage. The Constitutional Court declared that the credibility of a news item is not in itself reinforced by providing the name of a given person, but the public disclosure of the family relations and earlier workplaces of the petitioners was in the given case in the public interest. Their working relationship between the petitioners and the person accused in the case and their linkage to the attorney-general are personal data related to a communication concerned as a case of public interest, whose public disclosure cannot be regarded either as arbitrary or unwarranted with a view to discussing the public affair concerned, it enjoys a higher level protection for the freedom of expression.

Decision 3413/2020. (XI.26) of the Constitutional Court: the Constitutional Court terminated its procedure related to the establishment of the anti-constitutionality and annulment of Section 2 of Government Decree 179/2020. (V. 4.) on deviation from certain data protection and data request provisions – which established the period open for compliance with data requests in 45 days instead of 15 days – in view of the fact that the provision was no longer in force.

IV.3. Important court decisions

Pfv.IV.21.519/2018/15.: In a review procedure, the Supreme Court agreed with the earlier court statement, according to which the protected trade secret, knowledge of which would give unwarranted advantage to other competitors, cannot be accessed in the case of contracts concluded by the universal postal service provider; at the same time, in this case the contracting parties had to be aware that the contracts concluded with the defendant are more open to access because of the provisions concerning state assets. The reference to the trade secret does not automatically provide exemption from applying the rules concerning public access. The fact of disposing of state assets implies, without any further conditions, that the entity in public ownership qualifies as an "entity discharging other public duties" irrespective of whether it actually discharges public duties, or whether it carries out its activities in competitive circumstances.

Pfv.IV.21.732/2018/8.: Responding to a request for data in the public interest, the Prime Minister's Cabinet Office only sent the instruction concerning the use of the entertainment and protocol expenses of the prime minister's chief counsellor

concerned in the request for data, as well as the information as to what extent the chief counsellor used the appropriation available to him by the date of the request for data, requiring that the costs thereof be reimbursed. The court of the first instance ordered the defendant to disclose the detailed performance verifications of the entertainment expenses in a monthly breakdown, without requesting cost reimbursement. The court of the second instance ordered the Cabinet Office to issue also the copies of the invoices on the basis of which the payments were made. The Supreme Court found the defendant's petition for review unfounded and disagreed with the claim that the request to access the data would have been aimed at a comprehensive, invoice level audit of their financial management, as it only applied to a small fraction of the costs needed for the performance of the Prime Minister's Cabinet Office activities.

Pfv.IV.21.778/2018/8.: According to the relevant legal provisions, the service relationship of regular members of the law enforcement agencies has to be terminated by dismissal on the grounds of unfitness for service for breach of the requirement of impeccable conduct. This may be waived by the Minister of the Interior if the execution of the sentence of imprisonment imposed has been suspended by the court and the conduct on which the sentence is based is not likely to have an adverse effect on the performance of further service. Convictions on which such a ministerial decision is based are parts of the personnel records. According to the Supreme Court's position, the data of the specific data subjects are fundamentally personal data whose accessibility is not provided for by any legal provision; moreover, identification may be possible indirectly based on the data and the circumstances considered in the court sentences, thus anonymisation in itself is insufficient for making the personal data unidentifiable.

Pfv.IV.20.148/2019/8.: The petitioner, a Member of Parliament, requested the defendant, a business organisation exclusively held by the Hungarian state and founded for the organisation of the "2017 World Aquatics Championships" to issue all the contracts of assignment concluded with other firms and undertakings, but the defendant failed to respond to the request for data. The Supreme Court maintained the effect of the final judgment and confirmed the unbroken judicial practice that data concerning the use of public funds qualify as data in the public interest in accordance with the Fundamental Law, irrespective of the organisational structure or name of the body processing them. In relation to the objection concerning powers, the Supreme Court declared that if the scope or activities of a business organisation or institution are of national significance, the regional court according to its registered address has competence to conduct the procedure.

P.21.053/2019/30.: A parliamentary committee decided to exempt certain defence and law enforcement procurements from public procurement, but the ministry concerned rejected the request for data stating that it was not the controller of the data requested. According to the court's interpretation, the petitioner's request was targeting the investments of the given ministry and the development projects of the ministry can, and should, mean not only the transactions concluded by the defendant in person, which is revealed also from the evaluation of the contents of the questions. Moreover, the capacity as controller can be established even if the given ministry is not a contracting partner in the investment projects concerned.

Pfv.IV.20.305/2019/8.: A state-owned single member company limited by shares engaged in energy production and management, financed exclusively from public funds, voluntarily supports projects invented and developed by various individuals or companies as project initiators. The controller refused to disclose the data requested in relation to such projects on the grounds of trade secrets and insisted on the appointment of a forensic energy and technical expert, underlining that the field involved in this litigation was special, namely research and development, hence the evaluation whether the idea set forth in the contract, the name and brief description of the project could provide information from which competitors could make material inferences concerning its details was a matter for experts. According to the court's position, the defendant voluntarily undertook a public task by supporting start-up projects and the activities related to this cannot be withdrawn from the scope of the Privacy Act. The data referred to cannot be regarded as trade secrets, because the magnitude of the invested amount and the data concerning the persons of the investors are accessible from public sources, the data concerning the magnitude of the amount invested in the project are data accessible on public interest grounds, while the project description includes general statements whose disclosure does not give rise to disproportionate violation of interests from the viewpoint of conducting business activities.

2.Pf.20.049/2020/8.: In its judgment the court instructed the logistics and asset management company of a ministry to disclose information about what issues, business matters, cooperation issues were discussed by the chairman of the board during his official foreign trips and what was the position or the job of his negotiating partners. In the course of the litigation, the defendant failed to provide specific evidence in support of which decision of exactly which body the data were used and to what extent and how access to the data influenced the implementation of the decision and which parts of the documents requested to be released were subject to reasons for restricting access.

8.Pf.21.166/2019/5.: The petitioner requested disclosure of the 2017 annual report of the Group of States against Corruption (GRECO) operating within the Council of Europe, which however was to be handled confidentially according to Article 15 of GRECO's statutes. The court established that the data requested were in the public interest, but at the same time classified, hence not accessible to the public. In the meantime, the Government published the report.

2.Pf.20.048/2020/4.: The data request targeted documents related to the voting behaviour to be followed by the Hungarian Government at a specific negotiation and the related opinions received from societal reconciliation, the protocols of reconciliations with NGOs and professional organisations and feasibility studies. Not even the defendant disputed that the requested data were data in the public interest; at the same time, the court accepted that their nature allows the conclusion that their issue would render impossible to do official work free of influence and it would impede civil servants in discharging their tasks.

Finally, two court decisions whose final conclusions were contrary to the content of the NAIH statements made earlier in these cases:

2.Pf.20.105/2020/7.: Through its judgment, the court required the defendant to issue specific instructions of the national command of penitentiary institutions to the petitioner. The parties to the litigious did not dispute that the data requested via the petition were data in the public interest and none of the special instructions were classified. According to the court, the special instructions were not drafted in the course of bringing a specific decision by the defendant as they contained general provisions for the discharge of the defendant's tasks, hence they do not qualify as data on which a decision is based, and the defendant failed to demonstrate the "security risk" concomitant with their disclosure (whereas *NAIH accepted the reference to the security risk in its earlier investigative procedure*).

In its judgment 25.P.20.421/2020/12., the Budapest Regional Court (approved by Judgment 8.Pf.20.556/2020/5 of the Budapest Court of appeal) ordered MTVA to disclose the employment contract of its lead newsreader employee, together with its annexes and amendments, disclosing the data related to responsibilities, basic wage, supplementary wages and additional benefits. The fact that MTVA discharges public tasks and its activities are financed from public funds allows the inference that its employee is acting in the context of his public duties when reading the news. The court of the second instance shared the position of the court of the first instance that in order to appropriately enforce the right to a free discussion of public affairs and the right to free expression, it is indispensable that citizens can learn about the employment conditions of employees discharging

public tasks. Based on all this, specific data of the employment contract of the news anchor, primarily his remuneration, are data accessible on public interest grounds. *(NAIH based its different position on the fact that the news anchor could not be categorised as a senior managerial employee of the Fund or their deputies, or chairman and members of the Fund's Supervisory Board or the employees working in managerial positions and their deputies heading organisational units directly responsible for the discharge of the Fund's public tasks, hence the data of his employment contract cannot be categorised as data accessible on public interest grounds based on Privacy Act Section 26(2)).*

IV.4. Access to the data related to the coronavirus pandemic

"The impact of the corona virus pandemic brings unprecedented challenges for society both nationally and globally. Public authorities must make significant decisions that affect public health, civil liberties and people's prosperity. The public's right to access information about such decisions is vital."[15]

NAIH participated in the drafting of the above statement by the International Conference of Information Commissioners and it fully agrees with its findings, according to which openness, transparency and sharing information proactively are indispensable for people to understand the state's decision-making processes. However, we must also bear in mind that public organisations must focus their resources on protecting public health during a pandemic.

In order to reduce the burden on disease control bodies, data requests could be completed in 45 days instead of 15 days[16], but only if it was probable that performance within the ordinary due date would have jeopardised the discharge of the agency's tasks related to the emergency situation. One disaster management directorate reported substantial additional tasks – naturally that was an acceptable reason. (NAIH/2020/4603)

15 Statement of the International Conference of Information Commissioners (icic) (14 April 2020) https://www.informationcommissioners.org/covid-19

16 Section 2(3) of Government Decree 179/2020. (V. 4.) on deviation from certain data protection and data request provisions during the emergency. It has ceased to be in force since the day of the termination of the emergency, i.e. from 18 June 2020. Government Decree 521/2020. (XI. 25.) on deviation from certain data request provisions during the emergency will lose effect on 8 February 2021.

NAIH received several complaints objecting to the fact that controllers referred to the 45-day period without any justification. The Authority underlined in every case that any deviation from the due date according to the Privacy Act must be justified individually. An acceptable reason was if during the emergency municipal decision-making had to be carried out with short due dates putting extra burden on the employees of the municipality and as most of them were working in home office mode only few employees had physical access to the documents. (NAIH/2020/4147)

A substantial part of the notifications and questions related to the pandemic were about the data concerning the disclosure of the fact of the infections and access to data on the geographical distribution of the infected persons. NAIH declared in every case that the health statistics of geographically based groups of certain sick persons qualify as public statistical data, whose accessibility may be restricted because of their role in decision-making only if their accessibility would jeopardise the effectiveness of the agency's procedure. This should the decided by the controller, but its decision must be supported by detailed justification. Once the decision is made, the data request may be rejected, if the data would serve as the foundation of additional future decisions, or access to the data would have a negative impact on the lawful or smooth operation of the agency discharging public tasks. At the level of settlements, the number of infected people and the number of the deceased are statistical data that may be disclosed, provided the patients cannot be identified. Other processing without purpose or unlawful processing, such as posting a list of "infected" street names or indicating the exact place of an official quarantine by giving the street and house number on Facebook should be avoided as bad practice. (NAIH/2020/3506, NAIH/2020/2838, NAIH/2020/2904)

The municipal executive of Budapest 13th District applied to the Public Health Department of the 5th District Office of the Government Office of Budapest (hereinafter: Government Office) for the number of confirmed COVID-infected persons and the number of persons subject to an official quarantine in the 13th District in a daily breakdown. (According to the legal regulation, the 13th District belonged to the competence of the Public Health Department of the 5th District.[17])

17 Based on Section 3(1) and Section 5 of Government Decree 385/2016. (XII. 2.) on the discharge of the public health duties of the Budapest and county government offices and the district (Budapest district) offices and the designation of health care administrative agencies, the district office performs all the public health, authority, professional supervisory tasks of the public health administrative body in its field of competence, which are not referred to the competence of the national medical officer or the government office by legal regulation. Annex 2 to the Government Decree specifies the fields of competence of the district offices.

The Government Office rejected the data request with reference to the fact that Government Decree 41/2020. (III.11.) made it possible to transmit the requested data to the municipalities; with the end of the emergency, however, the legal basis of data transmission no longer existed.

The Government Office processes, inter alia, the onset and place of the infection, the place of nursing, the reported disease and its epidemiological description, the laboratory diagnosis and the qualification of the outcome with respect to COVID-infected persons in the Epidemiological Subsystem of the National Specialised Information System (hereinafter: OSZIR) run by the National Public Health Centre.

According to Section 2.1 of the *Amended procedures issued in relation to the new coronavirus identified in 2020* published by the National Public Health Centre (hereinafter: Procedures) the health care provider has to upload the data of the person suspected of being infected by COVID-19 or having positive laboratory results to the Communicable disease reporting subsystem of OSZIR within 24 hours. The public health staff of the district office creates a disease case from the Communicable disease reporting sheet received electronically within 24 hours and complete the individual data collection sheet with the available data. Section 2.2 of the Procedures contains the procedures to be followed to separate suspicious and confirmed cases. According to Section 2.2.(a) "*Separation of a suspected patient at home having mild symptoms shall be done upon the instruction of the health care provider (primary care, outpatient care). In warranted cases, the authority may act through an order in the case of the positive result of a PCR laboratory test designed to detect SARS-CoV-2."*

This means that the Government Office does have the requested data and it is able to obtain aggregated statistical data from the data stored in OSZIR, which are public data pursuant to Section 4(8) of Act XI of 1991 on the Activities of the Health Authority and Administration (providing for public access to data on the epidemiological situation). (NAIH/2020/7731)

The question was raised in several cases whether the fact that an identifiable person is infected can be published. As health data constitute one of the special categories of personal data according to GDPR Article 9, as a main rule, their public access is prohibited, thus a municipality lawfully refused to issue, for instance, the name of an infected municipal representative. (NAIH/2020/2926, NAIH/2020/6568). At the same time, the information whether the government office granted a licence to a family doctor to start working after participating in a conference abroad is a personal data accessible on grounds of public interest. The

reason is that there is a legal regulation[18] that stipulates that health care workers in direct contact with patients, in addition to their professional qualification for the job, are considered fit to perform their duties if they do not suffer from a disabling infectious disease. The information whether a person discharging a public task meets the legal conditions of discharging that public task is public data accessible on grounds of public interest as other personal data related to the discharge of the public task. (NAIH/2020/2963)

Several submissions asked about the accessibility of data concerning the epidemiological control of residential social care institutions. Data in the public interest include, for instance, how many people were shown to have coronavirus infection in the institution, the number of available protective devices, whether there is a designated epidemiological officer and whether he or she held an infection control training, or whether patients were returned from the hospital without testing them for coronavirus. These data are processed by the institutions, they are part and parcel of their activities and related to their operation and do not qualify as personal data. Pursuant to Section 32 of the Privacy Act, an agency discharging public tasks has to facilitate and ensure the accurate and rapid provision of information to the public concerning the cases within its responsibilities (NAIH/2020/3752). The findings of the inspection report concerning the professional supervision carried out in residential social care institutions are also data in the public interest; by anonymising the personal data they can be published in internet websites. The finding of the report that the managers of the institutions severely jeopardised the health of the people they cared for during the period of the emergency and epidemiological alert is closely related to the performance of their public duties and the public has a substantial interest in accessing it, thus it qualifies as personal data accessible on grounds of public interest. (NAIH/2020/6631)

Data of financial management related to the epidemic show a varied picture: for instance, those requesting data wished to have access to the municipalities' contracts related to the epidemic, the amounts spent on rapid tests, the quantities ordered, which are naturally data in the public interest. (NAIH/2020/6190, NAIH/2020/6299). A journalist asked for the contracts concerning the procurement of the ventilators from the Ministry of Foreign Affairs and Trade, but the Ministry did not send him the annexes containing the technical specifications. Once NAIH requested information concerning the restriction of access to the annexes, the Ministry made them available to the journalist, thus the public could be informed within a very short time. (NAIH/2020/7123)

18 Section 4 of Decree 40/2004. (IV. 26.) ESzCsM on the examination and certification of medical fitness to perform health care

Another journalist submitted a data request to the Hungarian National Blood Transfusion Service (hereinafter: OVSz). The subject matter of the data request was the contract on the sale of blood plasma and its amendment. The company with which OVSz concluded the contract regarded the entire contract as its trade secret, and because of this only the three data in the publication list of OVSz, the subject matter, value and period of the contract was to be issued. In the course of its investigation, NAIH underlined that in the event of a conflict between data in the public interest and trade secrets, access to the data in the public interest enjoy priority and Section 27(3) of the Privacy Act is to be interpreted strictly. The public had a substantial interest in the transparency of the management of the national blood supplies, particularly in the current epidemiological situation. NAIH requested the company to provide detailed justification for the classification of each point of the contract as trade secret and also to what extent access to the given point of the contract would cause disproportionate harm in business life. After this, the contracting company continued to state that 10 out of the 45 points of the contract were trade secrets. Of these, the Authority accepted the argumentation in the case of two points, so OVSz sent the rest to the journalist. Among other things, the Authority regarded access to the obligations undertaken by the parties in the contract as unconditionally justified because without knowledge of these, a well-founded societal debate on the appropriateness of the sales price could not evolve. When concluding a contract, whose subject matter was part of the national assets, the company had to expect that at least the main obligations would be accessible to the public. According to the Authority's position, it should also be transparent what legal consequences are stipulated by the contract if the contracting party fails in its obligation to facilitate the supply of domestic blood plasma to patients. (NAIH/2020/1800)

IV.5. About requests for data in the public interest targeting NAIH

In 2020, the Authority received altogether 72 requests containing 187 data requests from 43 petitioners (petitioners frequently asked for several data, at times complex information or sets of data in a single submission, so a petitioner turned to the Authority with 4 data requests on average). Of these, 144 requests were complied with, 6 were partly complied with and 37 requests were rejected.

The most frequent reasons for rejection:

- the requested data were not data in the public interest,

- the requested data was not available to the Authority,

- the requested data was used for decision-support,

- the requested data were criminal personal data generated in the course of a criminal procedure.

The most frequent subject matters of the data requests included: statistical data related to the administration of cases by the Authority (for instance, the Authority's data protection procedures, incident reports, complaints and data requests in the public interest, fines, secret supervision, etc.), NAIH information briefs, position statements and documents generated in the course of specific cases, NAIH's internal rules and NAIH's opinion on certain legal regulations.

IV.6. Cost reimbursement

It can be stated that legal practice concerning the applicability of cost reimbursement and the methodology of its calculation has been developing year after year ever since the entry into force of Government Decree 301/2016. (IX. 30.) on the extent of cost reimbursement for compliance with requests for data in the public interest (hereinafter: Cost Decree). In practice, this means that the process of calculation is becoming increasingly clear. Of the three different categories, labour expenses continue to be the cost element in relation to which difficulties in interpretation arise the most frequently. In every case, the Authority emphasizes that when complying with requests for data in the public interest, agencies discharging public tasks or those financed out of public funds do not provide a service but meet their obligations arising from a fundamental right set forth in the Fundamental Law. By default, as part of their ordinary daily operation, they have to make the requested data available to citizens free of charge. Labour costs may be charged as cost reimbursement, if providing the data requires disproportionate use of the labour required for the performance of the basic activities of the agency discharging public tasks, the period of the necessary labour use exceeds four working hours and all the conditions referred to are met. Agencies discharging public tasks must be ready to receive requests for data in the public interest or data accessible on public interest grounds with respect to any of their activities.

In 2020, the Authority received 23 complaints from citizens (2019: 32 requests, 2018: 39 requests) disputing the legal basis or amount of the cost reimbursement – this result is definitely positive relative to the preceding years. Controllers

demanding cost reimbursement included, for instance, the Municipality of Paks, the Veszprém County Government Office, the Municipality of the City of Bicske, various foundations and health care institutions.

Another positive experience was the decrease in the amount of the cost elements. While in earlier years, cost reimbursement demands frequently amounted to several million forints, in the case of those requesting legal remedy from the Authority in 2020, the highest cost reimbursement demand was related to the TASZ case to be presented at the end of this chapter (HUF 640,340), and frequently as a result of a NAIH investigation, the bodies discharging public tasks or those financed from public funds made the data requested available to the petitioner without demanding cost reimbursement.

In a specific case, the petitioner requested contracts and other data in large quantities from an association coordinating catch-up programmes. The association set a cost reimbursement demand of HUF 69,000 because the organisation did not have any employees. As a result of the Authority's intervention, the association finally was able to ensure access to the data by way of inspection free of charge. (NAIH/2020/56)

In another case, the petitioner turned to the Authority on behalf of an on-line news portal. They requested communications, marketing and media related contracts for the first 9 months of 5 years from a mayor's office, which demanded HUF 103.820 for 42 hours of labour and altogether 383 pages of electronic copies of the requested documents as cost reimbursement. In the course of the investigation, the Authority called upon the controller to reduce its demand on several occasions, so finally the original claim was reduced to HUF 10,759. In view of the number of documents, the Authority regarded the cost reduction as substantial and thus acceptable. (NAIH/2020/420)

Providing adequate information is very important; it should not be limited merely to disclosing the amount of cost reimbursement charged on the cost elements. Agencies discharging public tasks must indicate all the reasons and all the cost elements, which substantiate the grounds for the amount claimed, because the controller has the obligation to demonstrate that the amount of the cost reimbursement was well-grounded in an eventual court procedure. Adequate information greatly contributes to the petitioner truly understanding why he has to pay the cost reimbursement and in what amount in order to have access to the requested data. Furthermore, based on the information, he will be able to adopt the right decision in relation to an eventual legal remedy. In the given case involving inadequate information, finally the controller municipality issued the requested data free of charge after the call of the Authority. (NAIH/2020/4173)

As part of his studies as student reading finances and accounting had to draw up a case study on an EU project, and he selected a foundation, which he approached several times electronically with a request for data in the public interest without success. Finally, the chairman of the foundation informed him that he will issue the requested data if the student would pay a cost reimbursement of HUF 72,000 calculated by him (3 full days/24 hours, HUF 3,000/Man hour). The investigation of the case revealed that the details of the cost reimbursement were inadequate, moreover, according to the foundation's statements, compliance with the request did not impede the discharge of its basic duties. Having been called upon by the Authority, the foundation issues the requested data free of charge. (NAIH/2020/4267)

IV.7. Media and the public nature of the Internet

IV.7.1. The right "to be forgotten"

More and more people turn to NAIH in cases related to the media, the public nature of the Internet and, in this context, the enforcement of the right to erasure ("to be forgotten"), so this type of cases plays a much greater and much more emphatic role than in preceding years. It is warranted to provide help and guidance to broader strata of society with regard to the Internet, which increasingly determines our everyday life, using the instruments of publicity. Similarly to other rights of the data subjects, the right to erasure set forth in Article 17 of the General Data Protection Regulation is not absolute, hence it can be subject to restrictions, if appropriate guarantees are in place. Compliance with an unfounded or excessive request can be rejected, and EU or national law may also include restrictions; also, the General Data Protection Regulation specifies certain case types when the obligation to erase is not enforced: continued processing may be regarded as lawful, if it is necessary for the exercise of the fundamental rights and freedoms of others (...). One of these is the freedom of expression and the right to be informed. The right to free expression is one of the outstanding fundamental values of a democratic constitutional state, which guarantees that the individual is able to formulate and express his ideas and opinion, thus it contributes to the free flow of various views and ideas. The freedom of expression includes the right to be informed, i.e. the freedom to receive and disseminate information and, on that basis, the user has the right to obtain, forward or publish data in the public interest or data accessible on the grounds of public interest using modern technologies, within the framework of the constitution.

In a specific case, a former actor in a reality show initiated the launching of the Authority's data protection procedure, because a major Internet news portal did not remove an article published in 2014 containing his personal data in spite of his request (the article reports that the complainant got the worst score at a scheduled sympathy vote held among the actors). The article contained only the nickname of the complainant (VVX YZ) which however cannot be linked directly to the current professional career of the complainant. The full name of the complainant is not found among the search results of the Internet news portal concerned, whereas the Google search engine indicates hundreds of thousands of hits for the various modes of the nickname. According to the position of the Authority, taking all the essential circumstances of the case into account, the news portal rightfully referred to the freedom of information and the right to be informed when rejecting the erasure request. Moreover, NAIH attached importance to stating that the data subject himself disclosed in the course of the programme that he was going into law (he was a law student at the time when he was admitted to the show), and undertook to act in the reality show and all the concomitant risks in the knowledge that the Budapest Bar initiated a disciplinary procedure against the attorney-at-law acting in the previous season of the show to establish whether his acting in the show was worthy of and reconcilable with practising the vocation of an attorney-at-law. NAIH was also aware of the fact that the photo published in the news portal concerned was an official press photo, which the television company published and provided to all press organs expressly with the purpose of being used as an appropriate photographic illustration in all reports concerning the show. Summarising all this, in its decision closing the procedure, NAIH decided that reporting on a person who has volunteered to appear as a public figure in a programme with a particularly high audience rating broadcast for months on a national terrestrial television channel in Hungary and on a specific event related to the show complies with the exception rule based on Article 17(3)(a) of the General Data Protection Regulation (exemption from the right to be forgotten). (NAIH 2020/842)

An opposite example: NAIH helped in the full enforcement of the right to be forgotten in the case of a complainant who as an employee of a church had been involved in a notorious scandal over 10 years ago, since then he left his church vocation and requested a major Internet news portal several times to erase the article on him, but he did not receive an answer of merit to his request. As the article contained special category data of the data subject (those related to his sexual life and orientation), the Internet article can be lawful only if over and above the existence of the legal basis according to GDPR Article 6, the condition in Article 9(2) is also met. According to NAIH's position, the fundamental right of third

persons to be informed is not infringed, if an old information about a person who is no longer in his former public office, is no longer accessible; moreover, the article objected to has no news value owing to which the erasure or anonymisation of the article would have a substantially negative impact on the daily operation of the news portal. At the same time, it is unambiguous that the "scandal chronicle" has an extraordinarily negative impact on the current private life of the data subject. As the data processing practice of the news portal infringed the complainant's right to the protection of his personal data, NAIH called upon the controller to erase all the personal data on the basis of which the complainant could be directly or indirectly identified. If this can only be achieved by removing the entire article, the controller should erase the content accessible in the page objected to and process requests from data subjects appropriately in the future. Upon NAIH's call, the news portal fully complied with the data subject's earlier request. (NAIH 3865/2020)

Similar arguments and counterarguments clashed in the case which was also closed successfully. The content objected to was a report of four years ago about the Christmas preparations in a penitentiary institution and how the inmates experienced the festivities and in what kind of atonement programmes they participated during this period. After his release from prison, one of the actors realised how detrimental the publicity concomitant with his being in the report was for him. The content provider concerned expounded to NAIH that in their view, the complainant's erasure request was unfounded because he voluntarily made a statement in the report, hence the legal basis of processing was the data subject's consent and the processing of the data was necessary for the exercise of right of the freedom of expression and information. They also referred to Article 6(1)(c) of the General Data Protection Regulation, according to which the processing was necessary to meet the legal obligations of the controller. In terms of the appropriate legal basis, NAIH primarily examined whether the right of the community to be informed could in this case lawfully restrict the right of the data subject to protect his personal data. As the earlier status as inmate is a sensitive information enjoying particular protection, the lawfulness of disclosure would need to be considered even if the data subject were currently serving his sentence of imprisonment. In view of the passing of time and the fact that his term in prison ended, the primacy of the right to the protection of privacy can be clearly established. Ultimately, the Broadcaster fully met NAIH's call. (NAIH 5421/2020)

In 2020, the Authority launched its data protection investigation ex officio in two parallel cases in relation to the processing practice of the *markmyprofessor.com* website. Many complaints were lodged against the site earlier (see NAIH Report of 2018, p. 126), but the earlier position of the Authority was consistent: university

professors undertaking scientific public acting have an obligation to tolerate the negative evaluations and criticisms related to their professional activities from students; but this should not, of course, result in disrespecting human dignity for which the operator of the website is also responsible. In these cases, however, the infringement of the data subjects' rights could be established – by failing to respond in substance on time to the requests of the data subjects sent to it, the controller infringed their right to access and, closely related to this, the right to be informed. It should also be underlined that the provision of information as requested on time is of decisive significance from the viewpoint of the transparency of the operation and order of data processing by the controller as well as the enforcement of the requirement of a fair procedure. In accordance with the above principles, pursuant to Article 12(3) of the General Data Protection Regulation, the controller has to inform the data subject of the measures taken as a result of the request according to Articles 15 to 22 without undue delay but definitely within a month from the receipt of the request. In case of need, with a view to the complexity of the request and the number of requests, this period may be extended by an additional two months. Pursuant to Article 12(4) of the General Data Protection Regulation, if the controller fails to take measures as requested by the data subject, it has to inform the data subject of the reasons for not taking the measure and about the fact that the data subject may lodge a complaint with a supervisory authority or exercise his right to judicial remedy without delay, but at the latest within a month from the receipt of the request.

In one of its procedures, NAIH also examined that the controller failed to update its Privacy Statement published in its website since the entry into force of the General Data Protection Regulation (25 May 2018), and its contents were not updated. The purpose of the Privacy Statement is that the controller should provide full information to the data subjects of the possibilities of enforcing their rights to informational self-determination set forth in the General Data Protection Regulation and the Privacy Act in accordance with the expectations set in relation to the data processing operations it carries out. Following NAIH's action, the controller amended its Privacy Statement as appropriate and published it in the website operated by it on 1 September 2020.

In view of the controller's cooperation and the practical problems due to the pandemic, NAIH only reprimanded the controllers in both cases. (NAIH 4762/2020 and NAIH 5911/2020)

The Authority launched a data protection procedure upon request, in which the data subject complained that a writing was published in an investigative news portal, which it is still accessible there, whose video annex was a video captured

by a drone inter alia of the property held by the data subject, its location and internal areas, expressly pointing to the owner of the property. Basically, the drone video shows parts of the property that cannot be seen from a public area, its internal court and garden area, its design, the internal parts of the garden, the garden furniture installed and other parts of the building surrounded by high trees and not visible from public areas in high resolution. According to the Complainant's position, the parts of the property not visible from a public area carry information that can be clearly associated with the owner, thus qualify as personal data according to the General Data Protection Regulation, whose processing, particularly their publication, is unlawful. In its statement NAIH declared that the property shown in the drone video is not the residence of the data subject, it only shows the built environment, the plot of land, its location and the building on it, and the video does not show any natural person, no natural person could be identified in it, and irrespective of the fact that the video was not made from a public area, no conclusion can be drawn from the property (detrimentally) influencing the data subject or any other person, their reputation, rights and legitimate interests. Nobody objected to the other statements in the article containing the drone video complained about, such as the business and governmental relations of the business undertakings held by the data subject, the volume of their activities, the magnitude of their profits, nor was there any objection to the fact that the same article published the name of the data subject in relation to the purchase of the property shown in the drone video, the fact of the purchase, the property, the reference to the property as the registered address of the business organisations held by him, the size of the plot or its location. Based on the practice of the constitutional court concerning public affairs and public actors and the freedom of expression, NAIH accepted that the report on the data subject's investment into the property and on its development/refurbishment verifies the data processing by the controller news portal based on Article 17(3) (a) of the General Data Protection Regulation.

The decision notes that a number of data protection issues related to the use of drones await clear settlement and for this reason a uniform European regulation was enacted recently with a view to the safe use of drones. The rules of Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third country operators of unmanned aircraft systems, and Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft (hereinafter: Implementing Regulation) are mandatory and directly applicable in all the EU Member States, including Hungary. In its Implementing Regulation (EU) 2020/746 of 4 June 2020, the Commission decided to postpone the starting date

of the applicability of certain rules of the Implementing Regulation because of the COVID-19 pandemic. Accordingly, the provisions of the Implementing Regulation have to be applied only from 31 December 2020. (NAIH 4228/2020)

In the so-called “Forbes cases”, the Authority imposed data protection fines totalling HUF 4.5 million on Mediarey Hungary Services Zrt. publishing the Hungarian Forbes magazine (hereinafter: Publisher); it is, however, exceedingly important to underline that the position of the Authority is not that it would be fundamentally unlawful if, in the course of discussing an issue of public life, a journalist sorts businessmen and companies into a list according to well-grounded professional criteria and reports their activities to the public in this form. Such a list may be compiled from accessible sources and business data and the list can be published; there are, however, stringent requirements concerning this which is set forth by the General Data Protection Regulation and the Publisher as controller must meet these requirements.

In its decisions, the Authority established that the Publisher infringed the relevant provisions of GDPR by failing to carry out an adequate interest assessment of its own legitimate interest and those of third parties (the public) and failed to inform the data subjects of this in advance and it also failed to provide adequate information on all the substantial circumstances of processing and of the right of the data subjects to object to the processing of personal data and, furthermore, it failed to provide information on the possibilities of the enforcement of their rights in its answers to the requests of data subjects aimed at exercising their rights in relation to the processing of data in the printed and on-line versions of its publication listing the largest family undertakings and in the printed and on-line versions of its publication containing the 50 richest Hungarians published at different times in 2019. The court review of these decisions is in progress. (NAIH/2020/1154) (NAIH/2020/838)

In another of the Authority’s data protection procedures, the subject matter was an on-line report of a court hearing of a criminal case related to the discharge of public duties by a former mayor (the complainant was a mayor and as such had a public function and qualified as a public actor at the time of the alleged infringement upon the submission of the request and at the time of launching the Authority’s data protection procedure). The Authority did not establish any infringement here, because the removal of this information would violate the freedom of the press and of expression and the right of the public to be informed. (NAIH/2020/1354 and NAIH/2020/1356)

IV.7.2. Social media

NAIH or rather its Department of the Freedom of information received numerous complaints in relation to the data processing practices of the users of the Facebook social site, primarily those of various groups, often closed groups and individuals, as well as their shared content in 2020. In the light of these complaints, NAIH published a general information document[19] accessible in its website.

Only content which do not violate the rights of others, the principles of the social site and other rules and conditions related to the general use of the Internet may be shared. Of these, the most important is that an appropriate legal basis is needed for the processing of personal data (generally the consent or permission of the data subject). In the event of unlawful processing – for instance arbitrary posting of photos presenting another person in a unpleasant, embarrassing situation, libellous commenting, the sharing of prohibited content, etc. – the private individual controller can also be called to account and he may expect severe legal consequences. Pursuant to the General Data Protection Regulation, the rights of the data subject include the right to access (information related to processing), the right to rectification, the right to erasure ("the right to be forgotten"), which may in the given case be restricted by the right of others to freely express their opinion or to be informed, the right to restrict processing, the right to data portability and the right to object. It is very important that the data subject himself should be careful about his personal data, for instance, he should use the data protection settings appropriately and do everything in order to prevent unauthorised persons from accessing his personal information. NAIH clarified the responsibilities and possibilities of the administrator of a social site, as well as the action an injured person can take if the content shared on a social site violates his rights. Following the investigation of the case, NAIH may impose a heavy fine during its data protection procedure in the most severe cases and it may even file a criminal complaint. The data of the European users of Facebook and the so-called Facebook products (Messenger, Instagram, WhatsApp) are processed by Facebook Ireland Ltd., because of its registered office is in Ireland, the General Data Protection Regulation designates the Irish data protection authority as the lead supervisory authority in investigations against Facebook. If necessary, NAIH forwards the complaints received from Hungarian users to them and it may itself join the investigations as the supervisory authority concerned.

At the same time, substantial issues of jurisdiction have arisen not only in Hungary, but also in a number of Western democracies. The evaluation of some

19 https://www.naih.hu/files/Tajekoztato_kozossegi_mediaban_megosztott_tartalmakrol.pdf

of the technology-based data processing operations on the Internet depend to a great extent on the set of constitutional values of the given country; thus decision on these should not be left to the global tech giants operating on a business footing and run by their less than fully transparent self-regulators, rather than putting them under the jurisdiction of the country where the eventual infringement took place or in which its impact is strongest based on the principle of national sovereignty.

Only the bodies protecting rights acting within their constitutional powers of the given country (such as the data protection authority, the courts, the constitutional court) are authorised and called to make well-founded decisions on constitutional fundamental rights and values, in these cases the primacy of national law prevails in the sense of both substantive and procedural law (this is also acknowledged by the law of the European Union). The free opinion expressed on the Internet is a subject matter of the law to be protected in terms of data protection (if we assess opinion as personal data) and the assessment of the constitutional right to express an opinion is generally the result of serious constitutional weighing as shown by the cases expounded above. Soon EU law will have to find a reassuring response to this challenge.

IV.7.3. Is a message sent through Facebook a request for data in the public interest?

A citizen posted questions to a municipality through Facebook, the social media site, which remained unanswered. Pursuant to Section 28(1) of the Privacy Act, anyone may submit a request to access data in the public interest verbally, in writing or electronically; but there is no legal regulation to require municipalities to be present on social medial sites. So, it is also optional whether or not they respond to messages or questions received and read there. According to the Authority's position, the questions posed through social media sites do not generate legal obligations for which anyone could be called to account, thus we recommend those requesting data to contact municipalities, other bodies discharging public tasks directly as set forth in Section 28(1) of the Privacy Act through one of their official contact points. (NAIH/2020/8491)

IV.8. Data of persons in public service accessible on the ground of public interest

The interpretation of Section 26(2) of the Privacy Act continues to cause problems for controllers in the case of requests for the personal data of persons acting within the responsibilities and powers of a body discharging public tasks. The assumption that only those of the personal data of persons discharging public tasks are accessible, which are listed item-by-item in the legal regulations applicable to their legal standing. If these persons take action within the powers and responsibilities of the body discharging public tasks, other personal data related to the discharge of their public tasks are also accessible, but only to the extent indispensable for ensuring the transparency of the discharge of the public tasks. (Naturally, extended access does not apply to the personal data of administrative or cleaning staff.)

NAIH bore in mind this later condition when investigating whether a physician's prescription practice can be qualified as other accessible personal data of the physician related to the discharge of his public tasks. Here we have the entirety of actions taken with a view to discharging his public tasks and are closely related thereto. At the same time, there may be several degrees of access to the prescription practice with the most complete access being the prescription data of a physician for a specific medication. According to NAIH's position, access to the prescription data for specific medications is not indispensable for the transparency of the prescription practice of physicians as pursuant to relevant legal regulations, the expected values established by ATC groups[20] and not by individual medications constitute the basis for the legal consequences of the prescription behaviour of physicians. (NAIH/2020/4900)

As it has arisen in several cases, so it is important to underline that NAIH's position continues to be (in agreement with the unbroken Hungarian practice of applying the law, the earlier decisions of the Constitutional Court and NAIH's statement NAIH/2015/7163/2/V) that the range of data specified in Section 179 of the Act on Civil Servants are data accessible on the grounds of public interest in the case of employees subject to the Act on Government Administration (hereinafter: Government Administration Act) and the bodies of special legal standing and on the legal standing of their employees, even if there are no specific provisions requiring accessibility based on the phrase "personal data relevant to performing public duties" stipulated in Section 26(2) of the Privacy Act. (NAIH/2020/1305)

20 Pursuant to Section 3(13) of Act XCVIII of 2006 on the General Rules of Secure and Economical Supply of Medicines and Medical Aids and of Pharmaceutical Trade: ATC group means the classification of medications according to their anatomical, therapeutic and chemical effects.

Accordingly, NAIH did not accept the reason for rejecting a request concerning data for the salary and bonus payments of the district offices from the Zala County Government Office that the Act on Government Administration does not provide for the accessibility of the personal data of government officials subject to its scope with the exception of the data specified in Section 186. Data on bonus payments, for instance, is related also to the quality and quantity of work performed, as well as criteria characterising the discharge of the public tasks, access to the data requested can and must be adjudged exclusively based on Section 26(2) of the Privacy Act, in view of the fact that other legal provisions requiring access to the data are not currently in force. (NAIH/2020/1496).

The argumentation of the Bács-Kiskun County Government Office was also unacceptable because if the civil service legal relationship of the person discharging public duties is terminated for a reason related to the discharge of his public duty, the reason for and time of termination are “data relevant to performing public duty”. The Government Office accepted this position and complied with the data request. (NAIH/2020/2365)

In relation to whether the documentation of the winning application by the head of a social institution already elected can be issued, NAIH considered the situation unrealistic in which the technical materials of the tender dossier would contain data and information, which result in a positive evaluation by the decision-maker, but cannot be accessed by the public. (NAIH/2020/8803)

The detailed job specification of a given public employee (which includes his work processes and activities, tasks, functions and networks, including goals, main areas of responsibility and the conditions under which he performs his work as well as the authorities and powers he may exercise) are data accessible on grounds of public interest, irrespective of the fact that they Act on legal standing does not provide for it. (NAIH/2020/6526)

In relation to the accessibility of a work contract concluded with the employee in a non-managerial position of a non-profit limited liability company held by a municipality (municipal television), NAIH expounded that it must be established whether the person concerned discharges public duties, in which of the public duties performed by the non-profit limited he participates and which are the data in his work contract which are relevant to the discharge of public duties. (NAIH/2020/2948)

At the same time, the certificate verifying the highest level of education of a mayor is not accessible on the grounds of public interest because there is no

legal regulation specifying the level of education that would be the precondition to filling the position of mayor. (NAIH/2020/5627**).**

IV.9. Transparency of municipalities

IV.9.1. Data accessible with respect to the utilisation of municipal assets

Relative to NAIH's guidance concerning the transparency of the operation of municipal bodies published in 2019, a new question arose in 2020, namely what data are accessible under a request for data in the public interest in the case of a "*public actor tenant*". In view of the earlier statement of the data protection commissioner[21] and the judgments of the Constitutional Court[22], the Authority's position is that when a natural person, who is public actor, rents a property held by the municipality and this fact is in the public domain or there is a statement about it by the data subject, *the name of the tenant, the address of the tenement, the existence and period as well as the legal grounds for the rental relationship and the amount of the rent* established are accessible by anyone on the grounds of public interest. In the case of *so-called special public actors* [see Constitutional Court Decision 26/2019. (VII. 23.)] the controller (municipal executive) is responsible to assess access to which data would facilitate the transparency of the management of municipal assets without giving rise to disproportionate infringement of the privacy of the data subject (fundamental rights protection test). [NAIH/2020/6790.]

In another statement, the Authority separated access to the data of natural persons accessible on grounds of public interest, who have concluded a contract with the municipality, from the accessibility of the names and other personal data of the municipal tenements rented on a welfare basis. The name and the personal data concerning the existence of the rental relationship of a natural person renting a tenement from the municipality (the address of the tenement and the period of the rental relationship) are accessible on the grounds of public interest even if the tenant rents the property owned by the municipality on a welfare basis; however the tenants of municipal properties rented on a welfare basis cannot be

21 „[...] ***this category definitely includes all persons exercising public authority and deciding on the use of public funds****. It is also clear that this is not a homogeneous group of people. Also, there are also no precise legal limits on what data persons performing public functions or acting in a public capacity are required to disclose and where their private life in the public domain begins. This can and should be decided on a case-by-case basis.*" [26/K/1999.]

22 30/1992. (V. 26.) AB, 36/1994. (VI. 24.) AB, 60/1994. (XII. 24.) AB, 7/2014. (III. 7.) AB, 1/2015. (I. 16.) AB, 3145/2018. (V. 7.) AB, 26/2019. (VII. 23.) AB

“listed”. According to Annex 2 point (j) of Act LXXVIII of 1993 on Certain Rules concerning the Rental of Flats and Premises and their Sale (from which the law does not provide any possibility to deviate), the differentiated amount of the rent on account of the nature of renting – welfare, cost-based or market-based rent – is part of the mandatory content of the municipal decree enacted on renting flats. It follows from this that the rent established by the local body of representatives, including the amount of the welfare-based rent, is considered data in the public interest accessible to anyone. [NAIH/2020/5043.]

Related to the above, a citizen requested data concerning decisions made at a closed session of a city municipality with regard to the utilisation of municipal assets (designation of tenants, renting municipal property, sale, designation for sale) and the valuers’ opinions and data related to tendering as part of the decision-making process. In the course of its investigation, the Authority established that in contrast to the controller’s statement, the body of representatives regularly makes its decisions on asset utilisation issues in closed meetings and the data of the decisions made in closed meetings, which should be accessible are unavailable for citizens on a public interface. [NAIH/2020/7971.]

IV.9.2. Municipal meetings, “leakages”

The Authority carried out its data protection procedure investigating a request, according to which a representative of a rural municipality uploaded a voice recording he made of a private meeting convened by the mayor without informing, and obtaining the consent of, the data subjects, to his own public actor’s site of the community portal. The subject matter of the meeting was a construction project with severe impact on the built and protected natural environment, whose licensing process commanded nationwide attention because of the protestations of local residents and environmental activists. The mayor requested the Authority to conduct its procedures on the grounds that the voice recording – expressly his voice recorded – was published without his permission, whereby his right to the protection of personal data was infringed. The Authority rejected the complainant’s request on the following grounds:

Municipal transparency is a basic principle protected by law. The Municipal Board of the Supreme Court declared that access to the meetings of the municipal body of representatives is an important requirement of a democratic constitutional state, decision-making with the exclusion of the public may only take place in warranted cases predetermined by law within a narrow range. The participants of the given discussion might have been the participants of a meeting of a municipal body of representatives convened regularly who acted as public actors discussing and

obtaining new information on the planned investment into a hotel regarded as an outstanding public affair by citizens directly affecting the town and its residents. In its decision, the Authority underlined that the fact of a discussion on an investment planned in a Natura 2000 protected nature conservation area and any information discussed in relation to that investment are to be regarded as environmental information to which privileged wide-ranging access must be guaranteed to the public. Because of the above circumstances meriting individual consideration, the Authority exceptionally accepted the lawfulness of processing even though the voice recording was made in a covert, secret way and the recorder did not inform the data subjects of its publication. (NAIH/2020/4014)

The case in which a journalist turned to NAIH with regard to video and sound recording equipment "found" in the meeting room of the body of representatives of a city of county rights also commanded a great deal of interest. The data available to NAIH did not verify any fact or circumstance indicating that there actually was an infringement of data security (incident), but it called attention to the fact that if there was unlawful sound or video recording that would not qualify as a data protection incident, but as unlawful processing. (NAIH 6636/2020, NAIH 6599/2020)

In a case related to access to votes cast at a closed session, the election of a new external committee member took place under one of the agenda items of the initially public meeting, in the course of which a closed meeting was ordered upon the request of the person concerned. According to the complaint, the opposition representative unlawfully disclosed the data concerning the voting by name on the decision made in a closed meeting.

The legal rules applicable to the member of a committee of a body of representatives who is not a representative (conflict of interest, honorarium, benefits in-kind, cost reimbursement) are the same as those applicable to the municipal representatives as in the course of performing the committee's work, they participate in decision-making and may have functions with very similar responsibilities to those of members of the committee who are representatives. In the course of the procedure, the Authority underlined that pursuant to Section 46(2)(b) of Act CLXXXIX of 2011 on Hungary's Municipalities (hereinafter: Municipalities Act), the body of representatives shall hold a closed meeting upon the request of the data subject for the discussion of elections, appointments, dismissals, giving and withdrawing managerial mandates, launching disciplinary procedures and personnel cases requiring a statement. In such a case, the primary criterion is the protection of the personal data of the data subject as he is entitled to request a closed meeting. The data generated in the course of the discharge

of the public duties of the representatives making the decisions, including their votes cast for the decision, qualify as data accessible on the grounds of public interest pursuant to Section 26(2) of the Privacy Act. The Authority supported its position with the provisions of the statement ABI/1344/K/2006-3 of the Data Protection Commissioner, according to which "*[…] those applying the law shall take particular care in examining whether the conditions of ordering a closed meeting and thereby restricting access for the public obtain. […] In view of the justification for holding a closed meeting, the right of inspection does not apply to the protocol of the closed meeting. However, if the minutes of the closed meeting contain data which are otherwise accessible, information must to be provided on it. Such data are, for instance, the decision itself or specific data concerning public finances and contracts. In my view, the representatives' votes cast in a closed meeting should be regarded as data accessible on the grounds of public interest, unless it was a secret ballot. The constituents have a right to monitor the activities of the representatives and of the body of representatives even in the case of holding closed meetings to the extent that it is not concomitant with the infringement of trade secrets and the right of others to the protection of their personal data (excluding representatives). [...]"* (NAIH/2020/5737)

IV.9.3. The right of the mayor and of the municipal representative to access data

In our reports we regularly mention[23] the problems related to the right of municipal representatives to be informed emphasizing that if the representative wishes to exercise his right to access data in the public interest or data accessible the ground of public interest, and not his right to be informed as set forth in the Municipal Act, the rules of the Privacy Act are to be applied when complying with the data request just as in the case of any other citizen. Being a mayor or representative in itself does not authorise these persons to have access to and process personal data. A representative does not have independent responsibilities and powers, his "work as a representative" consists in the participation in the preparation of decisions on certain cases within the competence of the body of representatives and its committees, in the organisation of the implementation or the control of the decisions. It is another matter if a law or municipal decree enacted on the basis of some law authorises the mayor and/or the representative to have access to some kind of data and to process them with a view to discharging his public duties or if the body of representatives of the municipality entrusts him individually or as member of a committee with the planning organisation or control with a task within the competence of the municipality. In such cases, the representative/

23 See Annual Report of 2018 IV.2.2.

mayor may process the indispensable personal data and those listed in legal regulation complying with the principle of purpose limited processing.

In a submission for consultation received by the authority, the mayor of a rural municipality wished to have access to data related to local tax and taxpayers. The data concerning taxation qualify as tax secret, thus the mayor and the body of representatives are authorised to access them only if the municipal tax authority (the municipal executive) decides that pursuant to Act CL of 2017 on the Order of Taxation it is necessary to publish a refutation or to publish the range of data specified in Section 130(1) as is customary at the place or if the data subject has consented to using the tax secret. A mayor and members of the body of representatives are not authorised to have access to and process tax secrets, they may have access to certain tax types and the data concerning the amount of tax arrears in relation to local taxes in a way that is not suitable for the identification of persons. (NAIH/2020/7554/2).

In another submission for consultation, the head of a long-term residential home for the elderly asked questions in relation to forwarding certain personal data of the residents to the municipality. The data requested by the mayor concerning those looked after in the social institution, their relatives, those waiting for vacancies may be issued based on Section 24 of Act III of 1993 on Social Administration and Welfare Benefits. Just because a municipality wishes to takeover a social institution, the issue of personal data of the residents, the persons waiting for vacancies and their relatives does not comply with the rules of either GDPR or the Social Act even if it is said to be part of the preparation for the takeover. (NAIH/2020/7560/2)

In another case, a municipal representative submitted a request in connection with the processing of personal data from the land registry in the body of representatives' proposal related to their right of pre-emption. The Authority underlined that in making proposals for the meeting of the body of representatives on its agenda accessible to the public, the lawfulness of the processing of personal data must be complied with and in the specific case, in addition to Act V of 2013 on the Civil Code, the rules of Act CXLI of 1997 on the Land Registry must also be taken into account. According to the position of the Authority, using public access to the land registry and the right to access data on the property sheet in a way that deviates from the original purpose of the accessibility of property data infringes the right to the protection of personal data, including the requirement of purpose-limited and fair processing. With a view to the enforcement of the principles of data processing, the body discharging public duties must examine in every case whether the restriction of accessibility is warranted and if so, in the case of which data. (NAIH/2020/7660/2)

IV.9.4. Cases of the self-governments of ethnic minorities

In 2020 (unexpectedly relative to previous years), the Authority received a series of complaints against the self-governing bodies of ethnic minorities (requests for data in the public interest, unjustified extension of the time limits for compliance, demanding cost reimbursement, failure to disclose documents electronically). In the course of the procedures, the Authority paid particular attention to the content of the agreement between the municipality and the self-governing body of the ethnic minority in accordance with Section 80(3) of Act CLXXIX of 2011 on the Rights of Ethnic Minorities. Upon the recommendation of the Authority, the municipality under investigation initiated a review of the agreement already in force, and the amendment of the areas of cooperation in order to enable access to the data in the public interest and the data accessible on grounds of public interest of the self-governing bodies of ethnic minorities in the way required by the Privacy Act. (NAIH/2020/8134)

IV.9.5. Disclosure lists by municipalities

Every year, NAIH receives a number of complaints concerning the deficiencies in meeting the disclosure obligations of municipalities and business organisations in municipal ownership largely in relation to the documents of the meetings of the body of representatives (minutes, submissions, decisions, decrees) and data related to financial management (contracts, grant applications). If, in the course of its investigation, NAIH establishes deficient electronic disclosure, it calls upon the body concerned to disclose the relevant data and documents. By and large, NAIH's measures have been successful and the municipalities endeavour to comply with NAIH's call.

IV.9.6. Statements of assets

In view of the questions recurring year after year, particularly with respect to the mayor, the deputy mayor and the municipal representatives, NAIH published a summary guidance paper on the accessibility of statements of assets in its website in 2020.[24] Pursuant to the provisions of the Privacy Act and of the Municipalities Act, the statements of assets by the mayor, the deputy mayor and the representatives are accessible on grounds of public interest and they must be made accessible to anyone by way of data request. Based on the special

24 https://www.naih.hu/files/Tajekoztato_a_vagyonnyilatkozatok_megismerhetosegerol.pdf és https://www.naih.hu/files/vagyonnyilatkozat_leporello_20201005.pdf

rules of Section 39 of the Municipalities Act, the committee members who are representatives are subject to an obligation to make a public statement of their assets, while external committee members have to make non-public statements of their assets, as there are no special provisions in the Municipalities Act for this situation, the provisions of Section 3(3) of Act CLII of 2007 on Certain Obligations to Make Statements of Assets govern, which stipulates an obligation to make non-public statements of assets even for those not employed by the public sector who would otherwise not be required to make statements of assets based on separate legal regulations for filling positions and performing tasks of extraordinary significance for the integrity of public life..

Currently, Annex 1 to the Privacy Act does not provide for the mandatory publication of the statements of assets of municipal representatives. At the same time, there is no provision to prohibit the publication of statements of assets by the municipalities in individual disclosure lists. The legal provision referred to fundamentally serves the purpose of enabling anyone to access to the statements of assets of municipal representatives without restriction. In view of the fact that publication in the Internet facilitates simpler enforcement of the constituents' right to information and it is in line with the intentions of the legislator, publication in this way is permitted for municipalities but this option may be used only if they enact individual disclosure lists to that end. (NAIH/2020/755, NAIH/2020/1435, NAIH/2020/2813, NAIH/2020/7681)

IV.9.7. Canine registry

In 2020, NAIH received a substantial number of submissions, in which the person requesting data wished to have access to various items of the canine register kept by the municipalities largely to learn the number and breeds of dogs in the given settlement/district. NAIH contacted the municipalities concerned and based on their replies, the following problems emerged:

Municipalities have user level access to the national register, but users cannot query the list of dogs kept in a given settlement in a breakdown by breeds from the database. The only possibility to obtain the data is if the user queries the roughly 600 dog breeds from the database one-by-one. Unfortunately, in many cases, the veterinaries, who enter the data of the animals in the register after marking them with electronic transponders (microchips), use some alternative name rather than the official name of the breeds when entering it (e.g. German shepherd dog: German shepherd, Germanshepherd, Gs, or West Highland white terrier: westie, weszti, etc.). According to the information provided by the municipalities, the credibility of the data is greatly distorted by the fact that only the veterinaries have a level of access to the register, which allows for the modification or erasure of the

data of dogs that are no longer in a given settlement because they died or there was a change in ownership or the owner moved. Another problem is that the date of the dog census to be carried out by the municipalities every three years is not harmonised which means that the municipalities gather the data at different times. NAIH contacted NÉBIH (National Food Chain Safety Office), which confirmed that municipalities as users have access to the database, but they cannot launch a query by a single click that would list the dogs in their area of competence by breed. NÉBIH also agreed with the municipalities' statement according to which a breed may appear in several forms; having recognised this, dog breeds can be selected from a drop-down menu for years now, and the correction of the inaccurate legacy data has begun. The data in the database cannot be altered by the municipality, not even by the operator of the database, only by the reporting veterinary. In view of the fact that the municipalities are truly unable to provide credible data on the number and breed of the dogs in their area of competence, the Authority finds it acceptable that individual municipalities direct persons requesting data to NÉBIH when meeting the requests for data in the public interest. The findings of the investigation are presented in the public guidance available in the website[25]. (NAIH/2020/233, NAIH/2020/234, NAIH/2020/239, NAIH/2020/581, NAIH/2020/583, NAIH/2020/584, NAIH/2020/1057)

IV.10. TASZ's comprehensive data request case

In 2019, the Társaság a Szabadságjogokért (TASZ; Hungarian Civil Liberties Union), a human rights association (hereinafter: data requester) submitted requests for data in the public interest to every government office in connection with the implementation of the provisions of the new Civil Code calling for the mandatory court review of decisions made prior to 2013 concerning the guardianship of persons excluding legal capacity. Every one of the government offices assessing the data request demanded cost reimbursement on the grounds that meeting the data request would disproportionately use the available labour force, the extent of which was greatly different county by county. The lowest amount was requested by Vas county at HUF 27,275, while the highest amount was requested by Hajdú-Bihar county at HUF 624,340. In view of this, the data requester submitted *a second modified request for data* to the government offices, in which they waived answering the question that would have required a review of the files, but referred to Government Decree 388/2017. (XII. 13.) on the mandatory provision of data by the National Statistical Data

25 https://www.naih.hu/files/ebnyilvantartas-2020-tajekoztato.pdf és https://www.naih.hu/files/ebnyilvantartas-2020-leporello.pdf

Capture Programme,[26] which requires district offices to mandatorily provide data on the review of the guardianship of people. Counties Csongrád, Fejér, Jász-Nagykun-Szolnok, Nógrád, Pest, Szabolcs-Szatmár-Bereg and Tolna, as well as the capital city Budapest met the data request without demanding cost reimbursement, but they received absolutely no answer from 12 government offices, so they contacted them with *a third request for data in the public interest* on 13 December 2019, relative to the earlier data request, this time only asking the questions below:

- altogether how many reviews were launched for persons under guardianship,

- of them, for how many reviews began within the statutory period,

- and how many reviews were launched belatedly.

In their letter they stated that according to their experience (based on the answers of the government offices meeting the data requests free of charge) it can be established that the registries may be suitable for accessing more detailed data. The table summarises the results of the three submitted data requests:

Government office	1st data request	2nd data request	3rd data request
Bács-Kiskun	38,800	no reply	30,800
Baranya	111,956	no reply	no reply
Békés	282,239	no reply	8,742
Borsod-Abaúj-Zemplén	120,957	no reply	90,938
Csongrád	236,802	no reply	521,123
Fejér	57,200	data provided	57,200
Budapest	105,000	data provided	no 3rd data request
Győr-Moson-Sopron	50,275	no reply	16,088
Hajdú-Bihar	624,340	no reply	388,841

26 In table in Annex 1 to Government Decree 388/2017. (XII. 13.) on the National Statistical Data Capture Programme, (point 1210) subsection (21) of the part on the activities of the guardianship authority specifies the description of the data to be provided and the obligee: District office; the data of persons under guardianship (type of guardianship, persons under guardianship in a breakdown by age and sex, data on the review of subjecting them to guardianship, exclusion from the franchise, the person and employment relationship of the guardian and data of supported decision-making).

Heves	312,743	no reply	no such data processed
Jász-Nagykun-Szolnok	76,560	data provided	no 3rd data request
Komárom-Esztergom	37,220	no reply	38,356
Nógrád	120,609	data provided	no 3rd data request
Pest	did not respond	data provided	108,000
Somogy	38,552	no reply	7,586
Szabolcs-Szatmár-Bereg	185,918	data provided	28,533
Tolna	37,428	data provided	18,860
Vas	27,275	no reply	15,441
Veszprém	44,040	no reply	30,784
Zala	124,212	no reply	124,212

In the first phase of the investigation, the Authority focused on cost reimbursement. When contacted by the Authority, all the government offices responded in merit: two government offices (Borsod-Abaúj-Zemplén and Heves counties) met the 2nd and the 3rd data requests without demanding cost reimbursement. Based on the replies received, the Authority terminated the investigative procedures in the case of the government offices of the counties Borsod-Abaúj-Zemplén, Heves, Jász-Nagykun-Szolnok and Nógrád and the Budapest Government Office as the circumstance giving rise to the investigation no longer existed as they met the data request. Depending on the content of the responses, the fact of the infringement of the Privacy Act and the severity of the infringement, the Authority continued the investigation against the other government offices and called their attention to the following:

- if a body discharging public duties disregards a request for data in the public interest that in itself provides grounds for the infringement of the right to access data in the public interest,

- Section 29(1)(a) of the Privacy Act does not exempt the body discharging public duties from responding to the data request, but only from re-disclosing the data, and is only applicable if the data request has been previously fulfilled,

- the cost reimbursement communicated pursuant to Section 29(3) of the Privacy Act is not a preliminary calculation pursuant to the Act, but the actual

determination of the cost reimbursement, which is indicated by the fact that if the requester accepts the amount communicated, the body discharging public duties may deviate from that amount only downward based on the actual costs incurred and it also has a reimbursement obligation pursuant to Section 5 of the Decree on Costs; moreover the requester may dispute not only the amount of the cost reimbursement, but its justification also, either in court or before the Authority,

- transparency is best served by the institution providing information concerning the cost reimbursement charged for meeting the request for data in the public interest: the more detailed the information, the more efficiently it fulfils its role; also, the body discharging public duties will ab ovo be able to demonstrate both the justification for demanding cost reimbursement, its legal basis and the correctness of its amount in the event of a legal dispute/investigation in court or before the Authority,

- as head of the government office, the government commissioner is responsible for the implementation of tasks related to the freedom of information (see Section 7(f) of Decree 3/2020. (II. 28.) MvM on the organisational and operational rules of the Budapest and county government offices),

- in the cases under investigation, the data were collected by the organisational units of district offices or by government officials working for the county government office, which required 1 to 6 hours of work of one or two people at each organisational unit, which obviously does not qualify as disproportionate use of the labour force needed for discharging basic tasks, even if we otherwise naturally accept the fact that government offices are overburdened.

Upon the call of the Authority, the government offices complied with the data request almost without exception. Repeated third calls took place in altogether three cases with a view to the clarification of the data provided (the government office of one county continued to demand cost reimbursement even in the case of the third data request and another one failed to communicate the data generated to the requester for administrative or technical reasons). Based on the responses received, the case was closed finally in February 2021 in a reassuring manner. (NAIH/2020/1405)

IV.11. Data requests en masse

The following two new types of group requests for data should be separated

from the above “poster child case”. In the first one, a private individual requester contacted 55 hospitals requesting the same types of data; he intended to submit data request all over the country. The requester posted questions to the hospitals concerning methods and procedures of medical science. The claimant objected to the fact that the public institutions complained against did not answer his data requests, a smaller number of them rejected the issue of the data or demanded cost reimbursement for compliance with the data request. According to the position of the Authority, the data requests submitted en masse and in a comprehensive manner could be suitable for a full-scale statistical monitoring of health care, but the group request for data was not aimed at rendering public affairs more transparent or discussing them, they did not directly facilitate access to information of merit on the discharge of the public duties of the given institution, hence they did not comply with the social purpose of the fundamental subjective right. (NAIH/2020/6118, NAIH/2020/6119, NAIH/2020/6120, NAIH/2020/6121)

Another complainant submitted a significant number of data requests for different data to the same municipality. He lodged 22 complaints with the Authority in 2020, however, the body discharging public duties had to comply with a great deal more data requests over a short period of time. Some of the requests were well-founded and accordingly the Authority called upon the municipality to issue the data, but in relation to the extension of the period open for compliance, the Authority accepted the argumentation of the municipality, namely that compliance with the large number of data request within a relatively short period of time would be concomitant with the disproportionate use of the labour force needed for the discharge of its basic activities and would greatly encumber the operation of the mayor’s office working only with a small headcount. (NAIH/2020/5857, NAIH/2020/6587, NAIH/2020/6299, NAIH/2020/6584)

IV.12. The accessibility of environmental information

It can be concluded from the petitions that not only those requesting data, but also those processing them find it hard to negotiate their way in the system of environmental information: by which bodies process them, in what databases are they managed?

A request for the issue of the decisions concerning the environmental pollution reported by Mátrai Erőmű Zrt. (Mátra Power Plant Ltd, hereinafter: Zrt.) in the summer of 2019 and on 15 January 2020 was rejected by the Eger District Office of the Heves County Government Office (hereinafter: District Office) on the grounds

that it did not process the requested data, but the complainant did not receive any further information. NAIH called the attention of the District Office to Section 12(6) of Act LIII of 1995 on the General Rules of Environment Protection (hereinafter: Environment Protection Act): *"If the contacted body does not have the requested environmental information, it has to send the request concerning access to the information to the body that has the environmental information and to notify or inform the petitioner about the body having the environmental information from which to request the information."* The data requested by the complainant qualified as environmental information pursuant to Section 2(c) of Government Decree 311/2005. (XII. 25.) on the order on public access to environmental information. In addition to the District Office, the complainant contacted numerous other bodies and also lodged several complaints with NAIH. All this could have been avoided, had the District Office met its obligation to provide information. (NAIH/2020/4606)

The complainant also submitted a request for data in the public interest to the Mátrai Erőmű Zrt. (hereinafter: Zrt.), but according to the Zrt. the requested decision (imposing a fine because of the extraordinary water pollution caused by the sewage issuing from the industrial water reservoir at Őzse-völgy operated by the Mátrai Erőmű Zrt. between 22.07.2019. and 28.08.2020.) did not contain any data in the public interest or data accessible on the grounds of public interest because at the time of the data request, the Zrt. did not manage public funds, it was not a body discharging public duties and its shareholders did not include the Hungarian state whether directly or indirectly having majority or decisive influence; moreover, at the time of the data request it did not qualify as a public body or body discharging obligations related to the environment or providing public services or discharging other public tasks, which would have to make accessible the environmental information available to it, if requested pursuant to Section 12(3) of the Environment Protection Act. NAIH established that the Zrt. disregarded the obligation of users of the environment set forth in Section 12(9) of the Environment Protection Act, according to which "*The user of the environment shall provide information on the data related to environmental load caused by it, its use of the environment and threat to the environment upon request to anyone*". The justification of the act clearly explains that "*not only the bodies discharging public duties, but the users of the environment are also under an obligation to provide information, taking into account the rules of data protection and public administrative procedure*". The Zrt. clearly qualifies as a environmental user that uses the environment, burdens the environment and conducts activities polluting the environment, hence in NAIH's opinion, the data in the requested decision are data accessible on the grounds of public interest. According to the position of the Zrt., complying with the request of the complainant would be contrary to the

legitimate interest of the Zrt. that "*the eventual criminal liability of the company should not be discussed in public, it should not be established based on the data issued by us to those requesting the data during a criminal procedure*", because according to the information provided by the Zrt., there was a criminal procedure in progress at the police stage on the grounds of the felony of damaging the environment at the time of the submission of the data request. Although Section 27(2)(c) of the Privacy Act permits the restriction of the right to access data in public interest and data accessible on the ground of public interest specifying the types of data with a view to prosecuting criminal acts (provided that the law enforcement agency confirms this in the specific case with its statement), it however does not include the "legitimate interests" mentioned by the Zrt. Complying with NAIH's call, the Zrt. finally met the data request. (NAIH/2020/1819)

In another case, a waste management non-profit limited liability company (hereinafter: Kft.) should have answered the questions of what was the annual amount of waste received by one of its branches in a breakdown by type of waste in terms of quantity and the points specified in the IPCC permit. According to the Kft., the requested data are data accessible on the grounds of public interest, but they constitute trade secret of the Kft., which is not subject to Section 27(3) of the Privacy Act. In its investigation NAIH established that the requested data were accessible from the Uniform Waste Management Information System. According to Section 1(1) of Act LIV of 2018 on the Protection of Trade Secrets *"Trade secret is a fact, information, other data or a compilation of these, related to a commercial activity, which is secret in the sense that it is not, in whole or in a configuration of its components, generally known or readily accessible to persons performing the affected commercial activity and therefore it has a commercial value, and which has been subject to reasonable steps under the circumstances, by the lawful beneficiary of the information, to keep it secret".* As data accessible to the public cannot qualify as trade secret, hence NAIH called upon the Kft. to issue the requested data, which the Kft. did. (NAIH/2020/434)

A persistent problem with data requests for environmental information is that controllers interpret requests for data in the public interest concerning environmental information as requests for access and make compliance with them conditional upon client status. A government office referred to non- client status when the complainant wished to have access to building permits and the underlying documentation. The area affected by the development was a nature conservation area under Natura 2000 protection, hence NAIH established that the requested data qualify as environmental information and as such data in the public interest. The government office met NAIH's call and complied with the data request. (NAIH/2020/6703)

V. The Authority's activities related to legislation

V.1. The statistical data of cases related to legal regulation

Relative to the data of earlier years, the number of draft legislation and legal regulations, on which the Authority provided an opinion, shows a declining tendency overall in 2020, although no substantial difference can be detected, if the levels of legislation are studied one-by-one. Despite the decline in the number of cases, the number of observations and recommendations of merit put forward by the Authority in 2020 increased relative to the number of observations made in earlier years.

The Authority's experiences reveal that in some cases the ministries preparing the drafts of legal regulations failed to involve the Authority in the reconciliation of drafts related to the protection of personal data and the accessibility of data in the public interest. Unfortunately, this was particularly conspicuous in the autumn of 2020 as the Authority received a much smaller number of draft legal regulations to provide opinions on than was usual, at the same time many drafts were uploaded to the website of the Parliament among the submitted bills, which contained data protection aspects, yet the Authority was not involved in the reconciliation by the ministries preparing the drafts.

Number of cases related to legal regulation annually and by level of legislation

Level of legislation/ year	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
Act of Parliament	85	49	86	33	79	85	82	72	61	73
Government decree	75	60	89	63	133	98	89	47	49	52
Ministerial decree	104	70	92	85	126	83	94	55	41	27
Government decision	26	12	28	21	61	29	33	40	34	22
Other (Parliament decision, instruction, etc.)	10	16	15	7	27	20	23	17	29	10
Total	**300**	**207**	**310**	**209**	**426**	**315**	**321**	**231**	**214**	**184**

Statistics of substantive observations made in legislative opinions

Nature of observations							
	2014	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**
Related to data protection	145	298	222	461	487	323	436
Related to freedom of information	21	53	101	28	22	39	80
Other	53	137	127	92	79	78	37
Total	**219**	**488**	**450**	**581**	**588**	**440**	**553**

V.2. Cases related to legal regulation during the emergency

In 2020, the Authority regarded the provision of opinions on draft legal regulations under preparation as priority issues during the period of emergency just as in earlier years. To that end, it closely cooperated with the experts in the ministries responsible for the preparation of legal regulations, followed up on legislative trends in the European Union, monitored the bills submitted to Parliament and made substantive observations on issues related to the protection of personal data and the accessibility of data in the public interest.

V.2.1 Emergency

The Government announced an emergency from 11 March to 18 June in Decree 40/2020. (III. 11.), then Government Decree 478/2020. (XI. 3.) again announced an emergency on 3 November. During these periods, the Authority participated in providing opinions on draft legal regulations related to the announcement of emergency on an ongoing basis.

In relation to a state of emergency, it is important to underline that pursuant to Article 53(2) of the Fundamental Law, in a state of emergency the Government may adopt decrees by means of which it may, as provided by a cardinal act, suspend the application of certain acts, derogate from the provisions of acts and take other extraordinary measures. It was on the basis of this authorisation that Government Decree 179/2020. (V. 4.) on derogation from certain data protection and data request provisions during the state of emergency entered into force. According to the provisions of the Government Decree, any measures to be taken based on a request submitted to exercise data subject right according to Section 14 of the Privacy Act and Articles 15-22 of the General Data Protection Regulation shall be suspended until the end of the state of emergency, the starting day of the periods open for taking these measures shall be the day following the termination of the state of emergency. Data subjects shall be informed of this immediately after the termination of the state of emergency, but within ninety days from receipt of the request at the latest.

The Government Decree restricted access to data in the public interest and data accessible on the grounds of public interest for the period of the state of emergency as follows. Until the termination of the state of emergency, requests to access data in the public interest may not be submitted orally notwithstanding Section 28(1) of the Privacy Act and the data requests can be met in the form desired by the person requesting the data, if it does not involve the personal

appearance of the person in front of the body discharging public duties according to the Privacy Act.

The controller shall comply with request to access data in the public interest or data accessible on grounds of public interest within 45 days from receipt of the request if it is probable that compliance within the period set forth in Section 29(1) of the Privacy Act would jeopardise the discharge of the public duties of the body related to the state of emergency. The person requesting access shall be notified of his within 15 days from receipt of the request. This period may be extended on one occasion by 45 days, if meeting the request during the period of emergency according to paragraph (3) would continue to jeopardise the discharge of the public duties of the body discharging public duties according to the Privacy Act related to the state of emergency. The person requesting the data shall be informed of this prior to the expiry of the period set forth in paragraph (3)

The Government Decree lost effect simultaneously with the termination of the state of emergency.

With regard to the emergency declared in the autumn, Government Decree 521/2020 (XI. 25.) on the derogation from certain data request provisions during the emergency provided for data requests in the public interest.

V.2.2 Data protection incidents

Exercising its right to make recommendations guaranteed by Section 38(4)(a) of the Privacy Act, the Authority contacted the competent departments, the Ministry of Justice and the Ministry of the Interior to resolve the following problem:

Pursuant to Section 2(3) of the Privacy Act, the Privacy Act shall apply for the processing of personal data for law enforcement, national security and defence purposes. Sections 25/J. and 25/K. of the Privacy Act provide for the management of data protection incidents. Pursuant to Section 25/K(1), if a data protection incident is likely to have consequences that would substantially influence the enforcement of a fundamental right due to the data subject (high risk data protection incident), the controller shall inform the data subject of the data protection incident without delay except for cases of processing for national security purposes. Paragraph (2) of the same section lists the exceptions, which – if they prevail – the controller shall be exempted from the obligation to inform the data subject. Pursuant to Section 25/K(2)(d) such a condition is, if law excludes the provision of information. According to paragraph (6) of the same section, a law may exclude, restrict or delay the provision of information to the data subject under the condition set forth in Section 16(3).

It has already occurred in a case before the Authority concerning a data protection incident in the context of a criminal procedure that the controller authority did not inform the data subjects in general terms referring to law enforcement interest without indicating the relevant provision of a legal regulation. Moreover, because of the regulatory environment, a situation like this could arise again at any time in the future when a controller wants to be exempted from the obligation to provide information on the grounds of law enforcement interest because it is obvious that in certain cases providing information to the data subjects could jeopardise the success of the criminal procedure, and it is therefore justified not to do so.

It follows from the provisions of the Privacy Act that in such cases the provisions of the sectoral law could provide the appropriate legal basis for not providing information to the data subject. Act XC of 2017 on Criminal Procedure does not provide for the rules of on the information to be provided to the data subject in eventual data protection incidents.

In view of Sections 16(3)(a) or (d) of the Privacy Act similar reasons may arise in relation to misdemeanour proceedings. Act II of 2012 on Misdemeanours, Misdemeanour Proceedings and Registration System of Misdemeanours does not provide for the rules on the information to be provided to the data subjects in eventual data protection incidents.

V.2.3 The eradication of illegal waste disposal

The consultation on the submission to set up a waste management authority as a first step towards the eradication of illegal waste disposal and the rationalisation of the waste management sector was a process taking several months, in the course of which the Authority studied and provided opinions on several versions of the draft bill, draft government decree, ministerial decree and government decision jointly included in the submission. From the viewpoint of data protection the most important element of the draft package was surveillance for the 32,000 kilometre road network managed by Magyar Közút Nonprofit Zrt. using technical devices. There are many parts of the road network where it is possible to dump waste illegally and preventing it with human labour only is impossible. According to the submission, the fix camera systems already installed along the road network (surveillance cameras, web cameras, traffic AID cameras) are not suitable for the prevention of illegal waste disposal and the identification of the colour, registration number and type of vehicles and human faces with conclusive force owing to their technical solution and their points of installation. Because of this, the submission foreshadowed the future deployment of a new fixed set of cameras to be installed later to achieve this goal. The submission did not yet provide any information on the details, but wished to settle the data protection issues arising.

According to the submission, the following technical solutions were planned to be deployed in order to eradicate illegal waste dumps:

- fixed set of cameras (high resolution AID cameras and mobile, zoomable, focusable cameras) in places where illegal waste disposal is characteristic (at the resting points along the high-speed road network) in a single network using a uniform PC application;
- use of drones in places difficult to access, complemented with the use of spatial IT system;
- use of a mobile camera system: high resolution AID cameras, providing pictures of a quality suitable to identify registration numbers, in a single network, using a uniform PC application;
- on on-board camera built into a vehicle, whose recording would be manually saved, if warranted;
- use of body cameras by officers carrying out checks in the event of flagrante delicto;
- mobile device and application built into a vehicle, supporting the survey and eradication of illegal waste disposal;
- equipping road checkers with EDR radio to enable them to alert headquarters through shortcut keys.

From the viewpoint of data protection, the fact that the set of cameras will operate not as a separate unit, but in a uniform IT system has particular significance.

The Authority intends to continue to monitor the measures to be taken to eradicate illegal waste disposal, primarily the installation and deployment of the planned fix camera system, in view of the fact that this technical solution has substantial data protection aspects.

V.2.4 Cybersecurity Centre and Research Institute

The Authority underlined the following in its observation on the draft of the Act on the Amendment to Legal Regulations necessary for the establishment of the Cybersecurity Centre and Research Institute sent to it to provide an opinion on:

The draft intended to amend Section 56(e) of Act CXXV of 1995 on National Security Services (National Security Services Act). This amendment intended to provide an opportunity for national security services to intervene in the IT system without any restriction among the rules applicable to the covert collection of information subject to external permit.

In accordance with its earlier observation, the Authority maintained its position that the legal regulation of the possibility of intervening in the IT system should be developed separately from access to the data processed in the IT systems and their capture, i.e. data collection and obtaining information. Intervention in the IT system may constitute cyber-attack operations with regard to which the legal regulation must establish the guarantees of fundamental rights. Accordingly, it is also necessary to enact a set of rules on which areas, under which circumstances, for which purposes and against which entities (persons) cyber-attack operations cannot be carried out.

Finally, the legislator modified this provision by somewhat restricting the possibility of intervention by specifying the purpose, according to which national security services may intervene in the IT system based on an external permit for the purpose of preventing threats from cyberspace.

V.2.5 Governmental Personnel Decision Support System

The Governmental Personnel Decision Support System (KSZDR) is a new governmental IT system covering public service, whose purpose is to support the efficiency and professionality of human resource management in public service. The purpose of implementing KSZDR is

- to provide accurate and up-to-date information on the data of the personnel in the public service taken in a broader sense (public administration, law enforcement) relevant from the viewpoint of the operation and development of the state,
- to enable to a government to have access to statistics on the audited data of the bodies of public service more rapidly and in an automated manner to lay the grounds for decision-making,
- to provide information on the organisation and headcount of government agencies;
- to contain a cadastre of jobs and responsibilities based on the vacancies and job titles of government agencies;
- to operate a monitoring system on the human resource management of government agencies by involving fundamental and supplementary HR functions;
- to improve the efficiency of the use of institutional resources and to reduce and streamline the workload related to providing data by using the possibilities of automation;
- to enable institutions to simply reuse the collected information.

To date, government agencies were free to choose the IT system they used for keeping their basic records in the course of their HR activities. With the implementation of KSZDR in central public administration and law enforcement, the personnel record and administration system including data capture will become unified and HR process management will be more uniform than ever before. The new IT system to be developed will provide possibilities for including vocation-specific and unique employer requirements in the system. Updating in the new system will be built on its dynamic data processing capability, the heart of which is that it will be able to follow changes in legal regulations without using external developers.

From the viewpoint of data protection, the most interesting element of KSZDR is the public service personnel interface, which is a register with a data link capable of communicating with source systems, implementing full-scale recording, querying, maintenance and authorisation management functions.

The operation of KSZDR does not affect citizens in general, only those working in public service, including health care employees working in the state's health care institutions. Yet it is necessary for the Authority to pay particular attention to this new direction of personnel data processing, partly because of the large number of the data subjects concerned and partly because public service employees will not have an oversight of data processing in the newly implemented system in their everyday activities.

V.3. Providing opinions on draft legal regulations

The Authority continuously monitors the bills submitted to Parliament and uploaded to the parlament.hu website and reviews them from the viewpoint of data protection. If an unclarified data protection issue arises after submission or there is an obviously faulty regulatory solution in a bill, the Authority may turn to the designated parliamentary committee or to the legislative committee of Parliament to remedy the problem. Below, we address bills on which the Authority provided opinions ex officio.

V.3.1. Bill on family farms

Those responsible for preparing bill T/13261 on family farms failed to invite the Authority to provide an opinion, despite the content of the proposed legislation on data processing issues. On 25 November 2020, the President of the Republic sent the bill back to Parliament for consideration. The bill regulates the forms of operation of family farms and several of its provisions concerned the recording

and processing of data. The President of the Republic underlined that those responsible for preparing legal regulation have an obligation to invite the opinion of the Authority when bills relate to the protection of personal data and the accessibility of data in the public interest. The bill did not include the purpose of data processing with respect to the register of primary producers and the register of family agricultural companies and required access to, and publication of, personal data without this being necessary and proportionate to any purpose of data processing. The Ministry of Agriculture revised the returned bill based on the observations of the President of the Republic and invited the opinion of the Authority on it. In its opinion, the Authority called the attention of those responsible for the preparation of the bill to the mandatory elements of regulation set forth in Section 5(3) of the Privacy Act underlining that an act requiring data processing must define the purpose of processing personal data and transferring data with sufficient accuracy. (NAIH/2020/8323)

V.3.2 Bill to amend the Act on the Rights of Ethnic Minorities

Bill T/10303 on the amendment of Act CLXXIX of 2011 on the Rights of Ethnic Minorities (Ethnic Minorities Act) would have amended the Act by authorising the minister in charge of ethnic minorities policy to process the special sensitive data of students for the purpose of evaluating grant applications, grant disbursement and checking other requirements for entitlement. In relation to this, the Authority objected to the fact that the bill did not specify the types of special data to be processed, but it would have granted a quasi-general authorisation for the processing of any type of special data. Clearly, data processing for the above purposes cannot apply to any special data, such as the genetic data, political opinions or sexual orientation of the student.

According to the planned amendment, this provision of the Ethnic Minorities Act would not have complied with the principles of purpose limitation and data minimisation specified in GDPR Article 5(1)(b) and (c). Section 5(3) of the Privacy Act provides for the type of rules that have to be stipulated at the level of an Act of Parliament concerning data processing. This includes the type of data to be processed.

In order to develop a regulation aligned with GDPR and the general principles of data protection rules, the Authority recommended to clearly specify the relevant data type needed to be recorded for the purpose of evaluating grant applications, grant disbursement and checking other requirements regarding eligibility, such as the special data of the student concerning his nationality (his ethnic origin).

The Authority's objections were remedied by submitting a motion to amend the bill, hence Section 151(2) of the Ethnic Minorities Act entered into force with a regulation now appropriate from a data protection point of view on 1 July 2020.

V.3.3 Amendment of certain acts affecting defence

According to the bill on the amendment of certain acts affecting defence sent to the Authority to provide its opinion on, the designated forces of the Army and the Military National Security Service (KNBSZ) as joint controllers process the biometric data and the natural identification data of data subjects in the register of biometric data.

The Authority continued to maintain its earlier position set forth in its opinion in 2019 related to the 50-year retention period of biometric data, according to which it was unacceptable from a data protection point of view that the processing of biometric data should take place under the same conditions for the same period in a non-differentiated manner in the case of the forces of the Army and the opposing forces. According to the Authority's position, the processing of biometric data should be restricted to the data subjects participating in foreign operations. The Authority also maintained its earlier position concerning the erasure of the data as it was not aligned with the fundamental requirements of the protection of personal data and the rules of Act CXXV of 1995 on the National Security Services (hereinafter: National Security Services Act) concerning the erasure of data as the bill did not contain the possibility of erasing biometric data that were no longer needed or which were unlawfully processed. In relation to the rules of data transmission, the Authority observed that the bill failed to provide for which international treaties may allow the transfer of biometric data and differentiation with regard to the data subjects would be warranted also in this case so that only the biometric data of the opposing forces should be transmitted. The Authority also recommended to regulate the records of data transmission within the framework of an electronic log. The reason why the transmission of biometric data of opposing forces and persons is not exclusively required remains unknown, and the Authority has therefore expressed a reservation.

As the Authority had stated earlier, the National Security Services Act stipulates the responsibilities of the national securities services and the rules of data processing carried out by them. The data processing rules of KNBSZ related to its national security responsibilities must be aligned with the relevant provisions of the National Security Services Act. The National Security Services Act does not include any provision which would obligate data subjects to provide their biometric data, therefore KNBSZ can lawfully process only biometric data

voluntarily provided by the data subjects, obtained from open sources or through covert information gathering.

With regard to data processing related to the military police service, the bill set forth that warning signs and information have to be provided about the location of the camera and the essential elements of data processing in a manner that would facilitate the provision of information to persons shown in the video recordings. This general provision did not comply with the requirement of unambiguous comprehensibility, hence the Authority recommended that the act should specify these essential elements.

In relation to entry into the building, the 15-year retention period for the storage of the data as set forth in the bill results in unnecessary storage. In the case of data transmission, the bill referred to a body exercising the powers of an authority, not further specified, as possible addressee without specifically identifying it. Stating a broad collective notion instead of designating the addressees fails to comply with the constitutional requirements of data protection.

Based on the reconciliations, the ministry submitted amendments to the bill already submitted to Parliament, as a result of which the vast majority of the Authority's observations were included in the adopted act.

V.3.4 Opinion on the bill on the national data assets

With a view to launching a data economy, opening the state's data assets and the actual implementation of the reusability of the state's data assets, the Government set up the Nemzeti Adatvagyon Ügynökség (National Data Asset Agency - NAVÜ) and drafted the bill on national data assets, of which the Authority also provided an opinion. According to the bill, NAVÜ is responsible for facilitating the implementation of the Act on the Re-use of Public Data, the related operation of the national public data portal, the establishment and management of the national public data cadastre; the processing and analysis of databases anonymised with the cooperation of the key service provider designated by the Government and the body responsible for the processing of databases; providing data analysis services to the Government, the market and the citizens.

Furthermore, the bill recommended the establishment of the National Data Asset Board as the advisory body to the Government concerning the use of data assets, which also supervises NAVÜ's activities related to the provision of data. It is important to underline that the regulations governing data asset management have no bearing on the regulatory environment of accessing data in the public interest

as access to data in the public interest continues to be subject to the Act on the Right to Informational Self-Determination and the Freedom of Information. This regulation stipulates the rules of information services based on the appropriate linkage and analysis of registers managed by several controllers. Through these services, NAVÜ creates data sets based on data analysis carried out by it, which did not previously exist and were not available to any controller. Thus, there is a sharp delineation between data asset management and the regime of providing data according to the Act on Public Data, they have no bearing on one another's procedural rules.

NAVÜ's responsibilities include, inter alia, to provide data analysis services for the Government, the market and the citizens. In order to fully enforce the protection of personal data in the course of data provision and unauthorised bodies should not be able to access them even indirectly; in the case of requests related to the connection of databases based on personal data, the cooperating body processing the personal data has to use the services of the designated key service provider and carry out the appropriate anonymisation of the registers containing personal data and forward the data to the National Data Asset Agency in this way.

V.3.5 Consultation with citizens

Pursuant to Section 8(2) of Act CXXXI of 2010 on the Participation of Society in the Preparation of Legal Regulations, the minister in charge of drafting a legal regulation has to publish in the designated website (www.kormany.hu) and submit for consultation with citizens the drafts and concepts of acts of Parliament, government decrees, ministerial decrees, the summaries of preliminary impact analyses as well as the drafts not submitted for consultation with citizens and they may not be removed from there for a year from their publication. Anyone may express an opinion on the drafts and concepts published with a view to consultation with citizens through the e-mail address provided in the website.

The drafts of legal regulations on the following need not be submitted for consultation with citizens: payment obligations, state aids, the budget, the implementation of the budget, aid provided by the European Union or international funds, the announcement of international treaties and the foundation of organisations and institutions. Drafts and concepts may not be submitted for consultation with citizens, if it would jeopardise Hungary's particularly important defence, national security, financial, foreign affairs, nature conservation, environment protection or legacy protection interests. Draft legal regulations need not be submitted for consultation with citizens, if outstanding public interest is linked to its urgent adoption.

Although this legal provision has been in force since 2010 to this day, the Authority has noted that its implementation has not been carried out. In 2020, no drafts of legal regulations were uploaded to the website already operated by the Government. The Authority regularly calls the attention of the ministers drafting regulations to comply with their obligations concerning publication, but they failed to do so regularly. To date, the Authority has never received information on the reasons for this, or about any concept that may be behind this consistent behaviour on the part of the Government.

V.3.6 Regulatory recommendation concerning national security checks

The Authority made a regulatory recommendation to the Ministry of the Interior in relation to the regulation of national security checks. The Authority has for years followed the practice of informing the Alkotmányvédelmi Hivatal (Constitution Protection Office) of the termination of a legal relationship of a person with the Authority subject to national security checks, or if that legal relationship is no longer subject to national security checks. The objective was the full enforcement of data protection requirements, namely to prevent unnecessary checks and the unnecessary data processing by the Constitution Protection Office on persons whose legal relationship has in the meantime ceased to be subject to checks.

In 2020, the Authority recommended to the Ministry of the Interior that the obligation to notify the Constitution Protection Office about the termination of the legal relationship subject to national security checks of persons filling such legal relationships be stipulated in law. Section 72/A of the National Security Services Act in force contains the conditions of conducting, suspending and terminating national security checks; this provision, however, applies to national security checks in progress and not to those closed earlier. The relevant provision does not include any requirement for the initiator to notify the director general of the national security service in writing whether the legal relationship of a person subject to national security checks is terminated or it is no longer subject to national security checks. According to the Authority, it is advantageous for the protection of personal data if the Constitution Protection Office is notified of the termination of the legal relationship of a person subject to national security checks or if such a legal relationship is no longer subject to national security checks, because in this way it can be assured that the national securities services processed the personal data of data subjects with a view to discharging their duties set forth in the National Security Services Act only as long as it is verifiably necessary. It is important to note that such a transfer of data affects not only the cooperation between the Authority and the Constitution Protection Office, but also the operation of other agencies, such as the municipalities. *(NAIH/2020/5308)*

V.3.7 Act XLII of 2020 on the Amendment of Certain Acts concerning the Act on the Information Exchange within the Schengen Information System

In accordance with Regulation 1987/2006/EC and Council Decision 2007/533/JHA providing the legal framework for the operation of the Schengen Information System (SIS), the Commission carried out a wide-ranging and comprehensive evaluation of the system in 2016 three years after the entry into force of SIS II on 9 April 2013. The evaluation showed that SIS is indeed working successfully. The results of this assessment underlined that in order to appropriately respond to the new security and migration challenges, it is necessary to amend the legal basis of SIS. To that end, three new SIS regulations entered into force on 27 December 2018. Regulation (EU) 2018/1860 of the European Parliament and of the Council and Regulation (EU) 2018/1861 of the European Parliament and of the Council jointly regulate the legal basis of the establishment, operation and use of SIS. Regulation (EU) 2018/1862 of the European Parliament and of the Council on the use of the system for the return of illegally staying third-country nationals complements the regulation on the use of the system for border management purposes.

Act XLII of 2020 on the Amendment of Certain Acts concerning the Act on Information Exchange within the Schengen Information System was drafted in order to implement law harmonisation tasks stemming from the adoption of the regulations. Preparations for this were done by the working group set up with Government Decision 1538/2018. (X. 30.). The EES-ETIAS working group was responsible for coordinating Government measures necessary for the implementation of the national part of the Entry/Exit System (EES), the European Travel Information and Authorisation System (ETIAS), SIS and ECRIS-TCN (centralised system for the identification of Member States having information concerning judgments against third country nationals and stateless persons), as well as those needed for the implementation of the national part of the requirements in the European Union legal acts concerning the framework of interoperability between the information systems of the European Union. The president of the Authority is a permanent invited participant of this working group with the right of consultation.

The working group is continuously working on drafting legal regulations necessary for the national implementation of the interoperability of EES, ETIAS and ECRIS-TCN. The start of the live operation of the new systems is expected in the coming years.

VI. Supervision of secrets, classified data and data with restricted access

VI.1. Accessibility of data related to secret adoption

In one of the cases investigated by the Authority, the complainant was adopted by secret adoption in the 1970s and in 2020 he would have liked to learn who his biological parents were. Just because the adoption was secret, it does not at all follow that the relevant data should be protected by classifying them as "Secret!" or some other classification according to Act CLV of 2009 on the Protection of Classified Data (Classified Data Act). To have access to his personal data (names of his biological parents) the complainant turned to the organisational unit of the district government office dealing with guardianship cases. The district government office contacted the Hungarian National Archives (MNL) as MNL stores the documents generated in the 1970s including those related to adoptions in the county archives. The county archive found the relevant document, of which it was assumed that it contained the personal data indicated in the request; however, the document was marked "'Secret' For official use" at the time of its generation. Because of this, the complainant could not have access to its content.

At this point the complainant turned to the Authority to ask for its assistance to access his personal data related to his origin. The Authority launched an investigation and contacted the county archives and then, based on the information received from the archives, the minister in charge of the Prime Minister's Office as the legal successor of the classifier who may have had knowledge of the validity of the classification. The Authority investigated whether the conditions set forth in the Classified Data Act, which laid the foundations for the validity of the classification existed in the case of this document and whether a review of the classification was carried out, in the absence of which the document qualifies as open by force of the law. The Classified Data Act accurately specifies the conditions, in the absence of which the classification cannot be valid. Such a condition is, for instance, the indication of the name and position of the classifier and of the period of validity of the classification. In addition, the Classified Data Act requires the review of the classification of classified data generated earlier out of turn in several rounds. If the review was not carried out, the classification loses its validity by force of the law.

Finally, the minister in charge of the Prime Minister's Office informed the Authority that he established that the classification of the document lost its validity pursuant to Act LXV of 1995 on State Secrets and Service Secrets even before the entry into force of the Classified Data Act. So, the document became accessible in accordance with the provisions of Act LXVI of 1995 on Public Documents, Public Archives and the Protection of the Materials of Private Archives.

VI.2. Complaint to the Constitutional Court case No. IV/540/2019

The Constitutional Court invited the opinion of the Authority concerning a complaint to the Constitutional Court under Case No. IV/540/2019. The constitutional complaint called for the establishment of the anti-constitutionality and the annulment of Section 11(2) of Act CLV of 2009 on the Protection of Classified Data and Section 71/C(2) of Act CXXV of 1995 on National Security Services. According to the complaint, the Constitution Protection Office drafted a security opinion on the complainant in the course of its national security check and refused to allow the complainant to access the personal data processed in the opinion despite the complainant's request. The Constitution Protection Office based its decision on Section 11(2) of the Classified Data Act and Section 71/C(2) of the National Security Services Act, according to which the classifier shall refuse to issue the permit to access, if access to the data would lead to an infringement of the public interest serving as the basis of the classification and the national security service indicates the classified data, of which the person subject to the national security check may not be informed in the security opinion.

According to the justification of the constitutional complaint, the requirements of necessity and proportionality were violated, when the Constitution Protection Office refused access to his sensitive personal data unlawfully, unreasonably and disproportionately restricting the complainant's right to informational self-determination. The contested provisions do not contain the set of criteria that would limit the discretion of the person who classifies the access authorisation as to whether the disclosure of the data could lead to the harm of the public interest underlying the classification. In the absence of a set of criteria, the data subject cannot have access to his personal data and the right to legal remedy guaranteed in the Fundamental Law becomes empty because in the absence of knowledge it cannot be established whether the harm to the public interest underlying the classification of sensitive personal data concerning the data subject violates any of his rights or legitimate interests,.

The Authority regarded the constitutional complaint as unfounded. Section 5(1) of the Classified Data Act lists the public interests that may be protected

by classification item-by-item. The classifier is entitled to decide whether in the given case there was a public interest and whether the provisions concerning classification apply, i.e. whether the data should be classified within his own responsibilities and powers. Section 4(1) of the Classified Data Act lists the persons authorised to classify data. In every case a law or a government decree provides for the responsibilities and powers of the classifiers and within these responsibilities and powers classifiers must be able to assess whether the public interest named in the Classified Data Act exists or whether it is absent.

The Classified Data Act defines protectable public interest and when protection by classification is needed with adequate accuracy. The Authority believes it is not possible to stipulate a set of criteria more accurately than this in a legal regulation at law level; it would rather be the subject of legal publications and scientific dissertations. In the course of the implementation of the act, by virtue of his own public function, the classifier must be aware of the necessary criteria, which, in addition, are or can be different from one public body to another. The legal system guarantees legal remedy also in the case of the error or procedure in bad faith by the classifier as the head of a body discharging public power functions, in the course of which the lawfulness of the qualification may be examined. However, the complainant ab ovo was not looking for a legal remedy that would question the lawfulness of the classification based on the other documents submitted with the constitutional complaint, he only objected to the rejection of his request for a permit to access, but he did not really dispute the lawfulness of classification, at least his point of departure was not the unlawfulness of the classification, all he requested was to access his own data.

The Classified Data Act guarantees legal remedy against the decision of the classifier – in the present case against the decision rejecting the permit to access – in the form of administrative litigation. The complainant states that this legal remedy is in actual fact an empty right because the court cannot take a position with respect to the classification of personal data, all it can do is to examine the lawfulness of the decision of the Constitution Protection Office rejecting the request to access. The decision of the Supreme Court enclosed with the complaint reveals that the court truly does not examine the lawfulness of the classification of the data, but it does examine whether the restriction of the right to access was a result of a procedure stipulated by law and whether the restriction was necessary and proportionate to the purpose to be achieved.

In relation to this case, the Authority studied the constitutionality of the rules of the Classified Data Act applicable to the permit to access in a broader context. In the course of this, it found the following:

Section 2(1) of the Classified Data Act applies the principles of necessity and proportionality only to the restriction by classification of access to data in the public interest without mentioning the restriction by classification of the right to informational self-determination. At the level of basic principles, the necessity and proportionality of the restriction by classification of the right to informational self-determination is not implemented in the Classified Data Act. It, however, does not follow that the rules applicable to the restriction of the data subject's right to access by the permit to access in the Classified Data Act would violate the requirement stipulated in the Fundamental Law requiring necessity and proportionality with regard to the restriction of fundamental rights. The rules guaranteeing the enforcement of the necessity and proportionality of the restriction of fundamental rights may appear in the system of legal regulations not only as basic principles, but also as part of the substantive and procedural legal material of the permit to access.

At the same time, it can still be established that the regulation in force in Section 11(2) of the Classified Data Act fails to comply with the constitutional requirement concerning the proportionality of the restriction of fundamental rights because without the possibility of any consideration it categorically excludes access to the personal data by the data subject, if access to the data would lead to the infringement of the public interest on which the classification was based.

VII. International cases and social relations

VII.1. Review of the cooperative procedures conducted pursuant to GDPR

Since the application of GDPR beginning in 2018, the Authority has taken an active part in the cooperative procedures conducted according to Article 60 with the Member States of the EEA. The one-stop-shop procedure[27] is designed to investigate cases launched ex officio or on the basis of complaints related to cross-border processing.

Communication among the authorities in connection with cooperative procedures is conducted via an interface specifically transformed for these procedures within the Internal Market Information System (hereinafter: IMI system).

Prior to the cooperative procedures, the Authority in the Member State where the complaint against a controller pursuing cross-border processing is received (hereinafter: initiating authority) launches the procedure according to Article 56 within IMI to identify the lead supervisory authority and the supervisory authorities concerned.

The initiating authority may assume the lead supervisory authority based on the centre of operations or a single place of activity of the controller/processor[28], which authority may accept or reject this role with the appropriate justification.[29] In addition, the Member States in which the controller/processor does not have an centre of operation or place of activity may indicate themselves as authorities concerned, if the processing under investigation was likely to affect a large number of data subjects who are residents in their countries.

In 2020, the Authority received 784 cases from the authorities of other Member States through the IMI system and the Authority found itself concerned in roughly a quarter of them. The Authority acted as lead supervisory authority in 11 procedures and launched 15 procedures according Article 56 of its own during the same period.

Lead supervisory authorities investigate the complaint based on their own

27 GDPR Article 60

28 Based on GDPR Article 27 in the case of controllers or processors not having a place of activity in the European Union.

29 GDPR Article 56(3).

procedural rules and draft a decision in the given case. All the authorities concerned have an opportunity to state their opinion in the form of comments or relevant and well-founded objections to the draft decision within four weeks. If there are no objections to a draft decision, the lead supervisory authority sends the final version to all the Member State authorities as the binding decision.

If an authority concerns, submits a well-founded and relevant objection or amending motion to a draft decision, the lead supervisory authority may produce a revised draft decision based on the recommendations, which the authorities concerned may comment on again similarly to the earlier version over a four-week period. The lead supervisory authority may modify its draft decision as long as all the authorities concerned accept it, after which it can be sent to all the Member State authorities in the form of a binding decision.

In the event that a lead supervisory authority disagrees with the relevant and well-founded objections of the authorities concerned, it may request that the Board resolves the conflict and decide on the disputed issues through a dispute settlement procedure according to Article 65.

In 2020, the Authority received 86 draft decisions to be studied, 16 revised draft decisions and 97 binding decisions. In addition, the Authority received 98 informal consultations assisting the cooperation according to Article 60. During the same period, the Authority sent 7 draft decisions, 1 revised draft decision, and 5 binding decisions to the other authorities under the cooperative procedures.

In addition, mutual aid procedures according to Article 61 and voluntary mutual aid procedures are connected to the procedures according to Article 60. While the former is a procedure subject to stringent formal requirements to be conducted within a given period generally between two Member States, the latter is a more lenient procedure in terms of form and content, which the Member State authorities use inter alia for giving and obtaining information expressing interest in relation to investigative procedures and general consultation.

In 2020, the Authority participated in 4 mutual aid procedures and received 111 requests for voluntary mutual aid. During the same period, the Authority initiated 7 mutual aid procedures and 12 voluntary mutual aid procedures.

Although not closely related to the procedure according to Article 60, the opinions of the Board according to Article 64 should also be mentioned, of which the Authority received 34 in 2020.

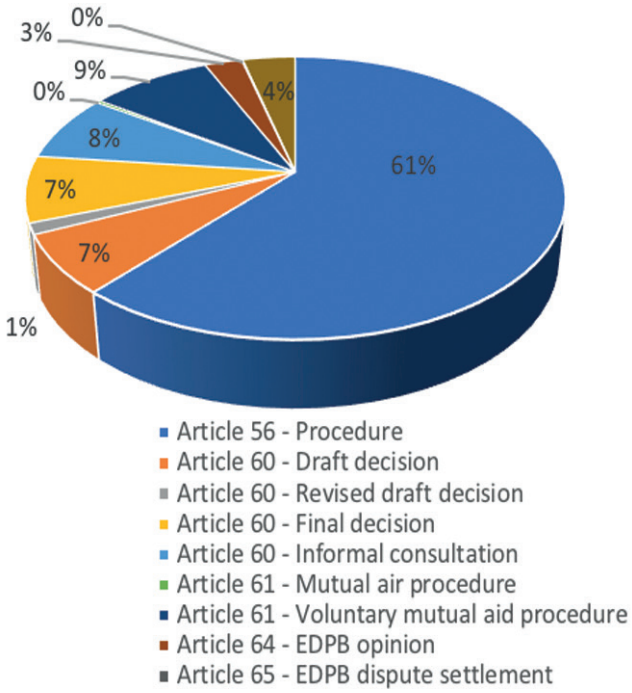
Beyond all this, the Authority received one binding decision following the Article 65 dispute settlement procedure of the Board in 2020.

The number of written procedures handled by the Authority in 2020 in relation to cooperation among the Member State authorities should also be stressed; these are votes cast in the IMI system to streamline the agenda of the plenary sessions of the Board. Although there was only one such procedure prior to 2020, the Authority participated in 48 such procedures in 2020, which is obviously a consequence of on-line operation forced by the pandemic.

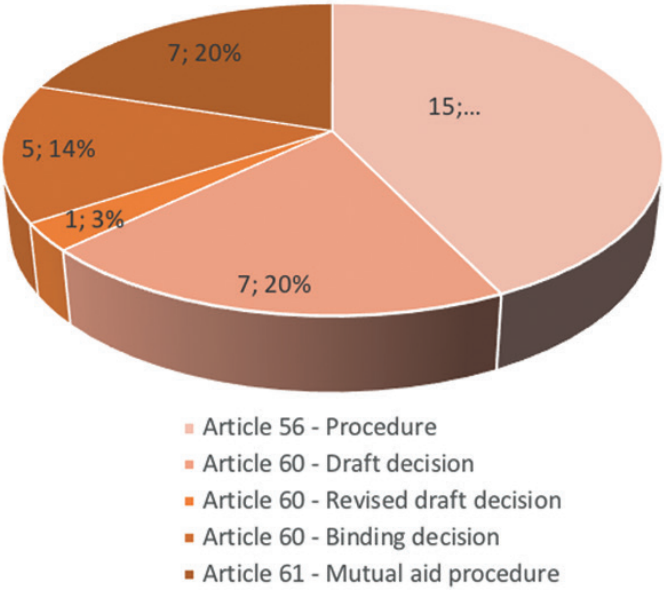
Based on the statistics since May 2018 when GDPR became applicable, it can be established that the cooperative procedures among the Member State authorities have been increasing both in terms of number and type year after year.

Cases in 2020:

Procedures received by NAIH through the IMI system in 2020



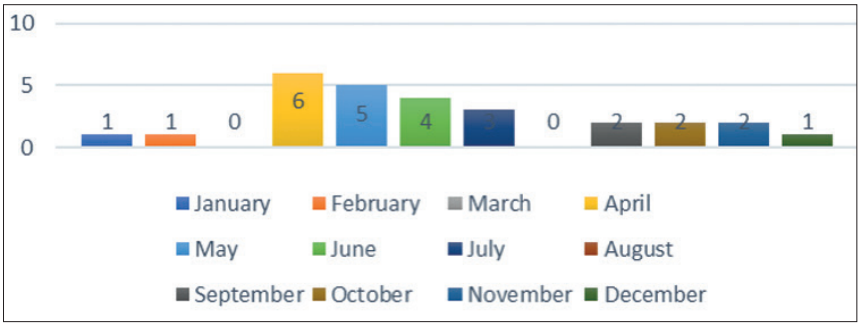
Procedures initiated by NAIH through the IMI systemin 2020



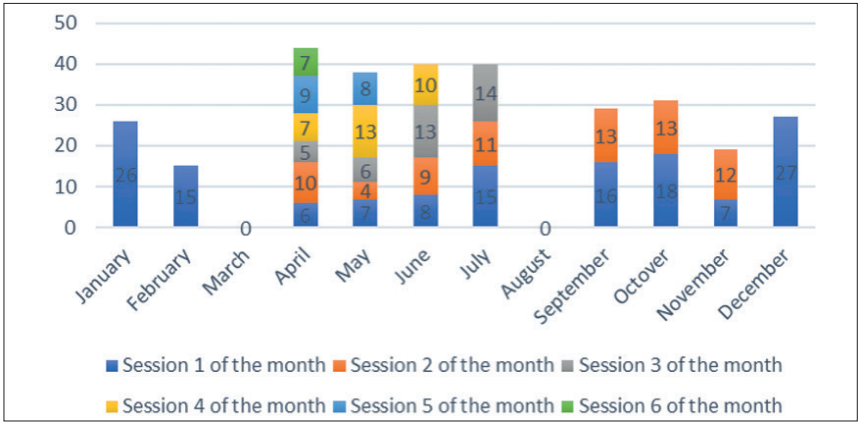
VII.2. NAIH's participation in the activities of the Board – sessions in 2020 – the operation of the European Data Protection Board in figures

Naturally, the pandemic had a direct impact on the operation of the European Data Protection Board. In 2020, the Board had altogether 27 sessions. This is an extraordinarily high number as it is two-and-a-half times more than usual. Of the 27 sessions held, two were still in person in Brussels, while twenty-five were organised as video conferences. Obviously, online sessions can be more flexibly organised, which was necessary in order that the Member State authorities confronting unexpected situations are able to regularly reconcile their positions. The European Data Protection Board discussed altogether 309 agenda items at its 27 sessions, which on average means 11.5 agenda items per session.

The number of EDPB session in a monthly breakdown



Number of Agenda items / month



VII.3. Guidelines and opinions of the Board, the activities of the expert subgroups

VII.3.1. Guidelines on connected vehicles

The Technology expert group drafted the text of the guidelines on connected vehicles[30], with which EDPB wished to call attention to the tendency seen in recent years that data-driven technologies and services developed significantly in the automotive industry. The car is increasingly becoming a general data centre, from which a lot of personal data flows outwards and inwards through various interfaces and communication channels.

An integral part of the idea is the collection and sharing of the personal data of the driver (e.g. routes and list of places visited, driving habits, but even the biometric data of the driver). From the viewpoint of data protection, the identification of the actors of this new system and the specification of their responsibilities are of particular importance. This mixed ecosystem includes not only car manufacturers, but also technology companies providing convenience solutions and driver assistance systems, and even public road infrastructure maintenance and operating companies. In addition to presenting this new world, the guidelines put forward recommendations as to how data protection criteria can be complied with and enforced in this new ecosystem.

VII.3.2. Guidelines on data processing in the context of the Covid-19 outbreak

The Compliance, eGovernment and Health (CEH) expert group of the European Data Protection Board drafted two guidelines with regard to the 2020 COVID-19 outbreak, which were adopted and published by the spring plenary session of EDPB. Guidelines 03/2020[31] focuses on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak, while guidelines 04/2020[32] deals with the use of location data and contact tracing tools in the context of the COVID-19 outbreak. The guidelines drafted in cooperation with the Technology expert group formulated recommendations

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

31 https://edpb.europa.eu/our-work-tools/our-documents/ohjeet/guidelines-032020-processing-data-concerning-health-purpose_en

32 https://edpb.europa.eu/our-work-tools/our-documents/ohjeet/guidelines-042020-use-location-data-and-contact-tracing-tools_en

concerning the contact tracing applications developed in the struggle against the coronavirus pandemic and the processing of the geolocation data used by them and clarified the conditions for using location personal data together with the data protection criteria to be taken into account.

VII.3.3. Guidelines on the management of data protection incidents

In the course of 2020, the Technology expert group drafted practice-oriented guidelines on examples regarding data-breach notification[33]. The guidelines present risk analyses for data protection incidents through practical legal case studies. The guidelines present the process of risk analysis through several case groups (e.g. ransomware attack incident caused by lost device, etc.). At the end of each chapter presenting a case group, there is a list of good practices including technical and organisational measures, which would have prevented the incident from happening or would have reduced its impact. Within each case group, the document illustrates through several fictitious legal cases, what special circumstances influence risk analyses in the case of the individual incident types. The only rapporteur of the guidelines was the Hungarian authority. EDPB adopted the guidelines on 19 January 2021, highlighting the work of the Hungarian authority.

VII.3.4. Guidelines on the targeting of social media users

The Social Media Expert Subgroup completed its work drafting the text of the guidelines on the targeting of social media users as envisaged in its 2020 work plan and submitted it to the Board for adoption. The guidelines[34] focuses on the processing of data in relation to the targeting of social media users. The Board adopted the guidelines under No. 08/2020 following a six-week period open for consultation. The public consultation ended on 19 October 2020, after which the expert group began the work on processing the observations received and on finalising the guidelines.

In addition, the expert subgroup began its work in 2020 on drafting guidelines on the front-end operation of social networks. Front-end is the layer of IT systems, that communicates with the user, i.e., what the user sees day after day on the display of his laptop or other smart device.

33 https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2021/guidelines-012021-examples-regarding-data-breach_en

34 https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-082020-targeting-social-media-users_en

VII.3.5. Guidelines on the restriction of data subjects' rights

The Key Provisions expert subgroup of the European Data Protection Board (hereinafter: KPESG) has an outstanding role in facilitating the uniform interpretation of GDPR. KPESG is responsible for the development of general guidelines to facilitate the uniform interpretation and application of the European data protection regulations, particularly GDPR and the data protection guidelines for criminal affairs. KPESG involves those applying the law and other experts in its work in the form of public consultations.

Guidelines 10/2020 on restrictions of data subjects' rights under Article 23 GDPR developed by KPESG and adopted by the Board should be highlighted. Subject to certain conditions Article 23 of the General Data Protection Regulation allows for national legislators to restrict the scope of the obligations of controllers and processors and the rights of the data subjects provided that such restrictions respect the essence of the fundamental rights and freedoms, and constitute necessary and proportionate measures to achieve some important purpose in the public interest of the European Union or a Member State, for instance the protection of public health in a democratic society. In relation to this document, the European Data Protection Board is mindful of the need to protect personal data even during the extraordinary times caused by the pandemic even when adopting emergency measures, thereby contributing to the respect of the overarching values of democracy, the rule of law and fundamental rights, on which the European Union is based. The guidelines, which were subject to public consultation for eight weeks, is accessible in the Board's website. [35]

VII.3.6. Guidelines for transfers of personal data between EEA and non-EEA public authorities and bodies

Guidelines 2/2020 on articles 46(2)(a) and 46(3)(b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies[36] was adopted early in the year on 18 February 2020. These Guidelines assist those public authorities and bodies, which intend to enter into agreements with third country addressees in order to establish guarantees for data transfer to third countries, be that an agreement of binding force or a provision inserted into an administrative agreement. The final version of the guidelines was adopted on 15 December 2020 after public consultations.

35 https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-102020-restrictions-under-article-23_en

36 https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22020-articles-46-2-and-46-3-b-regulation-2016679_en

VII.3.7. Recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

Following the Schrems II decision of the Court of Justice of the European Union of 16 July 2020, the drafting of Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data[37] took place within ITS, which was then adopted by the Board on 10 November 2020. In these recommendations, the Board clarifies the obligations of controllers and processors planning or carrying out data transfers to third countries in order to implement the provisions of the judgment referred to in practice. In addition, the annex to the recommendations contains a number of specific examples of additional measures that can be used to ensure and supplement the guarantees.

VII.3.8. Draft decision on the general data protection provisions applicable as safeguards in the event of data transfers to third countries

On 12 November 2020, the European Commission published its draft decision containing the general data protection provisions applicable as guarantees in the event of data transfers to third countries under Article 46(2)(c) GDPR, on which it also invited the opinion of the Board. The opinion[38] was also drafted within ITS towards the end of 2020, which was then published by the Board early in 2021 on 14 January 2021.

VII.3.9. Binding Corporate Rules

In the course of 2020, the ITS experts conducted consultations and exchanges of experience concerning the approval of Binding Corporate Rules (BCR) and other specific issues related to data transfers and began the review of the BCR-related work documents based on experiences to date and the points of the Schrems II judgment. In addition, a number of Board opinions on decisions of competent supervisory authorities concerning BCR approval were prepared within ITS during the year.

VII.3.10. Opinions concerning the accreditation criteria of bodies supervising codes of conduct and certification bodies

Another major task for the CEH expert group was to provide opinions on the set of

37 https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en

38 https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-22021-standard_en

criteria for the accreditation of bodies supervising codes of conduct to be issued by the various Member States' supervisory authorities. Pursuant to Article 64(1) (c) GDPR such a draft decision has to be adopted in a consistency mechanism. In 2020, the Board provided opinions on and adopted criteria compiled by the national supervisory authorities of altogether ten Member States (Belgium, Spain, France, Finland, Denmark, the Netherlands, Greece, Germany, Ireland and Italy). The opinions are available on the EDPB website.

Another task of the expert subgroup was to provide opinions on additional sets of criteria for the accreditation of certification bodies, the decision on which has to be adopted also in a consistency mechanism. In 2020, the Board provided opinions on and adopted sets of criteria compiled by the national supervisory authorities of altogether ten Member States (Austria, Denmark, the Netherlands, Greece, Italy, Ireland, Germany, the Czech Republic, the United Kingdom and Luxembourg). The opinions are available on the EDPB website.

Beyond these, the expert subgroup adopted internal guidelines for the procedure related to the European Data Protection Seal (Article 42(5) GDPR) and began work on guidelines concerning data protection issues of processing for scientific and research purposes.

VII.3.11. Guidelines concerning the processing of financial data

In 2020, a priority task of the Board's financial expert subgroup was to draft the guidelines on the links between Directive (EU) 2015/2366 on payment services in the internal market (PSD2) and GDPR, in view of the fact that following the transposition of PSD2 into Member State law, a number of issues arose in relation to data protection. PSD2 modernises the legal framework of the payment services market, inter alia by setting up the legal framework for services summarising account information or current account-based electronic payment solutions (online transfer services). PSD2 creates a possibility for service providers offering these new payment services to have access to the account management system of payment service providers and to the data stored in them upon request from the users.

The European Data Protection Board adopted the draft of the guidelines drafted by the expert subgroup at its plenary session on 17 July 2020, then it submitted it for public consultation. During the eight-week period of consultation EDPB received numerous comments from various stakeholders, most of which were private undertakings or associations, but recommendations were sent in by state authorities, natural persons and NGOs as well. The expert subgroup summarised

and assessed the feedback and then recommended a few amendments to the text of the guidelines. At its 43rd plenary session held on 16 December 2020; the Board adopted the finalised text of the guidelines[39].

The guidelines detail the conditions under which account managing payment service providers may grant access to information on the payment account to online transfer service providers and account information service providers. The guidelines clarify that PSD2 does not allow additional data processing, unless the data subject gave his consent, or processing is required by EU or Member State law. The guidelines also point out that in general the processing of special categories of personal data is prohibited under these conditions [in accordance with Article 9(1) GDPR], except if the data subject gave his express consent.

In May 2020, the European Commission adopted an action plan for a comprehensive Union policy on preventing money laundering and terrorism financing[40] and launched public consultation. The action plan refers to the intention of the Commission to invite the opinion of the European Data Protection Board on the data protection aspects. On 20 October 2020, the financial expert subgroup was mandated by the Board to draft a statement expressing the views and concerns of the Board with respect to the protection of personal data in the context of the action plan. In this statement[41] the Board expressed its desire to be associated with the drafting process of the new regulation and again called attention to the data protection challenges linked to the measures, in particular, the need to review the interaction between anti-money laundering measures and the right to privacy and the protection of data.

In addition to the above, the expert subgroup has been working on the preparation of recommendations concerning the online processing and storage of credit card data and is cooperating with the Technology expert subgroup in drafting comprehensive guidelines on blockchain and crypto currencies.

VII.3.12. Guidelines on the right to be forgotten

The Enforcement expert subgroup completed its preparatory work in 2020 on guidelines to facilitate the exercise of the right to be forgotten in relation to Internet search engines. The plenary session of the Board adopted the finalised version of

39 https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-062020-interplay-second-payment-services_en

40 https://ec.europa.eu/info/publications/200507-anti-money-laundering-terrorism-financing-action-plan_en

41 https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-protection-personal-data-processed-relation_en

the document in July 2020, which included the observations received in the course of the consultation process. The document analyses Article 17(1) GDPR cases of exercising the right to be forgotten (erasure) and the cases when a controller may claim exemption from the obligation to comply with a data subject's request to exercise this right (see Article 17 (3) GDPR). The document is accessible to the public in the Board's website.[42]

VII.3.13. The first dispute resolution by the Board

Ever since the beginning of the application of GDPR, the first dispute resolution procedure according to Article 65(1)(a) GDPR took place in 2020. This procedure applies when a draft decision in a case concerning the cross-border processing of personal data is the subject of a 'relevant and reasoned objection' by an authority concerned by the case against the draft decision submitted by the lead supervisory authority, but the lead authority does not agree with the decision and therefore requests the decision of the plenary session of the Board in the legal dispute. The subject matter of the first dispute resolution procedure was a draft decision of the Irish supervisory authority assessing the circumstances of a data protection incident related to the activities of the Twitter International Company based on the objection of the Hungarian supervisory authority in addition to other authorities. Decision 01/2020 of the EDPB plenary session brought in the course of the dispute resolution procedure, and the final decision of the Irish supervisory authority based on this decision are accessible to the public.[43]

Guidelines 09/2020 on the relevant and reasoned objection was adopted based on the mandate of the Board's plenary session with a view to settle the procedural issues arising in the course of the first dispute resolution procedure; this document is also accessible to the public in the Board's website.[44]

VII.3.14. Harmonisation work concerning the imposition of fines

In 2020, due to the epidemiological situation, the fines subgroup continued its activities to facilitate the alignment of the fining practice by the supervisory authorities through a reduced number of meetings held online compared to the previous calendar year . To this end, the expert group is currently working on a new draft document. The alignment of the steps determining fines, the possible modes of assessing the specific situation of micro-, small- and medium-sized enterprises, the interpretation of the notion of business undertaking with a view to

42 https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-52019-criteria-right-be-forgotten-search-engines_en

43 https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-decisions_en.

44 https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-092020-relevant-and-reasoned-objection_en

Recital (150) of GDPR and the interpretation of Article 83(3) GDPR were raised as the possible topics of this document.

VII.3.15. Recommendations concerning Article 36 of the Law Enforcement Directive

The Borders, Travel and Law Enforcement expert subgroup (BTLE) was mandated to draft the Recommendations concerning Article 36 of the Law Enforcement Directive[45]. It has become particularly important to examine the issue of data transfers on the basis of an adequacy decision especially in relation to the exit of the United Kingdom from the EU. The recommendations help in assessing the cases when law enforcement agencies of third countries may transfer personal data for non-law enforcement purposes (including processing for national security purposes), the cases when the law enforcement agencies of third countries may have access to data processed by the controllers and what is needed for the establishment of adequacy under the Law Enforcement Directive.

VII.3.16. Additional activity of the Borders, Travel and Law Enforcement expert subgroup

Requested by a Member of Parliament, a BTLE expert subgroup addressed the TFTP Agreement[46], and also responding to a question by another Member of Parliament, it assessed the findings related to the PNR Directive[47] reviewed by the Commission. The expert subgroup was mandated by the European Data Protection Board to draft guidelines concerning the face recognition systems used by law enforcement agencies; this work is currently in progress. The BTLE expert subgroup played an active role in the working group set up to examine the consequences of the Schrems II judgment in 2020. This expert subgroup worked on the opinion on the Second Additional Protocol to the Budapest Cybercrime Convention, which was adopted by EDPB early in 2021.

VII.3.17. Data protection officer network

The Data Protection Officer Network of the European Data Protection Board (DPO Network) held its inaugural session on 25 February 2020. The DPO Network got its first task from the plenary session of the Board in February 2020 to analyse

45 Transfers on the basis of an adequacy decision.

46 EU - US Terrorist Finance Tracking Programme (TFTP) Agreement.

47 DIRECTIVE (EU) 2016/681 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the use of Passenger Name Record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crimes.

the possible impact of the judgment of the European Court of Justice in case C-210/16 WirtschaftsakademieSchleswigHolstein on the Twitter use of EDPB and certain supervisory authorities. The Board adopted the analysis developed by the DPO Network during the year at its plenary session held on 2 February 2021. The additional planned tasks of the DPO Network include the development of joint training materials, the identification of data processing activities affecting several supervisory authorities and the discussion of positions related to the internal audit activities to be carried out by data protection officers.

VII.3.18. Shift to the online work order necessitated by the pandemic

In 2020, the most important task of the IT Users expert subgroup was to provide the background necessary for video conferences introduced in view of the pandemic situation and its customisation based on feedback received from the Member State authorities. This expert subgroup coordinated handling of the new procedures through the IMI system (e.g. written procedures), as well as the smooth procedural transition related to Brexit.

VII.4. Decisions on data protection by the Court of Justice of the European Union in 2020

VII.4.1. The Schrems II case

One of the most important international decisions of 2020 was the judgment of the Court of Justice of the European Union in case C311/18 Schrems II[48], in which the Court declared invalid Commission implementing decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC on the adequacy of the protection provided by the EU–U.S. privacy shield. Pursuant to this decision, personal data could be transferred to the United States of America in a manner not requiring the individual assessment of the adequate level of protection of personal data.

Under the General Data Protection Regulation, personal data may be transferred based on an adequacy decision of the European Commission or in its absence, if the controller or processor provides adequate guarantees, including rights and possibilities of legal remedy that the data subject can enforce.
In the case leading to the Schrems II judgment, Maximillian Schrems found it injurious that the United States does not provide adequate protection to the

48 http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=HU&mode=lst&dir=&occ=first&part=1&cid=1487478

personal data transferred to that country and requested the suspension or prohibition of the transfer of his personal data to the United States in the future, which was carried out by Facebook Ireland based on the general data protection provisions in the annex to the decision on the data protection shield.
As the Irish supervisory authority deemed that the handling of Schrems' complaint depends on the validity of Commission decision (EU) 2010/87 on standard contractual clauses for the transfer of personal data to processors established in third countries, and the Commission decision on the EU-U-S. data protection shield, it initiated a procedure before the Irish Supreme Court to request a preliminary ruling from the Court of Justice of the European Union.
In its request for a preliminary ruling, the Irish Court asked the Court of the European Union about the applicability of the General Data Protection Regulation to the transfer of personal data based on the general protection clauses in Decision 2010/87, the level of protection required by this regulation and in this context, the obligations of the supervisory authorities. The Irish Court also raised the issue of the validity of the Commission's decision on the general contractual clauses and on the data protection shield.
First and foremost, the Court of the European Union established that the General Data Protection Regulation is applicable to the transfer of personal data to business organisations established in third country, even if these data may be processed by the authorities of the third country concerned for purposes of national security, defence and public safety.
It also established that with regard to personal data transferred to third countries based on the general data protection provisions, a level of protection must be guaranteed, which is essentially identical with the level of protection provided in the EU by the General Data Protection Regulation interpreted in the light of the Charter. In relation to this, the Court declared that in the absence of a valid adequacy decision adopted by the Commission, certain data protection supervisory authorities have to suspend or prohibit the transfer of personal data to third countries, if they believe that the given country does not abide by the general data protection provisions or they cannot be respected there and the protection of the transferred data required by EU law cannot be guaranteed by other means.

In relation to the validity of the Commission's decision on the standard contractual clauses for data protection, the Court of the European Union established that the validity of the Decision is not called into question by the fact the standard data protection clauses do not bind the authorities of third countries because of their contractual nature. The decision under study contains efficient mechanisms, which enable compliance with the level of protection required by EU law in practice

and the suspension or prohibition of the transfer of personal data based on such clauses if the clauses are infringed, or compliance with them is impossible.

The Court of Justice of the European Union underlined in its judgment that in the absence of an adequacy decision, the controllers or processors established in the Union have to provide appropriate guarantees with which they can offset the data protection deficiencies in third countries. As the standard data protection clauses do not bind the authorities of third countries because of their contractual nature, supplementing them with additional vigorous guarantees may become necessary. Consequently, it is the responsibility of controllers and processors to cooperate in the given case with the addressee of the transfer to check case by case whether the laws of the destination third country provide adequate protection to personal data transferred on the basis of the standard data protection clauses by providing additional guarantees, if needed, over and above the guarantees provided by these clauses. Furthermore, if the controller and processor established in the EU cannot bring additional measures necessary to ensure such protection, the controller or, secondarily, the competent supervisory authority has to suspend or terminate the transfer of personal data to the third country concerned.

Upon review of the validity of the Commission's decision on the data protection shield, the Court of Justice of the European Union stated that this decision expressed the primacy of the requirements of national security, public interest and law enforcement, similarly to the decision on safe harbour. The primacy of these interests allow intervention into the fundamental rights of persons whose data are transferred from the EU to this third country. The internal regulations of the United States give rise to such restrictions on the protection of personal data, which allow American authorities to access personal data transferred from EU under surveillance programmes. The rules of the surveillance programmes are not enacted so as to comply with the requirement of the principle of proportionality under EU law as they are not restricted to what is absolutely necessary. It does not follow in any way from the regulation of certain surveillance programmes that there would be restrictions on the implementation of these programmes, nor that there would be guarantees for non-US persons.

In the context of the protection of rights by the courts, the Court of Justice of the European Union established that the ombudsman mechanism in the decision on the data protection shield does not provide an opportunity for legal remedy for data subjects in front of a body, which would provide guarantees essentially identical with the guarantees required by EU law. The Court also established that there was no special guarantee for the independence of the ombudsman from the executive power, and there were no provisions that would authorise the ombudsman to bring decisions binding for the American intelligence agencies.

For these reasons, the Court of Justice of the European Union established the invalidity of the data protection shield decision, i.e. that personal data shall not be transferred to the United States based on the adequacy decision.

The judgment also includes that the other instruments of outstanding importance for transferring data to the United States – the standard contractual clauses – continue to be valid and applicable, but such data transfer may not be automatic, the controller and the addressee of the data transfer must check the adequacy of the level of protection.

To supervise the implementation of the judgment, there are investigative procedures in front of the authority to establish whether controllers are aware of the judgment and whether they implement its provisions appropriately.

VII.4.2. The Orange Romania SA versus Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal case

From the viewpoint of the specification of the data protection requirements and practices for telecommunication service providers, it is important to mention the judgment of the Court of Justice of the European Union brought on 11 November 2020. In case C-61/19 the Court of Justice of the European Union stated that Articles 2(h) and 7(a) of Directive 95/46/EC and Articles 4(11) and 6(1)(a) of the General Data Protection Regulation shall be interpreted so that the controller is responsible for demonstrating that the data subject expressed his consent to the processing of his personal data by active conduct and he had received the information concerning all the circumstances of processing in a comprehensible, easy to access, clear and simple form in advance, enabling him to easily determine the consequences of his consent in such a way as to ensure that it was given in full knowledge of the facts.

A contract for the supply of telecommunication services with a provision, according to which the data subject was informed of the collection and storage of copies of

his identification documents containing personal data and he give his consent to that, is not suitable for demonstrating that such a person granted a valid consent for this collection and storage, if

- the box referring to that provision has been ticked by the data controller before the contract was signed, or

- the terms of the contract are capable of misleading the data subject as to the possibility of concluding the contract in question, even if he refuses to consent to the processing of his data, or

- the freedom to choose to object to that collection and storage is unduly affected by the controller in requiring that the data subject in order to refuse consent must complete the additional form setting out that refusal.

VII.4.3. The VQ versus Land Hessen case

In case C-272/19, the Court of Justice of the European Union interpreted the notion of controller and declared that Article 4(7) of the General Data Protection Regulation must be understood as meaning that insofar as the petitions committee of the Parliament of a federal state of a Member State determines, on its own or jointly with others, the purposes and means of the processing of personal data, the committee must be qualified as a "controller" within the meaning of that provision and consequently, the processing of personal data carried out by that committee falls within the scope of that regulation and in particular of Article 15 thereof.

VII.4.4. Privacy International versus Secretary of State for Foreign and Commonwealth Affairs and others case

A judgment brought in case C-623/17 is discussed in greater detail under "VII. 5. Participation in the joint supervisory activity of data protection authorities".

VII.5. Participation in the joint supervisory activity of data protection authorities

VII.5.1. Coordinated supervision committee

In 2019, the Coordinated Supervision Committee (CSC) was set up in order to jointly supervise the large information systems of the European Union. In 2020, CSC held two sessions, both as video conferences, in view of the virus situation.

At these sessions the Committee scheduled the tasks for the period 2020-2022. The data protection officer of Eurojust participated in both sessions as an invited guest, who also delivered a presentation to the members of the Committee. The colleague representing the Directorate General for Internal Market, Industry, Entrepreneurship and SMEs (DG GROW[49]) gave a presentation on the Internal Market Information System (IMI), detailing the legal background to the IMI system, its various areas, work flows, information on the distribution of access to the system and the levels of access authorisations. He discussed the basic principles along which the system was structured, the retention periods and the physical and administrative security measures introduced in relation to the IMI system. He also spoke about continuous, uninterrupted availability, vulnerability testing, incident management, the monitoring system and access logging.

One of the agenda items in the context of the Internal Market Information System was providing information to the data subjects. CSC intended to survey how information about data processing and data subjects' rights was implemented in the individual Member States in relation to the IMI system. The colleagues reported different experiences: in certain countries, providing information was the responsibility of the national IMI coordinator working at national level and controllers publish a joint general privacy statement, while elsewhere the individual controllers are responsible for providing appropriate information to data subjects. Most Member State authorities published the contact data of the IMI coordinator on their websites, or the appropriate link pointing to the national competent body/ person.

According to experience, the data protection supervision of the IMI system has not yet been built into the practice of the Member State authorities; CSC is developing a joint supervision plan for this, which requires, as a first step, an assessment of the resource needs by the Member State authorities. CSC contacted the data protection officer of Eurojust discussing issues related to cybercrime and their Counter Terrorism Register. The CSC meeting was also attended by a guest speaker from the European Union Agency for Fundamental Rights, who delivered a presentation on the issue of interoperability affecting the large information systems of the European Union. CSC plans to invite the data protection officer of the European Public Prosecutor Office (EPPO) to its session.

49 Directorate General – Internal Market, Industry, Entrepreneurship and SMEs.

VII.5.2. Working group supervising data protection in the Schengen Information System

The Supervision Coordination Group (SCG) functioning pursuant to Regulation (EC) 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) held two video conferences in 2020. In view of a drastic rise in the number of access request, the group sent a letter to the Albanian data protection commissioner requesting information about the reason why requests asking for information on the data stored in the Schengen Information System are received en masse from Albanian citizens by Member State data protection authorities.

At these meetings, the data protection officer of euLISA summarised the developments concerning the SIS II system in a short presentation as usual. Because of changes in legal regulations, SCG temporarily suspended its work began in relation to the alerts according to Article 24 of the SIS II Regulation[50] for an indeterminate period. It will be topical to to revisit the issue once the new legislative environment is in place. The communication from the Commission on a new Pact on Migration and Asylum was published on 23 September 2020. At the autumn session, staff members of the Commission reported on the Pact to SCG (a part of which is an improved Eurodac database) and its data protection aspects. Most of the questions from the members of the group to the Commission concerned the temporary suspension of the checks under the Schengen assessment mechanism and their relaunching. In view of the virus situation, the Scheval checks were temporarily suspended, thus the site visits planned for 2020 were postponed and remote checks were carried out.

Last year the number of requests related to data processed in SIS II evolved similarly to the preceding years. In 2020, data subjects contacted the Authority with regard to the processing of personal data stored in SIS II on 27 occasions. The majority of these requests was about an issue related to the exercise of data subjects' rights (request for information, erasure), in which cases the Authority provided general information concerning the right and process of turning to the SIRENE Office and about the available legal remedies.

50 Regulation (EC) 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 of stay.

VII.5.3. A The working group supervising data protection in the Visa Information System

The objective of the Visa Information System is to facilitate the implementation of the common visa policy, consular cooperation and consultations among the central visa authorities by way of the efficient identification of persons who failed to meet the conditions of entry to, stay or establishment in the territory of the Member States. For this reason the law enforcement authorities, the asylum authorities and Europol have access to the Visa Information System. The working group supervising data protection in the Visa Information System (VIS Supervision Coordination Group) held video conferences in 2020 instead of its usual meetings in Brussels.

The data protection officer of euLISA presented the statistical data to SCG on the use of the Visa Information System and explained that the 2020 security test was run on all three systems at the same time. Hungary participated in the security testing of SIS as an observer.

The working group is developing a joint audit plan taking the methods used to supervise the SIS II system as an example, which contains the Data Security Module, which is a questionnaire on data security in the Visa Information System, as well as the work schedule for conducting the coordinated on-site audits to be carried at the consulates and the External Service Providers (ESPs). With regard to the audit of External Service Providers, it has been suggested that in the case of ESPs contracted by ministries of foreign affairs or external representations of several Member States (most of the ESPs have such contracts), the Member State concerned could carry out coordinated audits.

NAIH developed a questionnaire for its audits conducted in 2019, which enabled it to carry out the data protection audit of several foreign representations at the same time. Upon request of VIS SCG members, the Hungarian authority sent the questionnaire referred to, together with the questionnaire used for auditing external service providers, to the EDPS Secretariat to share with SCG members, who are compelled to replace on-site audits with these questionnaire-based audits in view of the virus situation.

As to the Visa Information System, NAIH's 2020 audit plan included an on-site audit of the Hungarian consulate in Brasília, but the visit could not take place because of the pandemic. Finally, the Authority contacted the consulate with the questionnaire.

In 2020, the Authority received 8 requests in relation to the Visa Information System; in several cases, the data subjects wished to know more about the visa procedure. Typically, these requests were answered by way of providing general information.

VII.5.4. The working group supervising data protection in the Eurodac System

Member State sending data to the Eurodac system established with Regulation (EU) 603/2013 must ensure that fingerprinting and the operations related to the processing, transfer, storage or erasure of the data be lawful with a view to the protection of personal data. Processing by Eurodac is supervised by the European Data Protection Commissioner in cooperation with the national supervisory authorities. The working group supervising data protection by the Eurodac System (Eurodac Supervision Coordination Group, Eurodac SCG) held video conferences in 2020 similarly to the meetings of the SIS II and VIS SCG. At these meetings, the data protection officer of euLISA presented the statistical data and the most recent technical developments of the system, and shared the experiences collected from the reports of the Member States that participated in euLISA test with the group.

Similarly to the methods used for the audit of the SIS II system, the working group is developing a joint audit plan, which includes a questionnaire related to data security in the national Eurodac system, simplifying and harmonising the audit activities carried out by the Member State authorities.

A staff member of the Commission spoke of the planned joint database, which is part of the new migration and asylum pact[51]. He explained that the modernised Eurodac would help in following unlawful movements and the management of irregular migration. The improved database would enable the recording of individual applicants, ease relocation and better tracking of returned persons. The new system would help to establish the connection necessary between asylum and return procedures and provide additional support to those national authorities in charge of asylum applicants, whose applications had already been rejected by another Member State. As part of a comprehensive and integrated migration and border administration system, the new Eurodac would be fully interoperable with the border administration databases.

51 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a new pact on migration and asylum. 2020.09.23., COM (2020) 609 final.

The European Union Agency for Fundamental Rights and Eurodac SCG finalised their joint publication designed to assist authorities sending fingerprints to the Eurodac system in 2020. The Secretariat sent a leaflet presenting the mode and content of providing appropriate information to data subjects in English, in an editable format, so that each Member State can translate it to their own language and publish it on their websites. The Authority published the document in Hungarian and English on its website.

VII.5.5. Cooperation board auditing data processing by Europol

Europol provides assistance to the work of the Member State law enforcement authorities in combating international organised crime and terrorism by collecting, analysing and sharing data and coordination. The task of the Board supporting the audit role (Europol Cooperation Board, ECB) is to assist in this work with consulting.

At ECB's sessions this year, a colleague from Europol reported on the situation of Europol and its recent activities, from a data protection viewpoint, which revealed that there is increasing demand on the part of the Member States for Europol to take more initiatives and act more directly. The financial field takes an increasing role in its activities, for instance in the course of the investigation of the Maltese corruption (political) crimes. Europol closely cooperates with third countries, such as the United States, Canada, Australia and Norway. No new cooperation agreements were concluded with third countries lately, but negotiations on possible cooperation with other countries, such as New Zealand, is ongoing.

ECB regularly discusses the topical issues related to the operation of SIENA, a network enabling secure exchange of information among the Member States' law enforcement authorities and the status of the introduction of the European Tracking Solution (ETS). As to the latter, it was a significant development that Austria, Germany, Finland and Sweden executed the agreement and they are already using ETS.

VII.5.6. Judgment of the Court of Justice of the European Union: the Privacy International case

The Court of Justice of the European Union brought its judgment in case C-623/17, Privacy International versus Secretary of State for Foreign and Commonwealth Affairs and others (Privacy International case[52]). In its judgment,

52 http://curia.europa.eu/juris/document/document.jsf?text=&docid=232083&pageIndex=0&doclang=HU&mode=lst&dir=&occ=first&part=1&cid=1491557

the Court compared the E-Privacy Directive with the national legislation of the Member States concerned in the case (France, Belgium and the United Kingdom) applicable to the traffic and location data to be collected by electronic communication service providers. National regulations, which require electronic communication service providers to transfer or retain traffic and location data in general without any distinction for the purpose of combating crime or to protect national security in general, is contrary to EU law.

If a Member State is confronted with a real and direct or unforeseeable, severe national security threat it may deviate from its obligation to ensure the confidentiality of data related to electronic communication by taking legislative measures to require the retention of such data restricted to the strictly necessary period – which may be extended in the event that the threat is lasting – in general and without distinction. To combat severe crime and severe threats affecting public security, a Member State may provide for the targeted or extraordinary retention of the data referred to. Such an interference with fundamental rights must be accompanies with effective safeguards to be supervised by an independent court or authority. Similarly, a Member State may also require the general retention of IP addresses assigned to the source of communication without distinction, provided that the retention period is restricted to the strictly necessary extent and as well as the general retention of data concerning the identity of the users of electronic telecommunications devices without distinction, in the latter case without indicating a separate retention period.

Obviously, this judgement of the Court of Justice of the European Union may have a serious impact on the way Member States apply the law and the way electronic communication service providers collect data, however its details and accurate consequences could not be fully assessed at the time of drafting this report.

VII.6. Results of the Schengen data protection audit of Hungary

On 7 October 2013, the Council adopted its Regulation (EU) 1053/2013 establishing an evaluation and monitoring mechanism to verify the application of the Schengen acquis. In accordance with the Regulation, the Commission drafted its multi-year evaluation programme for the period 2014-2019 and its annual evaluation programme for 2019, detailing the on-site visits to the Member States to be evaluated, the areas to be evaluated and the sites to be visited. The areas to be evaluated extend to all the aspects of the Schengen acquis, namely the following: administration of the external borders, visa policy, the Schengen Information System, data protection, police cooperation, judicial cooperation in criminal matters and the termination of internal border controls. Beyond these, all

the evaluations extend to issues of fundamental rights, as well as the operation of the authorities applying the relevant parts of the Schengen acquis.

Based on the multi-annual and the annual programme, a group consisting of Member State and Commission experts evaluated the application of the data protection requirements by Hungary between 6 and 11 October 2019. The group's assessment report completed in 2020 includes the expert findings and assessments, including the proven methods and deficiencies identified in the course of the evaluation. Simultaneously with the report, the group formulated recommendations with respect to the corrective measures to be taken to deal with the deficiencies. These are reflected in the Council's implementation decision concerning the recommendations for Hungary aimed at the elimination of the deficiencies explored in the course of the 2019 evaluation of the application of the Schengen acquis in data protection, which was discussed by the Working Party for Schengen Matters at its session of 15 December 2020. In addition to the recommendations, the decision also includes good practices. In terms of implementation, neither recommendation enjoys priority. Pursuant to Article 16(8) of Regulation (EU) 1053/2013, Hungary has to submit its evaluation of the possible development projects and the description of the necessary measures to the Commission within six months from the adoption of the decision (at the latest in the summer of 2021).

VII.7. Application of the Tromsø Convention

The Council of Europe Convention on access to official documents entered into force on 1 December 2020. The Tromsø Convention is discussed in detail in the Chapter "Freedom of information".

VIII. Projects by NAIH

VIII.1. The STAR project

Project 769138: STAR *(Supporting Training Activities on the Data Protection Reform)* ran under the auspices of the Rights, Equality and Citizenship Programme 2014-2020 (REC-RDAT-TRAI-AG-2016) co-financed by the European Union with the participation of NAIH, the LSTS research team of Vrije University of Brussels and the Irish office of Trilateral Research, a research and development company, between 1 November 2017 and 31 October 2019. The project compiled new GDPR training materials for data protection authorities and other stakeholders expressly appropriate to the needs and challenges of the given sector in a way that could easily be adapted. The training materials focus on the challenges of GDPR, including the rectification of faulty interpretations and misunderstandings and the reflection of the needs of different audiences. The STAR Consortium published these material based on a "creative commons" licence (which means that the slides may be used free of charge and can be transformed as needed) in the form of a PowerPoint presentation in English (www.project-star.eu/training-materials) and on NAIH website in Hungarian (https://naih.hu/star-i/stari-eredmenyek) on the following 11 topics:

- Introduction to the European Union data protection regime
- Purposes and legal bases of processing personal data
- Data subjects' rights and their exercise
- The responsibilities of data controllers and processors
- The data protection officer
- The data protection authority
- Technical and organisational measures
- Risk-based approach
- Data protection impact study
- Data protection communication
- European Union data protection network

The individual training modules provide additional guidance to trainers about the methodology to be applied, include links to additional supplementary materials and sources and give guidance concerning the adjustment of the slide series to the needs of any given audience. To support the use of the training materials, the project produced other accessory materials assisting in the administration of training projects, such as the attendance register, or the evaluation sheet. In addition, a training manual was also developed[53], providing guidance to the use of the STAR training materials, including a list for the quality assessment of other GDPR trainings.

VIII.2. The STAR II project

Project 814775 STAR II *("SupporT small And medium enterprises on the data protection Reform II")* ran under the auspices of the Rights, Equality and Citizenship Programme 2014-2020 (REC-RDAT-TRAI-AG-2017) co-financed by the European Union between 1 August 2018 and 31 December 2020. The project was managed by NAIH with the participation of the LSTS research team of Vrije University of Brussels and the Irish office of Trilateral Research, a research and development company. The project provides support in the development of appropriate data protection practices and facilitates the consistent application of GDPR, cross-border cooperation and the spreading of best practices among the Member States taking the structure and needs of small and medium-sized enterprises into account.

Under the project between 15 March 2019 and 15 March 2020, NAIH operated a dedicated information hotline and answered the targeted questions of SMEs. Altogether 252 questions were received, most of them in relation to the GDPR compliance of specific data processing activities, followed by questions concerning the rules of video and sound recording, the processing of the personal data of employees, data subjects' rights, the legal basis of processing, data processing records, the scope of GDPR and the need for data processing rules.

Having analysed the experiences of the hotline, as well as the interviews and online questionnaires with the representatives of various data protection authorities, associations of SMEs and the SMEs themselves, we compiled a much-needed manual for SMEs entitled "GDPR simply for small and medium-sized enterprises", which is accessible in a wide range and can be used all over the European Union. Every chapter of this publication includes practical examples, recommendations and additional useful sources. The topics in the guidelines were determined

53 https://naih.hu/star-i/stari-eredmenyek

based on the issues of greatest concern for SMEs as identified under the project. In addition, we developed guidelines[54] for data protection authorities to assist their communication with SMEs.

On 26 November 2020, the Authority organised an online conference for Hungarian SMEs, where in addition to presenting the manual, several presentations were delivered containing a great deal of practical information[55]. From December 2020, the manual can be downloaded online from the website of the Authority[56] free of charge, and in January 2021 NAIH makes available 700 copies printed in Hungarian to the interested entities with the help of the Hungarian Chamber of Commerce and Industry. The manual was also presented at an electronic conference organised for data protection officers (and the public) in December 2020.

VIII.3. The Public Administration and Civil Service Development Operative Program (KÖFOP)

The project entitled "*Review of the range of data subject to disclosure obligation stipulated in legal regulation*" was approved by the amendment to Government Decision 1004/2016. (I. 18.) on the determination of the annual development budget of the Public Administration and Civil Service Development Operative Program at the end of 2018. As a beneficiary specified in the Government decision, NAIH submitted a grant application for the implementation of a priority project entitled "*Mapping out the Hungarian practice of the freedom of information and the improvement of its efficiency*" in August 2019. The grant contract concluded with the Managing Authority responsible for the administration of the Public Administration and Civil Service Development Operative Program entered into force on 24 September 2020, actual work on the project, however, could only begin in January 2021 because of the administrative obligations.[57]

VIII.4. The Integrated Legislative System (IJR) Project

The IJR Project is a NAIH project supporting its preparation for the application of the General Data Protection Regulation and the implementation of its specialised tasks.

The Integrated Legislative System (IJR) project came into being among the

54 https://naih.hu/star-ii/starii-eredmenyek/kkv-kezikonyv-es-dpa-guidance
55 https://www.naih.hu/star-ii/starii-eredmenyek/star-ii-zarokonferencia
56 https://www.naih.hu/projekt/344-starii-kkv-kezikonyv
57 Additional information: https://naih.hu/kofop-2-2-6-vekop-18-2019-00001

projects designed to reduce the administrative burden on budgetary agencies financed on the basis of Government Decision 1004/2016. (I.18.) under the KÖFOP 1.0.0. – VEKOP-15 priority government project.

NAIH's further development in terms of its procedures, administrative management, information technology and information security adapted to changes in legal regulations arising from its EU obligations is implemented under this project in 2019-2020.

Pursuant to Government Decision 1585/2016. (X. 25.), Amendment 1 to the grant contract of the IJR project was signed in April 2017, which lists the Authority among the consortium partners, as well as the supported tasks arising from GDPR under the project.

Meeting the requirements of GDPR called for a full-scale optimisation and redesign of NAIH's legal and professional fields and their implementation in 2019, as well as the development of an IT environment supporting the redesigned processes together with their operation, while ensuring its flexible re-planning. The implementation of these tasks continued in 2020.

The IRMA file management system was installed and its roll-out and integration into the administrative module under the IJR project was carried out in 2020.

The 2019-2020, the deliverables of the IJR project include the administrative and the decision-editing modules, whose roll-out and organisational implementation are in progress. The leader of the consortium (Ministry of Justice) initiated that the KÖFOP Managing Authority extend the implementation period of the project until 31.08.2021.

VIII.5. EKOP Project

Our first project, identified as EKOP-1.1.7-2012-2013-0001, ensuring the fundamental operation of the Authority arrived at the end of its maintenance period on 08.12.2020.

A successful final on-site audit on 11 December 2020 completed a complex IT infrastructure and IT solutions project that laid the foundations for the Authority's operations from 2013 to 2015, the deliverables of which will serve the Authority's efficient operation for many years to come.

IX. Annexes

IX.1. The financial management of the Authority in 2020

We have passed the 9th year of the operation and financial management of the Hungarian National Authority for Data Protection and Freedom of Information as at 31 December 2020. Below, we provide a brief presentation of the data related to its financial management.

IX.1.1. Revenue estimates and their performance data in 2020

Of the revenue figures, the Authority's operating revenue does not show any significant change in its composition compared to the 2019 financial year, but all the more so in terms of value. Because of the COVID-19 pandemic, the expenditures of missions abroad and reimbursements arising therefrom had an impact only on the first quarter of the budget.

The Authority's non-operating revenues arose from the sale of three official vehicles.

It is important to note that the Authority participated in three EU projects in 2020: an advance of HUF 64,878,000 on the grant was disbursed following the acceptance of the KÖFOP grant application to cover expenditures; the Authority drew down an additional HUF 7,441,000 to close the STAR I and STAR II projects under its grant contracts.

Converting the residual budget fund rolled over from 2019 into a revenue estimate increased the original revenue estimate by HUF 137,542,000.

Act CVII of 2019 on the Agencies of Special Legal Standing and the Legal Standing of their Employees (hereinafter: Special Legal Standing Act) entered into force 1 January 2020 whereby the agencies concerned were able to carry out a general wage increase. The Authority requested HUF 276,728,000 to support wages from the Ministry of Finance.

IX.1.2. Expenditure estimates and their performance data in 2020

Payments to personnel increased by 36% over last year, in line with the extent of the wage support discussed above, while expenditure on related employer's contributions exceeded last year's figure by no more than 18%. This can be

explained by the most recent reduction in the rate of the welfare contribution tax and in some cases (e.g. cafeteria) by waiving the tax liability.

In 2020, two factors had real significance for the budget of the Authority: the pandemic and the relocation of the Authority to a new building. A former resulted in savings on costs, while the latter resulted in substantial additional expenditure as revealed by the operating and non-operating expenditures of the Authority.

The costs of relocation and the expenditure related to the operation of the new building exceeded the figures for the previous year by close to 72%. The same applies to the non-operating expenditures, where the expenditures of the Authority doubled because of the procurement of office furniture.

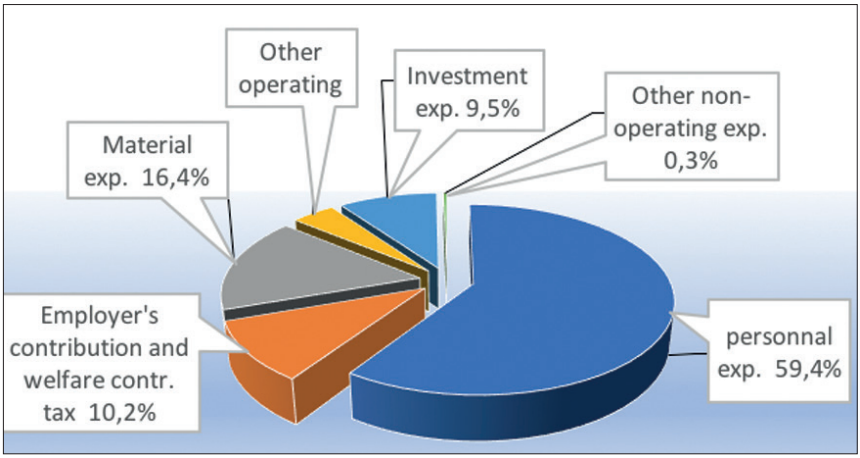
Residual funds rolled over from the Authority's budget in 2020, related to its basic activities, amounted to HUF 329,314,000, 74% of which is subject to liabilities.

The following table presents the figures for NAIH'S 2020 budget (in HUF '000):

Description	Original estimate	Amended estimate	Performance	2020 residue from basic activity
Original estimate	1,156,700			
Other operating support from a chapter (KÖFOP)		64,878	64,878	
Public revenue		393	393	
VAT invoiced		27	27	
Exchange rate gain		2,266	2,266	
Damages paid by insurer		285	285	
Other operating revenues		4,522	4,522	
Sale of tangible assets		8,614	8,614	
Other funds received for operating purposes (STAR I and II)		7,442	7,442	
Recovery of loan for non-operating purposes		504	504	
Residual funds from the 2019 budget		137,542	137,542	
Grant from central budget from Managing Authority	1,464,400	1,741,128	1,741,128	
of this: Wage support according to Special Legal Standing Act		*276,728*	*276,728*	
Revenue estimates total:	***1,464,400***	***1,967,601***	***1,967,601***	-
Estimates for payments to personnel	726,300	1,016,198	973,195	43,003
Employer's contribution and welfare contribution tax	126,300	175,217	167,110	8,107
Estimate for material expenses	456,400	511,660	268,187	243,473
Other operating expenses		68,732	68,732	-
Investment expenditure	155,400	165,794	156,063	9,731
Other non-operating expenditure		30,000	5,000	25,000
Expenditure estimate total:	***1,464,400***	***1,967,601***	***1,638,287***	***329,314***

The following graph shows the actual expenditures of the modified estimates in a percentage breakdown:

Breakdown of actual expenditure estimates



IX.1.3. Changes in the headcount of the Authority

As of 31 December 2020, the Authority's headcount according to labour law was 106.

Headcount management is based on the jobs according to the Special Legal Standing Act: The Authority has five administrative (councillor, lead councillor, senior councillor I, senior councillor II, head senior councillor), and two managerial (one heading an independent organisational unit and one heading a non-independent organisational unit) positions. According to the new regulation, the head of an agency of special legal standing is authorised to categorise jobs taking into account the categories specified in the Special Legal Standing Act and the budget, which was done by issuing presidential instruction 7/2020. (IV. 01.). On that basis the amendments to the appointments were issued to the employees as of 1 May.

In September 2020, the Authority moved to a new office building (1055 Budapest, Falk Miksa utca 9-11.), providing appropriate accommodation for the employees.

By providing salaries regarded as competitive and creating new, decent working conditions, NAIH has successfully reduced the extent of labour fluctuation and thus retaining highly qualified professionals.

IX.1.4. Changes in revenues from *fines*

In 2020, HUF 256,411,000 was credited to the account of the Authority as fines, which was close to 1.5 times the amount for 2019. It should, however, be noted that the fine is not entirely a revenue for the Authority, bur for the central budget.

IX.2. Participation of the President of the Authority in Hungarian and international conferences and events of the profession in 2020

8 January 2020, Zamárdi – Presentation for students participating in the Hungarian Public Administration Scholarship Programme organised by the Public Administration Scholarship Programmes of the Prime Minister's Office and the Department of Education for Government Offices – **Basics of information security and data protection**

15 January 2020, Zagreb **–** Data Protection Day 2020: Facing New Challenges – international conference

28 January 2020, Budapest – GDPR Breakfast organised by Ernst & Young Tanácsadó Kft. – **Experiences of the Authority**

27 February 2020, Budapest – "Impact of the use of artificial intelligence on fundamental rights" conference organised by the Information Society Research Institute of the University of Public Service, the Constitutional Court and the Hungarian National Authority for Data Protection and Freedom of Information – **Algorithms and data protection: Quo vadis?**

10 March 2020, Balatonakarattya – Hungarian Army Data Protection Conference – **2019: The first full year from the viewpoint of the Authority**

29 September 2020, Budapest – "*The impact of the Internet on children and the young"* international Internet conference organised by the International Children's Safety Service - **NAIH's practice in data protection cases affecting children**

25 September 2020, Zagreb – International online scientific conference: *"Workplace Whistleblower Protection in the V4 countries, France and Slovenia – in Search of an Effective Model of Protection"*

2 October 2020, Budapest – *think. BDPST – Connect to the Future* strategic conference organised by the Antall József Knowledge Centre – Data Protection in the Post-COVID Era **panel discussion**

4 November 2020, Budapest – "*Pandemic challenges – digital answers*" scientific online conference organised the by Belügyi Tudományos Tanács [Scientific Council for Home Affairs] – **Data protection of aspects of artificial intelligence**

23 November 2020, Budapest – "*The great challenge of the digital era: the human being who is (large) data set*" mini-conference organised by the Hungarian Representation of the European Commission - **round-table discussion**

IX.3. List of legal regulations and abbreviations mentioned in the report

- Fundamental Law, Hungary's Fundamental Law (25 April 2011)
- General Data Protection Regulation: see: GDPR
- Taxation Act, Act CL of 2017 on the Order of Taxation
- Act LXIII of 1992 on the Protection of Personal Data and the Accessibility of Data in the Public Interest
- Administrative Procedures Act, Act CL of 2016 on General Administrative Procedures
- Penal Code, Act C of 2012 on the Penal Code
- 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 Counsel Framework Decision 2008/977/JHA
- Act CCXL of 2013 on the Implementation of Sentences, Measures, Certain Coercive Measures and Retention of Misdemeanours
- CSC: Coordinated Supervision Committee (carrying out joint supervision of the large information systems of the European Union)
- ECB: Europol Cooperation Board
- ETS: European Tracking Solution
- CJEU: Court of Justice of the European Union
- Health Data Act, Act XLVII of 1997 on the Processing and Protection of Health and Related Personal Data
- GDPR, General Data Protection Regulation: Regulation 2016/679 of the European Parliament and of the Council 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. Applicable from 25 May 2018
- IMI system: Internal Market Information System
- Privacy Act, Act CXII of 2011 on the Right of Informational Self-Determination and the Freedom of Information
- KAFIR: Automated Processing Information System for Traffic Security
- Act LXIII of 1999 on the Supervision of Public Areas
- KNBSZ: Military National Security Service
- KSZDR: Governmental Personnel Decision Support System
- Act CXCIX of 2011 on Civil Servants
- Act on Government Administration, Act CXXV of 2018 on Government Administration

- Cost Decree, Government Decree 301/2016. (IX. 30.) on the extent of cost reimbursement that may be determined for compliance with request for data in the public interest
- Special Legal Standing Act, Act CVII of 2019 on the Agencies of Special Legal Standing and the Legal Standing of their Employees
- Act LIII of 1995 on the General Rules of the Protection of the Environment
- Classified Data Act, Act CLV of 2009 on the Protection of Classified Data
- MNL: Magyar Nemzeti Levéltár
- Municipalities Act, Act CLXXXIX of 2011 on Hungary's Municipalities
- Labour Code, Act I of 2012 on the Labour Code
- NAVÜ: Nemzeti Adatvagyon Ügynökség
- National Security Services Act, Act CXXV of 1995 on National Security Services
- Act CLXXIX of 2011 on the Rights of Ethnic Minorities
- Civil Code, Act V of 2013 on the Civil Code (new)
- Civil Code, Act IV of 1952 on the Civil Code (old)
- SCG: The Supervision Coordination Group functioning pursuant to Regulation (EC) 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)
- SIENA: a network enabling secure exchange of information among the Member States' law enforcement authorities
- SIS: Schengen Information System
- SIS II, Regulation (EC) 1987/2006 of the European Parliament and of the Council on the establishment, operation and use of the second generation Schengen Information System
- Act CLXXXI of 2012 on the Information Exchange under the Second Generation of the Schengen Information System and the amendment of certain acts on policing and the Hungarian Simplification Programme
- Act III of 1993 on Social Administration and Welfare Benefits
- Act CXXXIII of 2003 on Condominiums
- Act LIII of 1994 on Court Distraint
- 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
- Ministry of Justice Decree 1/2002. (I.17.) on the administration of court distraint and the management of funds

Other legal regulations:

- Ministry of Justice Decree 1/2002. (I.17.) on the administration of court distraint and the management of funds
- Act CLXI of 2011 on the Organisation and Administration of the Courts
- Commission delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third country operators of unmanned aircraft systems
- Commission implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft
- Act XC of 2017 on Criminal Procedure
- MvM instruction 3/2020. (II. 28.) on the organisational and operational rules of the Budapest and county government offices)
- Act CXXXI of 2010 on the Participation of Society in the Preparation of Legal Regulations
- Government Decision 71/2020. (III.27.) on curfew
- Government Decree 521/2020. (XI. 25.) on derogation from certain data request provisions related to requests for data in the public interest
- Government Decision 1585/2016. (X. 25.) on the amendment of Government Decision 1004/2016. (I. 18.) on the determination of the annual development budget of the Public Administration and Civil Service Development Operative Programme
- Act LXVI of 1995 on Public Documents, Public Archives and the Protection of the Materials of Private Archives
- Act LXXVIII of 1993 on Certain Rules concerning the Renting Flats and Premises and their Sale
- Act CLXXIX of 2020 on the amendment of certain acts related to the operation of unmanned aircraft
- Act XLII of 2020 on the Information Exchange under the Second Generation of the Schengen Information System and the amendment of certain policing related acts related to this and to the Magyary Simplification Programme
- Act II of 2012 on Misdemeanours, Misdemeanour Proceedings and Registration System of Misdemeanours
- Council Regulation (EU) 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
- Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the Second Generation Schengen Information System (SIS II)

- Government Decree 179/2020. (V. 4.) on deviation from certain data protection and data request provisions during the emergency
- Government Decree 40/2020. (III.11.) on the announcement of an emergency
- Government Decree 478/2020. (XI.3.) on the announcement of an emergency
- Commission implementing decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU–U.S. privacy shield
- Act XXXI of 1989 on the Amendment of the Constitution
- Act CLII of 2007 on Certain Obligations to Make Statements of Assets
- Government Decree 46/2020. (III.16.) on the prevention of an epidemic causing en mass sickness endangering life and security and the prevention of its consequences and the measures to be taken in the course of the emergency ordered with a view to protecting the health and life of Hungarian citizens
- Regulation (EC) 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)
- Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency and amending Regulations (EC) 2111/2005, (EC) 1008/2008, (EU) 996/2010, (EU) 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council and repealing Regulation (EC) and 552/2004 and (EC) 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) 3922/91
- Regulation (EU) 2018/1860 of the European Parliament and of the Council of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third country nationals
- Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks and amending the Convention implementing the Schengen Agreement and amending and repealing Regulation (EC) 1987/2006
- Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters amending and repealing Council Decision 2007/533/JHA and repealing Regulation (EC) 1986/2006 of the European Parliament and of the Council, and Commission Decision 2010/261/EU
- Regulation (EU) 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of “Eurodac” for the comparison of finger-

prints for the effective application of Regulation (EU) 604/2013 establishing the criteria and mechanisms for determining the Member States 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 request for the comparison with Eurodac data by Member States law enforcement authorities and Europol for law enforcement purposes and amending Regulation (EU) 1077/2011 establishing a European agency for the operational management or large-scale IT systems in the area of freedom, security and justice

- Act CXLI of 1997 on the Land Registry

Government Decree 388/2017. (XII. 13.) on the National Statistical Data Capture Programme,

- Act LIV of 2018 on the Protection of Trade Secrets
- Church Act, Act CCVI of 2011 on the Freedom of Conscience and Religion and on the Legal Standing of Churches, Religious Denominations and Religious Communities
- Tromsø Convention, Council of Europe Convention on access to official documents (CETS No. 205., promulgated in Hungary by Act CXXXI of 2009)

Table of Contents

Introduction 3
I. Statistical data on the operation of the Authority 5
I.1. Statistical characteristics of our cases 5
I.2. Annual conference of data protection officers 14
I.2.1. The results of the preliminary questionnaire survey 15
I.2.2. Electronic training materials of the conference for data protection officers 20
I.3. Media appearances of the Hungarian National Authority for Data Protection and Freedom of Information 22
II. Application of the General Data Protection Regulation 23
II.1. Data protection cases 23
II.1.1. The Authority's guidances related to the coronavirus and its procedures and consultations on corona virus-related data processing 23
II.1.2. Personal data processing through video devices in the practice of the Authority 31
II.1.3. The most important data protection requirements related to data processing by political parties and organisations 52
II.1.4. Other important and interesting cases 58
II.2. Reporting data protection incidents 76
II.2.1. Guidelines on data breach notification 77
II.2.2. Significant data breaches 78
II.2.3. Data breaches notified based on the Privacy Act 83
II.3. Cases of litigation for the Authority 84
III. Procedures related to the processing of personal data for the purposes of law enforcement, defence and national security 101
III.1. Data processing by penitentiary institutions 101
III.2. The processing of personal data in decisions brought in infraction proceedings 104
III.3. Visit to the Headquarters of the Traffic Security Automated Processing Information System 106
III.4. Drone regulation 107
IV. Freedom of information 109
IV.1. Introduction 109
IV.2. Important decisions of the Constitutional Court 110
IV.3. Important court decisions 112
IV.4. Access to the data related to the coronavirus pandemic 116
IV.5. About requests for data in the public interest targeting NAIH 120
IV.6. Cost reimbursement 121

IV.7. Media and the public nature of the Internet 123
IV.7.1. The right “to be forgotten” 123
IV.7.2. Social media 129
IV.7.3. Is a message sent through Facebook a request for data in the public interest? 130
IV.8. Data of persons in public service accessible on the ground of public interest 131
IV.9. Transparency of municipalities 133
IV.9.1. Data accessible with respect to the utilisation of municipal assets . .133
IV.9.2. Municipal meetings, “leakages” 134
IV.9.3. The right of the mayor and of the municipal representative to access data 136
IV.9.4. Cases of the self-governments of ethnic minorities 138
IV.9.5. Disclosure lists by municipalities 138
IV.9.6. Statements of assets 138
IV.9.7. Canine registry 139
IV.10. TASZ’s comprehensive data request case 140
In 2019, the Társaság a Szabadságjogokért (TASZ; Hungarian Civil Liberties Union), a human rights association (hereinafter: data requester) submitted requests for data in the public interest to every government office in connection with the implementation of the provisions of the new Civil Code calling for the mandatory court review of decisions made prior to 2013 concerning the guardianship of persons excluding legal capacity. Every one of the government offices assessing the data request demanded cost reimbursement on the grounds that meeting the data request would disproportionately use the available labour force, the extent of which was greatly different county by county. The lowest amount was requested by Vas county at HUF 27,275, while the highest amount was requested by Hajdú-Bihar county at HUF 624,340. In view of this, the data requester submitted a second modified request for data to the government offices, in which they waived answering the question that would have required a review of the files, but referred to Government Decree 388/2017. (XII. 13.) on the mandatory provision of data by the National Statistical Data Capture Programme, which requires district offices to mandatorily provide data on the review of the guardianship of people. Counties Csongrád, Fejér, Jász-Nagykun-Szolnok, Nógrád, Pest, Szabolcs-Szatmár-Bereg and Tolna, as well as the capital city Budapest met the data request without demanding cost reimbursement, but they received absolutely no answer from 12 government offices, so they contacted them with a third request for data in the public interest on 13 December 2019, relative to the earlier data request, this time only asking the questions below: 115

IV.11. Data requests en masse. 143
IV.12. The accessibility of environmental information 144
V. The Authority's activities related to legislation. 147
V.1. The statistical data of cases related to legal regulation 147
V.2. Cases related to legal regulation during the emergency 149
V.2.1 Emergency 149
V.2.2 Data protection incidents 150
V.2.3 The eradication of illegal waste disposal 151
V.2.4 Cybersecurity Centre and Research Institute 152
V.2.5 Governmental Personnel Decision Support System 153
V.3. Providing opinions on draft legal regulations 154
V.3.1. Bill on family farms 154
V.3.2 Bill to amend the Act on the Rights of Ethnic Minorities. 155
V.3.3 Amendment of certain acts affecting defence 156
V.3.4 Opinion on the bill on the national data assets. 157
V.3.5 Consultation with citizens 158
V.3.6 Regulatory recommendation concerning national security checks . . .159
V.3.7 Act XLII of 2020 on the Amendment of Certain Acts concerning the Act on the Information Exchange within the Schengen Information System. . . .160
VI. Supervision of secrets, classified data and data with restricted access .161
VI.1. Accessibility of data related to secret adoption 161
VI.2. Complaint to the Constitutional Court case No. IV/540/2019 162
VII. International cases and social relations 165
VII.1. Review of the cooperative procedures conducted pursuant to GDPR 165
VII.2. NAIH's participation in the activities of the Board – sessions in 2020 – the operation of the European Data Protection Board in figures. 168
VII.3. Guidelines and opinions of the Board, the activities of the expert subgroups 170
VII.3.1. Guidelines on connected vehicles 170
VII.3.2. Guidelines on data processing in the context of the Covid-19 outbreak 170
VII.3.3. Guidelines on the management of data protection incidents 171
VII.3.4. Guidelines on the targeting of social media users 171
VII.3.5. Guidelines on the restriction of data subjects' rights 172
VII.3.6. Guidelines for transfers of personal data between EEA and non-EEA public authorities and bodies 172
VII.3.7. Recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. 173
VII.3.8. Draft decision on the general data protection provisions applicable as safeguards in the event of data transfers to third countries. 173

VII.3.9. Binding Corporate Rules 173
VII.3.10. Opinions concerning the accreditation criteria of bodies supervising codes of conduct and certification bodies 174
VII.3.11. Guidelines concerning the processing of financial data 174
VII.3.12. Guidelines on the right to be forgotten 176
VII.3.13. The first dispute resolution by the Board 176
VII.3.14. Harmonisation work concerning the imposition of fines 176
VII.3.15. Recommendations concerning Article 36 of the Law Enforcement Directive 177
VII.3.16. Additional activity of the Borders, Travel and Law Enforcement expert subgroup 177
VII.3.17. Data protection officer network 178
VII.3.18. Shift to the online work order necessitated by the pandemic 178
VII.4. Decisions on data protection by the Court of Justice of the European Union in 2020 178
VII.4.1. The Schrems II case 178
VII.4.2. The Orange Romania SA versus Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal case 181
VII.4.3. The VQ versus Land Hessen case 182
VII.4.4. Privacy International versus Secretary of State for Foreign and Commonwealth Affairs and others case 182
VII.5. Participation in the joint supervisory activity of data protection authorities 182
VII.5.1. Coordinated supervision committee 182
VII.5.2. Working group supervising data protection in the Schengen Information System 184
VII.5.3. A The working group supervising data protection in the Visa Information System 185
VII.5.4. The working group supervising data protection in the Eurodac System 186
VII.5.5. Cooperation board auditing data processing by Europol 187
VII.5.6. Judgment of the Court of Justice of the European Union: the Privacy International case. 187
VII.6. Results of the Schengen data protection audit of Hungary 188
VII.7. Application of the Tromsø Convention 189
VIII. Projects by NAIH 190
VIII.1. The STAR project. 190
VIII.2. The STAR II project 191
VIII.3. The Public Administration and Civil Service Development Operative Program (KÖFOP) 192

VIII.4. The Integrated Legislative System (IJR) Project 192
VIII.5. EKOP Project. 193
IX. Annexes 194
IX.1. The financial management of the Authority in 2020 194
IX.1.1. Revenue estimates and their performance data in 2020 194
IX.1.2. Expenditure estimates and their performance data in 2020 194
IX.1.3. Changes in the headcount of the Authority 197
IX.1.4. Changes in revenues from fines 198
IX.2. Participation of the President of the Authority in Hungarian and international conferences and events of the profession in 2020 198
IX.3. List of legal regulations and abbreviations mentioned in the report . . 200
Table of Contents 205

National Authority for Data Protection
and Freedom of Information

1055 Budapest, Falk Miksa utca 9-11.
Postal address: 1530 Budapest, Pf.: 5

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

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

Published by: Nemzeti Adatvédelmi és Információszabadság Hatóság –
Hungarian National Authority for Data Protection and Freedom of Information
Responsible publisher: Dr. Attila Péterfalvi President
ISSN 2063-403X (Printed)
ISSN 2063-4900 (Online)

National Authority for Data Protection and Freedom of Information

National Authority for Data Protection and Freedom of Information

1055 Budapest, Falk Miksa utca 9-11.
Postal address: 1530 Budapest, Pf.: 5

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

Published by: Nemzeti Adatvédelmi és Információszabadság Hatóság –
Hungarian National Authority for Data Protection and Freedom of Information
Responsible publisher: Dr. Attila Péterfalvi President
ISSN 2063-403X (Printed)
ISSN 2063-4900 (Online)