National Authority
for Data Protection
and Freedom of Information

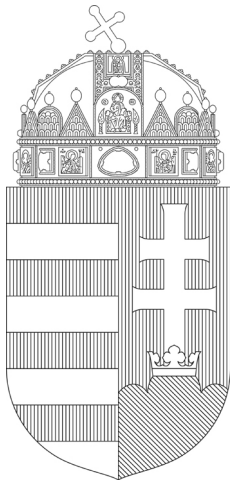
ANNUAL REPORT OF THE HUNGARIAN NATIONAL AUTHORITY FOR DATA PROTECTION AND FREEDOM OF INFORMATION (NAIH) 2022

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

on its activities in 2022

B/2589

Nemzeti Adatvédelmi és Információszabadság Hatóság
(Hungarian National Authority for Data Protection and Freedom of Information)
Budapest, 2023.



Introduction

Greetings, Dear Reader

The Hungarian National Authority for Data Protection and Freedom of Information celebrated the 10th anniversary of its foundation in 2022. Taking into account the experience of the past decade, NAIH has made a major contribution to enforcing data protection rights in collaboration with the countries of the European Economic Area with its powers to impose sanctions and to conduct authority procedures.

This year, the Authority has continued to deal with and adopt decisions on many significant data protection cases, and the number and amount of data protection fines has risen further; this year, we imposed a record HUF 250 million fine in a case related to the use of artificial intelligence.

It was a significant event of the year 2022 that Parliament decided to amend Act CXII of 2011 on the Right to Informational Self-Determination and the Freedom of Information during its session on 8 November 2022. The amendment, incorporated in the law as lex specialis, determines the rules of litigation that may be launched in relation to a request to access data of public interest different from those of civil procedure, and it also establishes the Central Information Public Data Registry. The new elements of the legislation are discussed in detail in the chapter on “Freedom of information”.

On 31 December 2022, our project “Exploring local practices of freedom of information and increasing their effectiveness” was closed. Freedom of information is one of the most fundamental guarantees of democratic operation, therefore it is important that both regulation and practice in Hungary function as optimally as possible, and the deliverables of our project help to achieve this.

We will have cause to celebrate in 2023 also, as the European Union’s General Data Protection Regulation (GDPR), the world’s most powerful data protection legislation, became mandatorily applicable on 25 May 2018. Cooperation between the authorities of the Member States can be termed successful: through their unified action, coordinated by the European Data Protection Board (EDPB), they have helped the different data controllers (organisations, companies) to comply with the rules of the GDPR, and they intervened in cases of breaches of the principles and unlawful processing and, where necessary, imposed significant fines.

Budapest, 20 February 2023

Dr. Attila Péterfalvi

Honorary university professor
President of the
Nemzeti Adatvédelmi és Információszabadság Hatóság

I. Statistical data on the operation of the Authority, social relations of the Authority

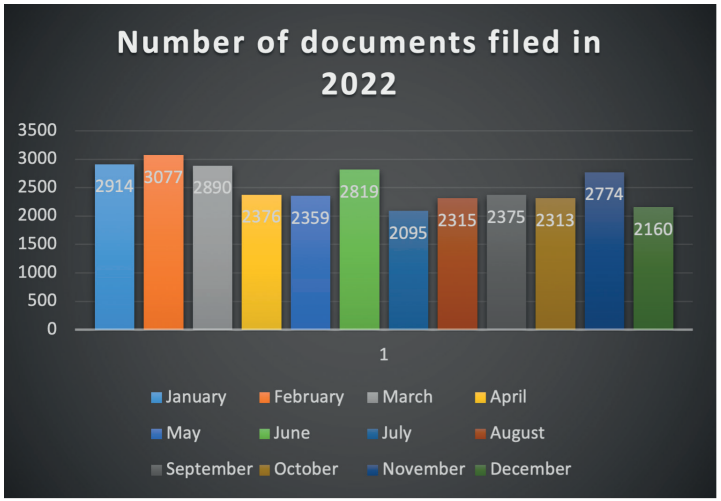
I.1. Statistical characteristics of our cases

Keeping in mind the objectives of previous years, the Authority has continued to focus its modernisation efforts on the customer-oriented and efficient discharge of its tasks, its continuous improvement and monitoring. In order to successfully achieve the tasks ahead, it is continuously monitoring its own operations, examining whether its objectives have been met and achieved in terms of the problems encountered and the prevention of shortcomings in the future.

Over the past year, the Authority has successfully implemented machine access to its office repository and an electronic mail module integrated into its case management system, and it has taken decisive steps to integrate a useful and easy-to-use component of the transition towards electronic administration, the template-driven technology of iForm and rapidly implemented its roll-out. The iForm electronic form filler will be accessible on the Government website's SZÜF interface (Personalised Administration Interface).

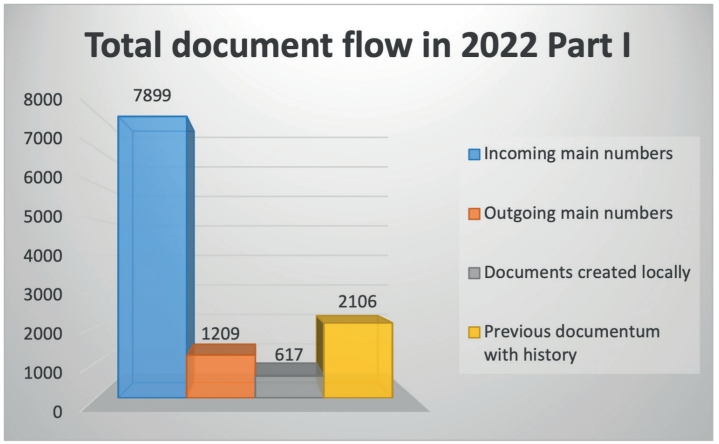
Simultaneously with reducing the administrative burden, the Authority strives to develop simplified, logical processes and implement them quickly and cost-effectively. The primary role of the case management area is to organise tasks into a system, grouping together the tasks with the same purpose or subject matter and focusing on the practical management of cases to ensure speedy administration and operational activity.

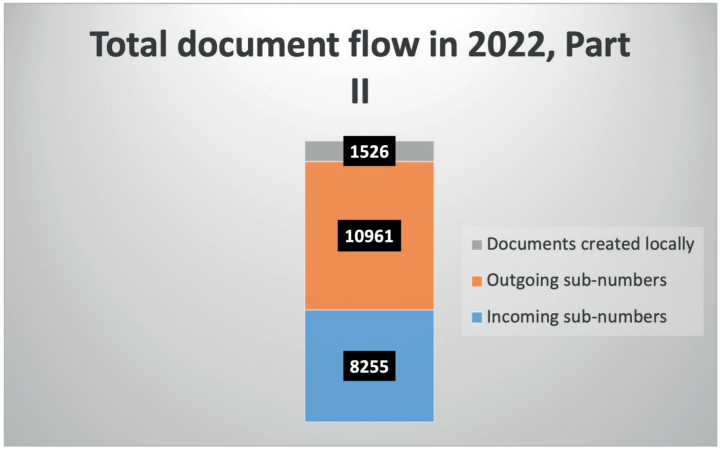
The priority strategic objective of the Authority remains the implementation of e-administration in the most comprehensive manner, the introduction of e-administrative services in the broadest possible circle, and the development of the related internal case management system (IRMA). The administrative management area can support the efficient, transparent, plannable and predictable operation of the Authority by streamlining internal administrative processes to better align the Authority with customer needs and broader environmental requirements.

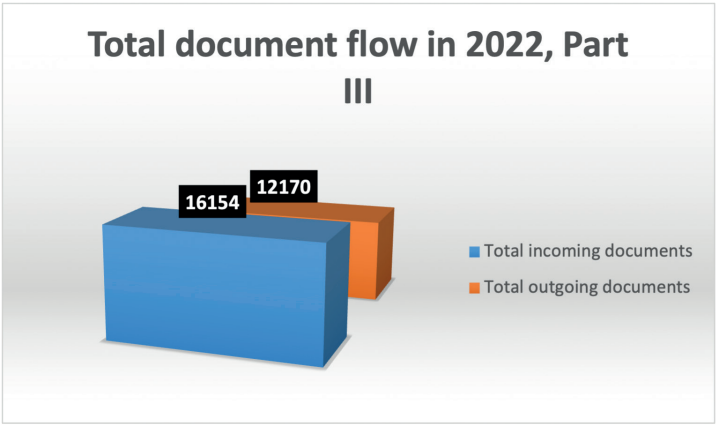


In a customer-oriented organisation, the form of contact is tailored to the needs of the customer. At the Authority, we therefore provide opportunities for the most energy-intensive, but also the most efficient and effective face-to-face customer contact, while at the same time using all interactive methods of customer contact (communication by telephone, in writing and by e-mail). The versatile discharge of our tasks has been accompanied by the reorganisation of the technical tasks of customer relations and the comprehensive provision of a broad range of information.

Total document flow of the Authority in 2022







In 2022, 7,619 new cases were filed in the Authority's internal case management system. Together with cases carried forward from earlier years (2,106), altogether 9,725 cases were in progress.

As shown by the data series, the number of authority audits increased by a third compared to the previous year (from 630 to 940), but the number of other authority cases increased just as sharply (from 556 to 708), while the number of inquiry and consultation cases did not exceed the previous year's level.

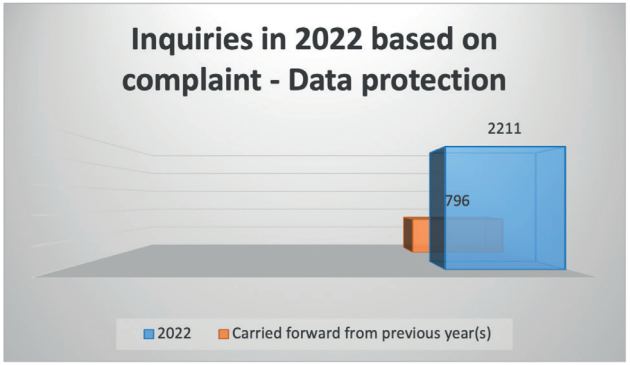
Major case types of the Authority in 2022

Authority cases	708
Inquiry cases	2836
Consultation cases	1293
Authority audits	940
Statements of opinion on legislation	151
GDPR cooperation (IMI)	1288

Inquiry procedures in 2022 – Data protection

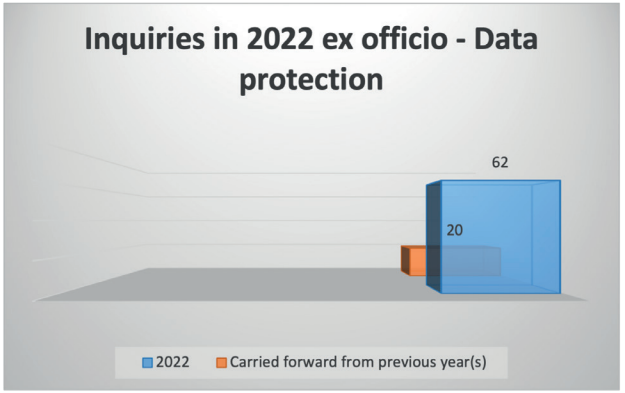
Inquiry cases based on complaint in 2022:

2022	2211
Carried forward from previous year(s)	796



Inquiry cases in 2022 ex officio

2022	62
Carried forward from previous year(s)	20



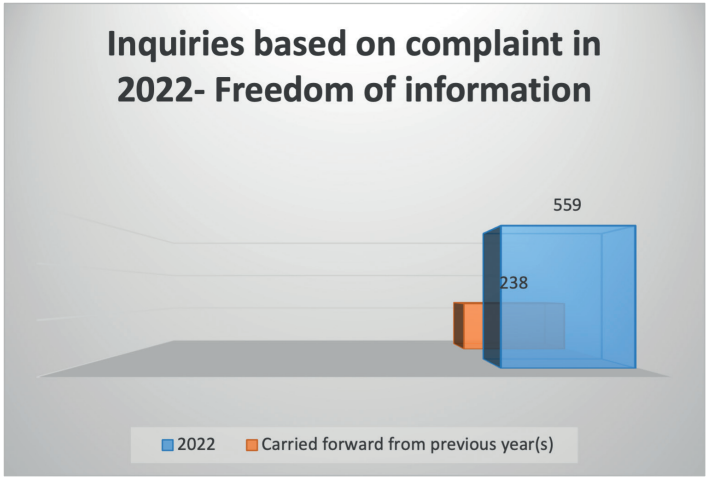
Data protection inquiry procedures in 2022 per case type

Case type	*Total*	*Carried forward from previous years*	*New cases*
Inquiry procedure ex officio	**62**	**20**	**42**
Inquiry procedure ex officio in data protection cases - Law Enforcement Directive	12	7	
Inquiry procedure ex officio in data protection cases - GDPR and other	49	13	36
Inquiry procedure ex officio in data protection cases - GDPR and other - data protection incident	1	-	1
Inquiry procedure based on complaint	2211	796	1415
Inquiry procedure based on complaint in data protection cases - data protection incident	178	47	131
Inquiry procedure based on complaint in data protection cases - Crime prevention data protection incident	9	2	7
Inquiry procedure based on complaint in data protection cases - Law Enforcement Directive	76	31	45
Inquiry procedure based on complaint in data protection cases - GDPR and other	1948	716	1232

Inquiry procedures in 2022 – Freedom of information

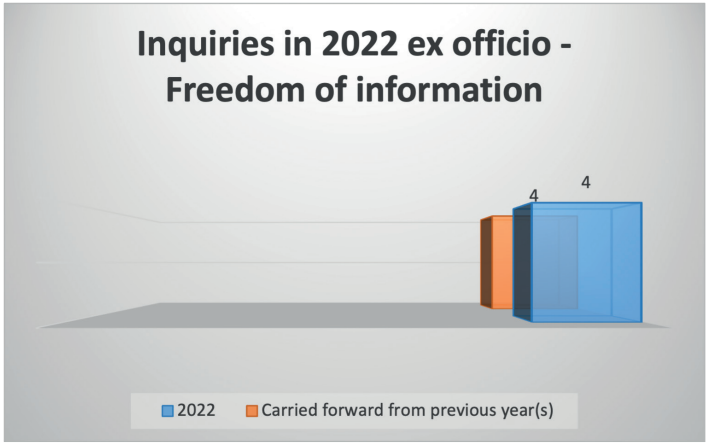
Inquiries based on complaint in 2022

2022	559
Carried forward from previous year(s)	238



Inquiries in 2022 *ex officio*

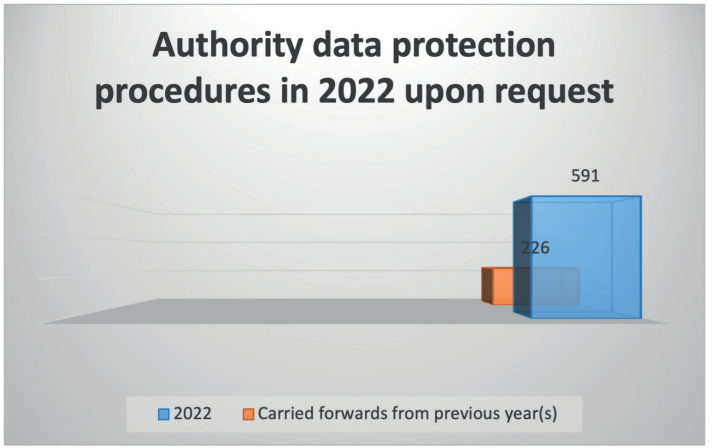
2022	4
Carried forward from previous year(s)	4



Number of authority data protection procedures in 2022

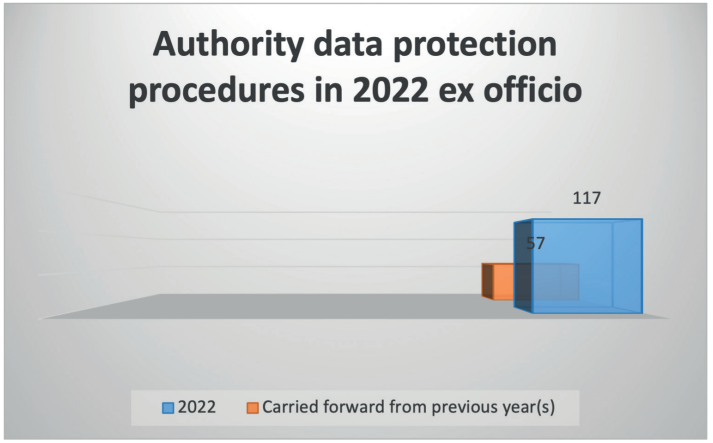
Authority data protection procedures in 2022 on request

2022	591
Carried forward from previous year(s)	226



Number of authority data protection procedures in 2022 *ex officio*

2022	117
Carried forward from previous year(s)	57

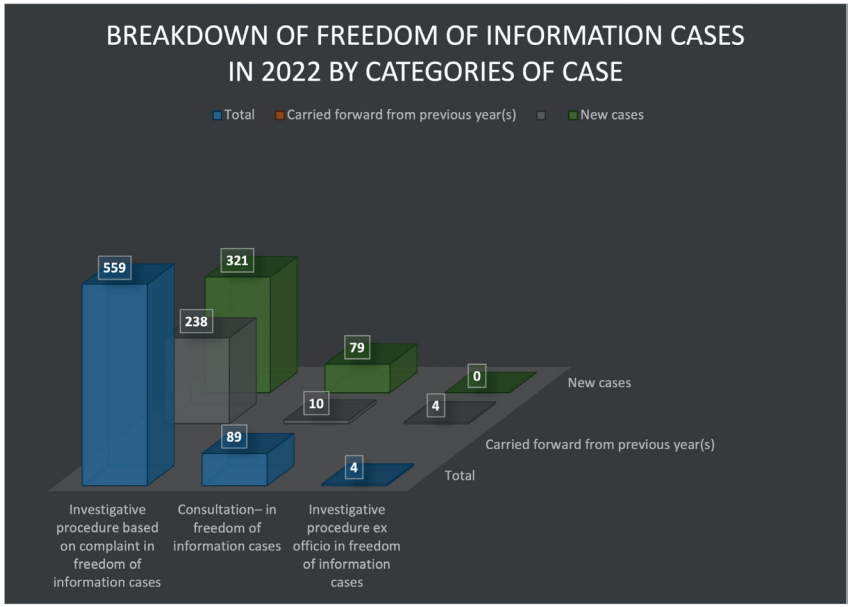


Authority procedures in 2022 by case type

Case type	*Total*	*Carried forward from previous years*	*New cases*
Authority data protection procedures *ex officio*	**117**	**57**	**60**
Authority data protection procedures *ex officio* - Law Enforcement Directive	3	2	1
Authority data protection procedures *ex officio* - Law Enforcement Directive - data protection incident	4	2	2
Authority data protection procedures *ex officio* - GDPR and other	77	42	35
Authority data protection procedures *ex officio* - GDPR and other - data protection incident	32	10	22
Authority data protection procedures *ex officio* - GDPR and other - freedom of the press and expression	1	1	-
Authority data protection procedures on request	**591**	**226**	**365**
Authority data protection procedures on request - Law Enforcement Directive	18	9	9
Authority data protection procedures on request - Law Enforcement Directive - data protection incident	1	-	1
Authority data protection procedures on request - GDPR and other	540	203	337
Authority data protection procedures on request - GDPR and other - data protection incident	31	13	18
Authority data protection procedures on request - GDPR and other - freedom of the press and expression	1	1	-

Breakdown of freedom of information cases in 2022 by categories of case

Case type	*Total*	*Carried forward from previous years*	*New cases*
Inquiry procedure based on complaint concerning freedom of information	559	238	321
Consultation – concerning freedom of information	89	10	79
Inquiry procedure *ex officio* concerning freedom of information	4	4	-



Authority audits in 2022

Authority audits in 2022	940
Carried forward from previous year(s)	304

Case type	Total	Carried forward from previous years	New cases
Authority audits in the data protection cases – Law Enforcement Directive	1	-	1
Authority audits in the data protection cases – Law Enforcement Directive – data protection incident	28	5	23
Authority audits in the data protection cases – GDPR and other	21	13	8
Authority audits in the data protection cases – GDPR and other – data protection incident	890	286	604

Statements of opinion on legislation in 2022

2022	151
Carried forward from previous year	7

Case type	Total	Carried forward from previous year	New cases
Statement of opinion on legislation on request (opinion on bill, consultation)	149	7	142
Proposal of legislation (statement of opinion of own bill, legislation initiated)	2	-	2

Major areas in international cooperation in 2022 (GDPR, IMI)

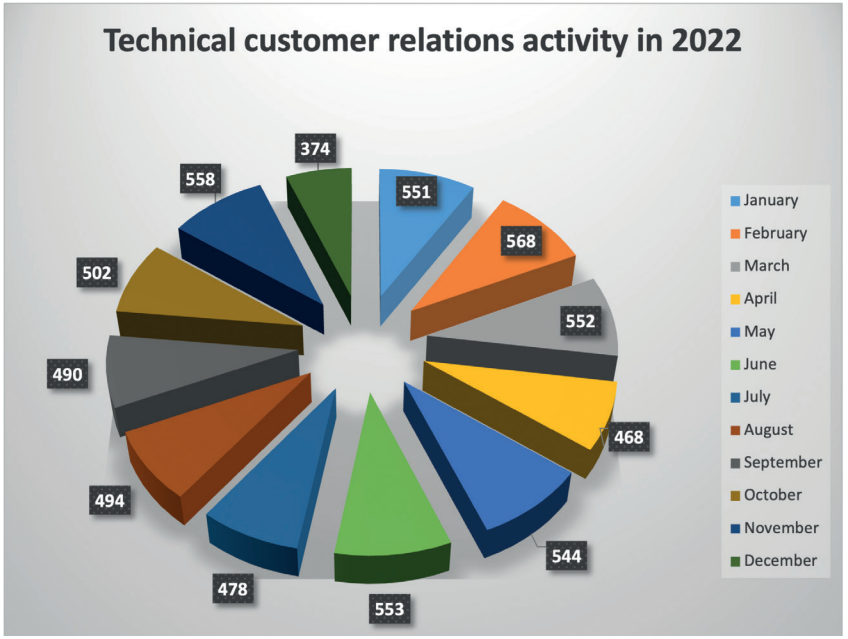
2022	**1288**
Carried forward from previous year	**198**

Case type	Total	Carried forward from previous year	New cases
Cooperation as concerned authority in procedures by EEA partner authorities – data protection incident	21	11	10
Cooperation as concerned authority in procedures by EEA partner authorities – GDPR 56,60,61,62,64,65	1265	187	1078
Cooperation as concerned authority in procedures by EEA partner authorities – freedom of the press and expression	2	-	2

The Authority's customer service received 6,132 phone calls in 2022, an increase of nearly ten percent compared to last year, which confirms the validity of the decision to make the Authority's customer service staff available to customers forty hours a week.

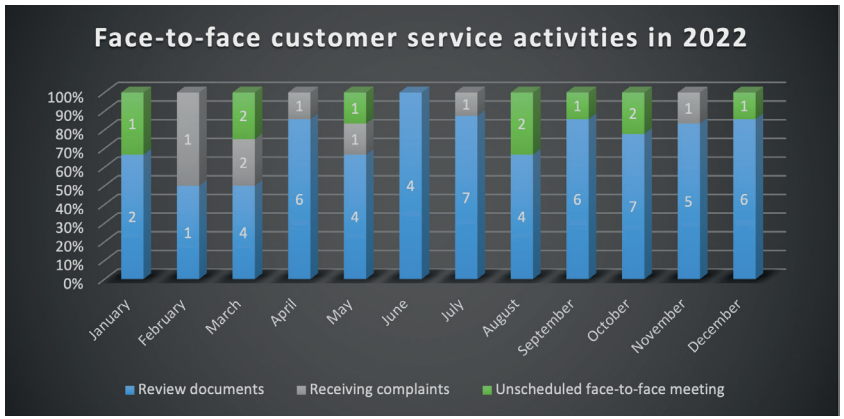
There have been no changes to the issues raised in the petitions, other than those mentioned in previous years' reports. The Authority's staff stressed that from 2022 onwards, no inquiry procedure can be initiated by e-mail, in addition to the authority procedure. Data subjects are advised to carefully study the complex procedural information available on the Authority's website in order to be able to exercise their rights in a meaningful and effective way. The attention of those calling on behalf of entities subject to electronic administration (e.g. legal representatives of clients, business organisations, public bodies) was drawn to the exclusive use of e-paper as a form of communication, as provided for in Article 9 of Act CCXXII of 2015 on the general rules of electronic administration and trust services (Eüsztv.).

With regard to the exercise of the right of access to documents in the case of public administrative procedures, information was provided in particular on the fact that access is granted primarily in person, and transfer of documents not submitted by the client requesting access to the document by electronic means is only available upon express request thereto.



In 2022, our customer service staff provided general written information in response to 17 requests for appointment applications, and they provided assistance on how data subjects can contact the Authority in relation to cases concerning the protection of personal data and access to and dissemination of data of public interest or data accessible on public interest grounds.

The Authority's face-to-face customer service activities evolved in 2022 as follows:



I.2. Annual conference of data protection officers

The conference on the most important achievements and experiences in the field of data protection and freedom of information in 2022, convened by the President of the Authority with regard to Article 25/N(2) of the Privacy Act, was held on 8 December 2022 for the data protection officers notified to the Authority and registered for the event, with the personal participation of 50 persons, in a live online broadcast.

In his opening address Dr. Attila Péterfalvi reviewed and assessed the Authority's annual activities and results. He directed attention to the most important elements of the 2022 amendments to the Privacy Act, including changes to the rules on the fees for the fulfilment of data requests, changes to the public disclosure obligations in relation to the Central Public Data Repository, changes to the procedural rules for lawsuits for the disclosure of data of public interest, and the tasks related to the entry of the transparency authority procedure.

Dr. Endre Győző Szabó, Deputy President, spoke of the activities of the European Data Protection Board in 2022 and current issues of data transfers to third countries
The Board pays particular attention to the impact of new technologies on the processing and protection of personal data. This is reflected in its statement on the digital euro and its guidelines on the use of facial recognition technology in the field of law enforcement. The Board has also issued guidelines on the use of the so-called "dark patterns" on social networking sites, which is a point of reference for data controllers. The guidelines on certain issues relating to the calculation of data protection fines and on the application of the one-stop shop rules aim to promote cooperation and the uniform application of the law among the Board's own members. Opinion No. 28/2022 represents a milestone in the application of the GDPR, because it approves the first European data protection seal.

As regards data transfers to third countries, the Board adopted a statement following the outbreak of the war between Russia and Ukraine, in which it highlighted the risks to the protection of personal data. The legislative work undertaken in the United States of America, which re-regulates the use of information collected in the course of intelligence activities and introduces a redress mechanism for EU citizens, offers a new perspective and an opportunity to examine whether the level of protection of personal data provided in the United States is recognised as adequate by the European Union. It is expected that the Board's opinion and,

if appropriate, the European Commission's conformity decision will be adopted in the first half of 2023.

Dr. Norbert Vass, a data protection expert, in his presentation on the issues arising on account of joint data management, addressed the problem of identifying joint controllers. He stated that not everyone who holds personal data is a controller, but that entities that do not carry out processing operations but take substantive decisions in relation to them may also qualify as controllers.

In his presentation, he provided delineation criteria between joint processing and multiple separate processing activities. This is mainly possible on the basis of case-by-case assessment, whereby it has to be considered whether the processing would be possible without coordinated decision by several parties, and not only with an explicit joint decision (using the analogy of competition law). It is not the identity of the data that is relevant, but the joint definition of the purposes and means of processing and the possibility of modification only by joint agreement. For this, the agreement of the parties may serve as a starting point, but the Authority is not bound by it, as confirmed by EDPB Guidelines 7/2020 and 8/2022.

The next step is to delineate the controller from the processor. A processor is a person or organisation separate from the controller making the decisions, who can only act in accordance with the instructions of the controller. This may have the effect of overriding the parties' agreement in certain cases, typically where one party reserves a lot of rights for itself in the contract and it can unilaterally modify the material conditions of processing without the agreement of the other party, then this cannot be considered joint processing, despite the agreement of the parties. However, discretion may be given to the processor in certain technical and organisational matters, the qualification of which also requires case-by-case assessment in view of the variety of data processing operations.

The fact that personal data are used separately for other purposes at a later stage of the data processing process does not exclude joint processing, but it is to be assessed on a purpose-by-purpose basis whether this is also a common purpose of processing. Albeit to varying degrees, providing adequate information is generally the responsibility of all joint controllers, even if the data are obtained only at a later stage of the processing and only one of the controllers has had contact with the data subject up to that stage. Sharing the responsibility between them should not lead to an erosion of data subjects' rights under the GDPR, as it only concerns the accounting between the parties. Joint controllers

are also obliged to regulate in their agreement, *inter alia*, how they are going to communicate with data subjects and data protection authorities. However, the designation of a contact point does not in itself constitute a common designation of a principal place of business, as this is determined by the data protection authorities for each controller separately under the GDPR (there is no "forum shopping"). After presenting several legal cases, Dr. Norbert Vass finally pointed out that if several Member States are concerned, Chapter VII of the GDPR (*Cooperation and Consistency*) shall also apply.

Dr. Dániel Eszteri, head of department, summarized the data protection interfaces of artificial intelligence (AI) in his presentation, touching upon the issues of machine learning, automated decision-making and profiling. In the introductory section of his presentation he explained the philosophical background of AI and its impact on society, and then showed its relationship with the management of personal data through the process of machine learning. Then, the provisions of the GDPR on automated decision-making and profiling and the interpretation of the transparency requirement (e.g. the black box phenomenon) in relation to such data processing were presented. The presentation also covered the dilemmas and possible solutions regarding the proper supply of information to data subjects; then he proceeded to present the key findings of the Authority's decision (NAIH-85-3/2022), which included the use of voice analytics AI by a bank.

Dr. Róbert Fischer, data protection expert, gave a brief presentation on camera systems using artificial intelligence and their possible functions, and drew attention to an earlier decision of the Authority concerning the use of such a camera system in a public place in Hungary.

First, he defined the concepts of identification and authentication in relation to the different functions of the systems, and then he discussed the potential risks of their use. He recalled the 2019 Report of the European Union Agency for Fundamental Rights, which states that determining the required level of accuracy of facial recognition software is a challenge for law enforcement: there are many ways to assess accuracy, depending on the task, purpose and context. When the technology is used in places frequented by millions of people, such as train stations or airports, even a relatively small percentage of errors (as low as 0.01%) means that hundreds of people have been misidentified.

The decision described in his presentation was related to the purchase of a camera system capable of facial recognition in a rural town. In relation to this, the Authority's position is that the current legislation does not allow for the operation

of a public area surveillance system in Hungary that handles biometric data. The provisions of Article 7(3) of Act LXIII of 1999 on public area surveillance (Ktftv.) and Article 42(2) of Act XXXIV of 1994 on the Police Force (Rtv.) which allows the public area surveillance and the Police to take pictures in public areas, provide a legal basis for this processing of personal data. These provisions cannot be interpreted as also authorising the processing of biometric data subject to stricter conditions for processing which require the application of additional safeguards, since the legislator's purpose in creating them did not include the use of facial recognition.

Dr. Anita Román, head of department, described the shortcomings and frequent errors encountered during the camera surveillance of municipal public areas. She emphasised that, in the course of public area camera surveillance, the surveillance system may be operated and managed primarily by the public area surveillance unit established by the municipality, or by the public area warden(s) if there is no public area surveillance unit, or by the municipal executive or a civil servant appointed by the body of representatives and employed by the municipality in the absence of a public area surveillance unit or public area warden. No other person, including the mayor, may carry out any data processing activities with the surveillance system of the municipality. However, other persons may also assist in the operation of the system, the maintenance of the cameras, and certain data processing operations may be carried out by others (e.g. the citizen's guard) on the basis of statutory provisions. She emphasized that, in the Authority's view, live monitoring without recording also constitutes data processing.
To start the data processing, a decision is required by the body of representatives on the placement of the image recorder, i.e. the use of the surveillance system, and the designation of the public area to be monitored. The Police must be informed of the installation of the image recorders and the public area to be monitored and this information must be published on the website of the Mayor's Office.

She highlighted that the recordings may only be used or transmitted for the purposes listed in the Act, and any use other than for the purposes specified in the Act is unlawful. Should any need arise to initiate a procedure not falling within the remit of the controller (public area warden) – without any other use of the recording (e.g. publication) – this must be initiated with the body or authority entitled to initiate the procedure.

She also pointed out that the controller must apply appropriate data security measures and may be assisted by a Data Protection Officer to be appointed mandatorily.

In addition, the Authority's experience has shown that there is often a lack of authorisation records, incomplete logging of access (manual/electronic) in municipal systems, and cameras may be integrated into public area surveillance systems that may have a number of vulnerabilities.

Dr. Anna Schnell, data protection expert, spoke of decisions in her presentation in which the Authority found that the municipality or the mayor either used or published the images. In her first example, a local authority published the full content of a decision taken during a closed meeting of the municipal board concerning a specific natural person on the official website of the municipality and, in its paper-based publication, thereby breaching the principle of data minimisation. In the course of the work of a municipal board, the adoption of a decision by the board and the publication of the decision adopted constitute separate data processing, and it is therefore necessary to examine the lawfulness of both separately.

In another case, documents containing personal data (nomination forms, memos, lists) found in the mayor's office when scrapping documents were photographed by the municipal executive in the presence of the mayor and forwarded to the local news portal. In doing so, they carried out autonomous data processing, defining a purpose and a means as controller, irrespective of the fact that the news portal also carried out processing by publishing them.

In the third decision described above, the Authority had to assess whether an audio recording of a closed meeting convened by the Mayor on a matter of public importance could be lawfully disclosed. In the course of the procedure, the statements made by the persons on the recording were assessed as public data on public interest grounds, first because the subject of the meeting was a matter of public interest and, second, because the participants were all members of the body or committee of the body and could therefore have been participants in a duly convened meeting. In the Authority's view, the fact that the closed meeting was held in circumvention of the rules of Act CLXXXIX of 2011 on the local governments of Hungary (Mötv.) did not exempt the meeting from the legal obligations of data protection and freedom of information. Although the Authority does not consider it acceptable and appropriate to make and publish audio recordings

in a covert manner, even at events related to public affairs, it has nevertheless found that the processing was lawful.

Dr. Ferenc Schiffer, freedom of information expert, presented the experience with the increasing number of requests for authority procedures for data protection related to the disclosure of personal data received by the Authority every year. In these procedures, freedom of expression and freedom of information come into conflict with the right to the protection of personal data, since the exercise of the right to freedom of expression necessarily involves - in most cases - the processing of personal data. This includes the issue of the removal of personal data from the search results of Internet-based search providers. The question of the legal basis is a recurrent problem in procedures against various press products. In the Authority's practice and view, the legal basis for processing for journalistic purposes may be primarily the legitimate interest of the controller. It is not acceptable for the controller to attribute several legal bases to the processing, for example, if the respondent indicates Article 6(1)(e) of the GDPR as the primary legal basis, and, in addition, in the light of the Authority's practice, Article 6(1)(f) as a secondary legal basis, since in this case the Authority would have to find a breach of the principles of the GDPR even in the case of a properly conducted interests balancing test.

The speaker also drew the audience's attention to the fact that, also in the cases described above, data controllers are obliged to provide appropriate information to data subjects on the circumstances of the processing of their personal data before the processing starts. In accordance with the principles of fairness and transparency, controllers should also provide the information most relevant to the data subject in relation to the addressee. An important, but recurrent, problem in relation to the provision of information to data subjects is that, where processing is based on the legitimate interest of the controller, the data subject should be explicitly, clearly and separately from any other information, informed that he or she may object to the processing on grounds relating to his or her particular situation, in accordance with Article 21 of the GDPR.

In relation to the "delisting" procedure by search providers, the Authority's position is that the data subject cannot and should not be expected to submit a request for the exercise of their rights as data subjects with precise legal references and indicating the legal basis of their request, but should, where possible, provide documentary evidence in support of the request. The controller must be able to identify, on the basis of the content of the request, which right the data subject is actually requesting to exercise.

Dr Júlia Sziklay, head of department, presented the research results of the Authority's Freedom of Information project, which are described in a separate chapter of this report.

In his presentation, István Csajági, head of unit, analysed the amendments to the Privacy Ac. and related legislation adopted in autumn 2022, resulting from the government's commitments made in the negotiations with the EU on the disbursement of EU financial resources and the implementation of the deliverables of the KÖFOP project implemented by the Authority.

After six years, the possibility for public bodies to charge labour costs incurred in fulfilling the data request to the data requester has been abolished (the possibility to charge postal expenses remains unchanged). The legislator established the Central Public Data Information Register and, in parallel, gave the Authority new procedural and sanctioning powers (authority procedure for transparency) from 28 February 2023. The Parliament rewrote the procedural rules for lawsuits for the release of data of public interest, modelled on press rectification procedures, and also repealed Government Decree 521/2020. (XI. 25.) on derogation from certain data request provisions in times of emergency from 31 December (possibility of extending the 45+45-day deadline).

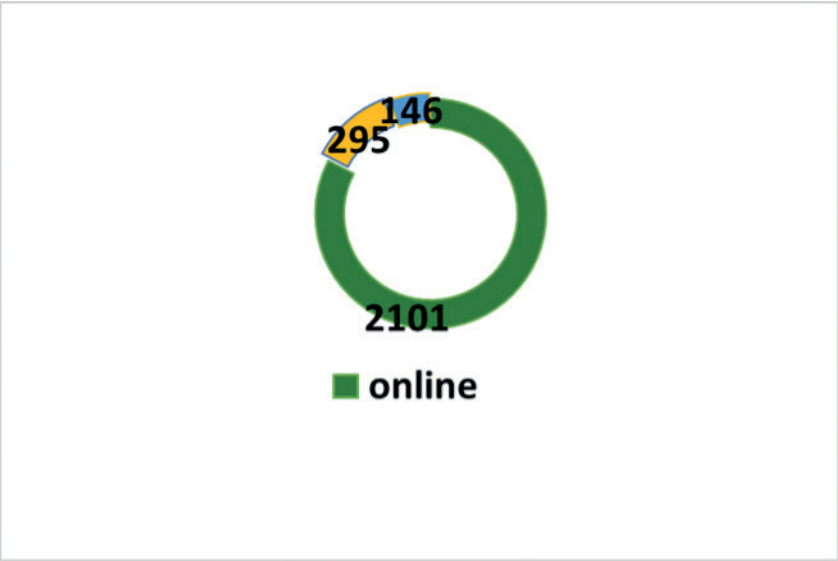
By way of closure of the conference, Dr. Attila Kiss, head of department, answered questions in connection with the presentations.

The recordings of the presentations at the conference can be accessed through the website of the Authority using the MTVA Médiaklikk streaming service; thanks to the support of MTVA, the presentations recorded over the past years also remained accessible to those interested in data protection and freedom of information (https://naih.hu/adatvedelmi-tisztviselok-konferenciaja/).

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

Between 1 January and 31 December 2022, members of the media published altogether 2,542 news items about the Hungarian National Authority for Data Protection and Freedom of Information. As to the types of media, most of the time used on the activities of the Authority were broadcast by the online media altogether on 2,101 occasions (82.65%). NAIH was presented in the printed press in 146 cases (5.74%) and 295 times (11.61%) in the electronic media.

Share of NAIH's appearances in the various media in 2022



Source: Observer Budapest Médiafigyelő Kft.

II. Data protection cases

II.1. Application of the General Data Protection Regulation

II.1.1. Data processing by forensic experts

The Authority continues to receive notifications concerning data processing by forensic experts (hereinafter, for the purposes of this heading: experts), including primarily psychologists. Whereas earlier the subject matter of the notifications was primarily procedure by seconded experts, in 2022 several notifications concerned the activities of private experts.

With regard to the fact that an expert qualifies as an independent controller and he/she has to comply with access requests from data subjects, the Authority has already taken a position in a previous authority decision and analysed also in detail how access requests can be met in the case of processing involving minors[1].

The notifications concerning the activities of experts included requests by data subjects to have access to data provided by them (e.g. answers given when completing tests and questionnaires, records of what they said in examination protocols, data of sound recordings, etc.) and data generated in the course of the professional work of the expert and the professional evaluation of the examinations in order to check the activities of the seconded expert and the final conclusions of their opinions. The persons participating in expert examinations wished to get the data by enforcing their right to access essentially with a view to checking their professional work because they disputed the findings of the expert. The Authority has also previously evaluated the assessment of requests for the professional data of experts[2]. In an inquiry procedure in 2022, the Authority confirmed its former interpretation of the law and declared that the rights of the data subject were not violated when the expert did not ensure the right of access of the person examined because the data subject is not entitled to check the expert. (*NAIH-2970/2022*) In a case, the petitioner also lodged a report with the police with a view to having his psycho-diagnostic data issued, and wished to use them in a litigation in order to have the expert's decision and opinion revised (*NAIH-656/2022*).

1 Report of the Nemzeti Adatvédelmi és Információszabadság Hatóság (Hungarian National Authority for Data Protection and Freedom of Information) on its activities in 2020, pp. 67-68

2 Report of the Nemzeti Adatvédelmi és Információszabadság Hatóság (Hungarian National Authority for Data Protection and Freedom of Information) on its activities in 2021, pp. 56-57

At the same time, it happens that forensic experts failed to make the data available which are rightfully claimed by the examined person, moreover, experts frequently fail to provide even a possibility for the exercise of data subjects' rights or are not even aware of their obligation to do so.
In a case, complainants objected to processing by the same forensic expert, who was seconded in court procedures and as a result of the secondment, examined the complainants. After this, the examined persons requested the forensic expert to make their examination documentation available to them, but all their letters were returned to the sender with the marking "Not sought", i.e. the expert did not receive the letters addressed to him at his office. The expert invoked erroneous postal delivery, which was ungrounded, and he attempted to be exempted from his obligation to respond. The Authority underlined that controllers have to implement appropriate technical and organisational measures in order to provide a possibility for the efficient exercise of data subject's rights. Such a measure can be, if the controller/expert ensures the receipt of data subjects' letters through postal redirection or the use of a post office box.

In 2022, two major issues arose from the examination of the notifications, which proved to be novelties relative to former cases in relation to processing by experts:

1. One problem related to *data subjects' rights in sound recordings made in the course of expert examination*. In the case of procedures by an expert seconded in a court authority procedure, the legal basis of processing by the expert is compliance with legal obligations set forth in GDPR Article 6(1)(c), which means that the processing does not require the data subject's consent. Once the secondment is completed, the expert has to block the data and during this period he can transfer these data only for the supervision of his work or for use in another procedure, then he has to erase them after ten years. At the same time, the relevant legal regulation allows the expert to make sound recordings of the examination provided that he obtained the data subject's consent, so the data subject's consent according to GDPR Article 6(1)(a) is the legal basis for making and processing the sound recording.

The issue of processing sound recordings arose in relation to two essentially contradictory requests from data subjects. In one notification, the notifier objected to the fact that the expert erased the sound recording once its transcript was complete, because according to the notifier, the transcript was not the same as what he actually said. The recording would have verified the information the expert used for producing his opinion, but proving this became impossible with

the erasure of the recording (*NAIH-1560/2022*). While in the other case, the data subject requested the erasure of the recording after it was made, but before using of what was said for drafting the opinion; in his view, he had the right to erasure, if he withdrew his consent (*NAIH-160/2022*). In one case, the data subject requested the erasure of the sound recording, while in the other case the data subject objected to the erasure.

In both cases, there was an identical circumstance in that the expert seconded in a court procedure made the sound recording on the basis of the data subject's consent in order to draft a thorough and professionally substantiated opinion. In the context of the data subject's request what needs to be analysed is the circumstance when the purpose of processing should be regarded as achieved in the course of processing the sound recording made during the expert examination, when the data content of the sound recording is no longer needed: once the transcript of the sound recording is made, or when the data subject already had access to the opinion produced in accordance with the procedural rules and has no longer any claim or objection to the transcript or the recording. The Authority's experience is that many experts erased the sound recordings once their transcripts are made in view of the principle of data minimisation. At the same time, this practice may infringe the data subject's rights, if the principle of accuracy is violated. The question of the period of time during which consent to the making a sound recording may be withdrawn and the sound recording may be erased also requires interpretation because this has an impact on the basic principles of court and authority procedures. Based on all this, the Authority deems it necessary to rethink and review the legal regulations concerning the issue of making and processing sound recordings.

2. The other group of cases in the forefront in 2022 concerned the *activities of private experts*.

The problem in one of the notifications was based on the fact that one of the parents about to be divorced had a psychological opinion drawn up on their child by a private expert. However, the parent did not submit the opinion in the court procedure, presumably because it contained a result other than what he expected, while the other parent did not have access to information on the content of the opinion, although it contained findings with respect to both her and her child, and the expert did not provide them to her even as part of the exercise of the right to access. The Authority established that neither sectoral legal regulation, nor procedural rule guarantees access to such a private expert opinion not submitted in litigation.

This case gave rise to a practical problem also with regard to the legal basis of processing. In contrast to the legal basis for processing by experts seconded in court or authority procedures, a private expert may process data related to an examination only with the prior written consent of the data subject. In the case investigated, the other parent did not give her consent either to the examination of the child or to the processing of their data. The Authority's position is that a private expert is not authorised to process the data of the child – and thus in the absence of lawful processing, ultimately to conduct the examination of the child – unless he has the consent of both legal representatives. At the same time, the best interests of the child, has to be taken into account when the findings of the expert examination to be carried out could serve his/her future interests in the context of the exercise of parental supervision or the regulation of contact. In such a case, the fact or condition which a parent wishes to prove has to be subjected to expert examination in some other lawful way. According to the Authority's position – if there is no court procedure in progress between the parents – the desired condition can be demonstrated in an extra-judicial procedure before a public notary and the legal basis of processing by an expert seconded by the public notary can be the mandatory requirement of the legal regulation and not consent; in this way, any eventual conflict of interest of the parents would not influence the feasibility of the expert examination. (*NAIH-1525/2022, NAIH-1528/2022*)

According to another notification related to processing by private experts, which also concerned a minor, in a toxic relationship between the parents one parent secretly made a sound recording of the other parent, which he/she wished to use to demonstrate that the child was endangered. The parent forwarded the recording to a private expert requesting him to produce an opinion showing that the other parent maltreated the child. The private expert could have processed and used the sound recording only with the written consent of the other parent, whose voice was recorded; obviously obtaining this consent would not be lifelike here either. In the absence of a legal basis, the private expert should not have taken on the case and could not have processed the data. It should be noted that the best interests of the minor must be borne in mind and if the child is genuinely in an endangered situation, it serves the child's interest, if this is exposed promptly and verifiably by the authorities. (*NAIH-5032/2022, NAIH-5033/2022, NAIH-5162/2022*)

As shown above, the work of experts is an area in Hungarian law, which represents substantial public interest because of its close relationship to the administration of justice, hence it is indispensable that experts take action on the basis of clear-cut regulations and a uniform interpretation of the law. Based on the experiences of the past period, the Authority has initiated consultations with the Hungarian Chamber of Forensic Experts with a view to developing a uniform legal practice.

II.1.2. The experiences of the 2022 national elections and the election campaign

Data protection problems and the areas and processing operations (such as contacting voters by phone/e-mail/mail, providing information them about various events, asking for their opinion on topical issues, filling in signature collection forms) where infringements may occur in relation to the processing of the voters' personal data were outlined already in the context of the election of members of the European Parliament in May 2019 and in the election of municipal representatives and representatives of the self-governing bodies of ethnic minorities in Hungary on 13 October 2019.

Collecting the experiences of earlier elections and summarising the problems arising in relation to processing activities, the Authority in its recommendation issued in February 2020 called the attention of those participating in processing, i.e. political parties and organisations, to the most important requirements. Despite this, according to the experiences of the Authority, the complaints related to processing of a political nature did not decline. The national general election of Members of Parliament was held on 3 April 2022, in relation to which the Authority received numerous notifications and complaints.

1. The 2022 general elections were preceded by a rather lengthy campaign period beginning with *the campaign activities related to the primaries administered by the opposition parties*. As it is well-known, prior to the general elections six parties decided to nominate a joint prime minister candidate at the national elections and have joint candidates in every individual constituency whose selection took place on the basis of the results of primaries held in two rounds.

In the course of the primaries at mobile ballot points where paper ballots were cast, the barcode of the address card as well as the *QR code on the ballot* were recorded. A complainant was concerned whether the QR code on the ballots contained a unique identifier, or the same information on each ballot – i.e. wheth-

er the ballot can be linked to the person casting it to find out who voted for which candidate. The investigation could not find any information pointing to the linkage of the QR code to the person casting the ballot, on that basis therefore it was not known who voted for which candidate.

At the same time, in the course of the investigation the Authority found that the parties processed the personal data of the persons casting their ballots in the primaries provided in relation to their participation without a legal basis, because the parties did not verify that the legal basis indicated by them existed, i.e. that the processing was necessary for carrying out a task of public interest or a public task. Furthermore, the Authority established in relation to the processing of data provided for maintaining contact that the controller did not provide adequate information on the purpose of processing, as a result of which an important notional element for the validity of the data subjects' consent was missing, so the personal data provided for maintaining contact was also processed without a legal basis. According to the Authority's findings, the information provided to data subjects on essential circumstances of processing was deficient also with regard to data for maintaining contact. (*NAIH-6001/2022*)

During this period, the Authority received a large number of complaints and notifications concerning the fact that voters were contacted by e-mail and phone (both calls and text messages) and post for campaign purposes. The Authority conducted an inquiry because of *unsolicited political campaign calls* encouraging support for the candidates of the opposition primaries and participation in the elections. During a campaign by phone, automated calls were initiated to the phone numbers in the database of the company handling the calls on behalf of an organisation supporting one of the opposition candidates for prime minister, during which a political message could be heard on behalf of the candidate for prime minister. First, the Authority clarified the roles in processing. The phone calls were made by the company using the phone numbers stored in its own database, hence it regarded itself as controller in the context of a campaign by phone and this was confirmed by the political organisation contracting them in the course of the inquiry.

The influence of the controller on the purposes and means of processing is an essential element of determining the controller. On this basis, the Authority established the capacity of both the political organisation and the company making the phone calls as controller with regard to the processing under investigation. In addition, however, the Authority also examined whether the political organisation and the company should be regarded as joint controllers or independent controllers.

Based on the facts of the case explored, the Authority found that the political organisation and the company making the phone calls jointly determined the purpose of processing, namely calling the attention of data subjects to the primary and to voting and, in relation this, to carry out a public opinion poll. The means of processing were also jointly determined as the political organisation decided that the purpose of processing was to be achieved by means of voice calls, but the way in which this was to be achieved, the use of personal data and the messages to be sent to the data subjects by means of voice calls were determined jointly by the political organisation and the company. Therefore, the political organisation and the company jointly participated in determining the purposes and means, they made coordinated and mutually dependent decisions about the mode of processing; their activities in the processing were inseparable and closely interrelated because of which they qualify as joint controllers.

In this context, the Authority underlined that in the event of joint processing, controllers need not equally divide controller's obligations, they can share fulfilment of these obligations among themselves. The controllers have to enter into an agreement, in which they have to decide in what way they are going to meet their obligations according to GDPR, i.e. on what legal basis, what personal data are to be processed by the controllers and for how long, or how they would act in relation to providing preliminary information to data subjects, and they have to determine who will be responsible for responding to requests when data subjects exercise their rights guaranteed in GDPR. However, a contract concluded by the joint controllers does not replace the controller agreement in itself, it may qualify as such only if it contains provisions with regard to the responsibility for meeting the controller's obligations and for the performance of the controller's tasks.

Furthermore, the Authority also found, in relation to the processing under investigation, that neither the political organisation, nor the company provided the basic general information to data subjects concerning the processing of their personal data in the course of the phone calls, nor did the company provide truthful information to the data subjects on the processing operations related to the outgoing phone calls it makes. (*NAIH-3182/2022*)

The Authority reached the same conclusion, namely the establishment of the capacity of joint controllers, when it investigated the processing of data in relation to a phone campaign taking place on the government's side. In this case, the

Authority found that neither the political party, nor the organisation administering the phone calls provided information to the data subjects on the processing of the personal data in the course of the phone calls, whereby data subjects' rights were infringed and this was closely related to the fact that their processing activities were not organised in a way to appropriately ensure and facilitate the exercise of data subjects' rights. (*NAIH-82/2022*)

The Authority also investigated a *data collection operation* of a party linked to the primaries whose purpose was *opinion polling*, after it received a notification on the information provided by the party on processing, on the range of data collected and the unlawfulness of the consent to maintaining contact in the future. During the period of signature collection, the controller collected data on two different signature collection forms consecutively, data were collected on the forms partly to support the petition and partly to collect contact data optionally provided by data subjects for the purpose of maintaining contact in the future, asking for opinions, providing information on the elections and other issues. The information provided on the forms used in the initial period of data collection was inappropriate, because it did not include the primary purpose of signature collection and, because of this, the consent given by those signing the form was in invalid. The information provided on the circumstances of processing was also inappropriate as the forms and the notice did not unambiguously display that the provision of the data was not mandatory for the purposes of maintaining contact and on the online petition support page of the website data subjects did not even have an opportunity not to provide these data. (*NAIH-1775/2022*)

2. The Authority also brought a decision concerning the legal compliance of a *processing practice related to opinion polling by phone.* A company entrusted by another company called the landline phone numbers in a database generated by querying the public phone directory, played the voice message and handed over the aggregated answers given to the four questions using the buttons of the phone to the company commissioning the opinion poll. In addition, the names and contact details of data subjects giving their consent by pressing a button were converted into machine-readable text by the automated system.

In the course of the phone campaign under investigation, two processing operations took place with different purposes and different legal bases: on the one hand, calling a list of phone numbers using an automated device, whose purpose was political opinion polling; on the other hand, recording the names and phone numbers of data subjects aligning address data to them, with the aim of promoting the services, obtaining more readers and increasing awareness through

direct marketing. Based on the Authority's practice, as a main rule, the phone number is in itself personal data according to the definition of personal data, for data to be characterised as personal data it is not necessary that the controller be able to link it to a specific natural person; indirect identification is sufficient, if it can obtain additional information needed for identification by lawful means.

The Authority found that the company did not provide any information to the data subjects apart from the purpose of its processing based on its legitimate interest. The controller is actively responsible for meeting controller obligations, including the availability of the information. Merely "putting on paper" in a processing contract that the subcontractor chosen and used by the controller has to abide by legal regulations – which is self-evident even without writing it down – does not exempt the controller from its responsibility under the law.

Information not provided by phone but merely online and after the event does not meet the obligation to provide information in advance, it does not ensure actual access to fundamental information for data subjects, it does not provide truthful information on how to exercise their rights of access and to object, if it is not clear from the phone call. To find this out is not the task of the data subject, information needed for exercising rights must be effectively communicated to the data subjects.

In the context of the legal basis of legitimate interest, it is important to underline that its purpose is not that in the absence of any other option the controller could refer to this to process personal data at any time, for any purpose in the absence of the applicability of other legal bases. Though it may seem as 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. Appropriate consideration, design and safeguards must ensure in practice the possibility for data subjects to become aware of the processing and to be able to object to it because after processing – particularly in the case of processing for a short period of time or non-recurrent processing such as a phone call – all the rights of data subjects are falling through. The identification and justification of the purpose of processing and the controllers' legitimate interest is not a task of the data subject, nor is it a task and responsibility of the Authority in the course of an authority procedure, instead of the controller. The controller has to specify for what purpose and on the grounds of what legitimate interests it wishes to process personal data, it has to justify them broken down to the level of data and purpose, it has to consider them and establish the safeguards. Failing to do so, and mentioning

no more than its own interests, turn the balancing of interests into an illusory activity, the result of which cannot be real.

In terms of lawfulness and safeguards, the two companies failed to ensure that phone numbers not listed in the online directory and those marked as prohibited for research and marketing purposes in the online directory were filtered out from the database. An additional problem was that the company erroneously classified pseudonymised phone numbers as non-personal data and did not meet any of the obligations of a controller, such as providing information in the course of processing the phone numbers. The Authority ordered that the processing related to the phone number database be brought in line with GDPR and imposed data protection fines on both companies. (*NAIH-770/2022*)

3. The Authority received several complaints in the period directly preceding the elections and in the weeks following the day of the election. The most complaints (altogether 138) related to the issue that *text messages were sent* to phone numbers in the personal use of data subjects *containing a form of address associated with the complaint, but excluding any information on the controller* in the days preceding the day of the elections. Over a hundred complaints were submitted in the days preceding the day of the elections because of unsolicited campaign calls of political content.

Based on the notifications, the Authority launched ex officio investigations in the course of which first it identified the person of the controller. Based on information available to date, voters were contacted with the campaign messages based on long contractual chains with the collaboration of many actors, because of this the identification of the person of the controllers take substantial time and is currently still in progress; once this is done, the Authority will be able to examine the lawfulness of processing. (*NAIH-4360/2022, NAIH-5243/2022, NAIH-4949/2022*)

Complaints were received also in relation to the fact that persons received *campaign letters* by post *addressed to them by name* encouraging them to vote for a candidate in their constituency. In these cases, voters were informed that in accordance with legal regulations, candidates have an opportunity to request the election office to issue the names and addresses of voters included in the constituency list for the electoral district concerned, and they were also informed that if they wished to avoid this in the future, they may submit requests to prohibit the issue of their data in the way indicated. (*NAIH-4143/2022*)

In the course of the 2022 parliamentary elections, citizens had an opportunity to request data online from the National Elections Office concerning whether their personal data are included in the recommendation form of a candidate for Members of Parliament in 2022. In this context, several notifications were received because the personal data of voters who did not support the given candidate were shown in the candidate's recommendation form. According to the Authority's position, the confirmation received from the elections office verifies only the recommendation form, which includes the recommendation of the given citizen, and the nominating organisation and the person collecting the recommendations, which can be associated with the form. It is, however, possible only with great difficulty, or not at all, to prove with the instruments of the Authority who was the actual person, who entered the personal data and signatures on the recommendation form, who was the actual person who signed the form or forged the signature, which is a precondition to establishing the lawfulness of the use of the other personal data indicated in the recommendation form. (*NAIH-3541/2022*)

The Authority investigated the *lawfulness of processing* by a political party in relation to *sending text messages for campaign purposes* in the days preceding the day of the elections. In the course of its investigation, the Authority found that the text messages contained absolutely no information of importance related to the processing, they did not indicate which political party sent it, only the content of the text allowed inferences as to the sender. The Authority underlined that appropriate information is indispensable for data subjects to be in a position to exercise their data subjects' rights. It should also be made clear who the text message is from when the contact is made by SMS; and transparency of processing can be ensured, for instance, by a link to the current privacy notice. (*NAIH-5542/2022*)

According to the findings of the Authority, the nature of the data protection infringements and the experiences of the cases clearly show that the problems occurring in the preceding election period have persisted, i.e. prior to the start of the processing, it is not specifically determined who or which organisation is responsible for the conduct in question or for meeting the obligations specified in the General Data Protection Regulation. As far as data subjects are concerned, perhaps the most substantial problem is that in most cases data subjects received no information about the processing at all, they learn of it only through the fact of the infringement, but in the absence of appropriate information – in many cases in the absence of knowledge of the person of the controller – they are not able to exercise their data subject rights at all.

II.1.3. Video surveillances

Complaints related to video surveillance make up a substantial portion of the cases before the Authority; many decisions were made concerning this subject matter in earlier years, which clearly reveal the Authority's interpretation of the law. Over and above the "usual" cases related to disputes among neighbours related to the surveillance systems of condominiums, the Authority adjudicated different criteria relative to earlier cases and decided on new issues of interpretation in some cases in 2022.

1. In one such case, the Authority investigated the *set of cameras mounted on the premises of a company*, because according to the complainant, the camera monitored a public area as well as the movement of the residents of a nearby condominium. The controller company operated a bar/coffee shop, renting a part of the pavement in front of the shop, i.e. public area, from the municipality and put up a terrace there. According to the relevant agreement on use, it did not extend to the 1.5-metre pedestrian corridor, only to the area in front of the shop and beyond the pedestrian corridor, i.e. expressly to the area occupied by tables and chairs. The company had the cameras mounted for the protection of the life and limb of the guests and the staff of the shop as well as for the protection of the assets on the terrace, citing the protection of its vital interests – GDPR Article 6(1)(d).
The Authority established that the legal basis of vital interest cannot be applied to processing related to video surveillance. The legal basis applicable to video surveillance could typically be legitimate interest, so the Authority found that the company processed personal data without any legal basis by monitoring the coffee tables on the terrace and recording images and voices of the guests on an ongoing basis with the cameras, which fails to meet the requirement of proportionality.

Guests can expect not to be monitored in public places, particularly if these places are typically used for leisure activities. A surveillance system operating at night and outside ordinary working hours generally meets the requirements of controllers to avoid threats to its assets. Based on this, a surveillance system operating at night and outside ordinary working hours directed at a public area may be proportionate restriction provided that necessity/lawfulness can be verified based on the other circumstances of processing. Sound recording, however, cannot be regarded as a lawful mode of processing even at night and outside ordinary working hours.

With regard to information on video surveillance, the controller has to apply a multi-level approach. To ensure transparency, the most important information on video surveillance must be displayed on a warning board (first level), so that a person is able to recognise the most important circumstances of surveillance prior to entering the surveyed area, such as detailed information concerning the purposes of processing, the person of the controller and the existence of the data subject's rights. Additional data to be communicated for comprehensive information can be provided by other means (second level), but its availability must be indicated at the first level of information. For these reasons, the Authority ordered the controller to operate the cameras based on the appropriate legal basis, while providing appropriate information, or cease processing. (*NAIH-88/2022*)

2. A serious infringement was found at another company, which operates *accommodation* at the Lake Balaton where it ran *two separate surveillance systems*. The first set of cameras consisted of fixed analogue cameras, which only streams live images, while the second one consisted of IP cameras, which recorded both images and sound. The cameras of the analogue system monitored the parking lot and the bend from the gate to the entrance of the accommodation, while the IP cameras monitored the reception, the dining room, the internal courtyard and the Jacuzzi located on the terrace of the building. These cameras were activated on motion and began recording. The camera aimed at the Jacuzzi was set so that it was suitable for monitoring also the persons staying at the neighbouring property. The controller cited GDPR Article 6(1)(f) – legitimate interest – as the legal basis of processing through the set of cameras, while the purpose of controlling was indicated as the protection of persons and assets.
The Authority found processing through the analogue set of cameras to be lawful as the viewing angle of the cameras included only those parts of the property where guests merely pass through and where they are actually able to achieve purposes of asset protection, e.g. the parking lot. In addition, as the cameras can be seen from the street, they also have deterrent force against unauthorized entry to the area of the property or committing other criminal acts against assets. According to the Authority's position, the fact that the system merely streams live images constitutes a much lower degree of intrusion into the data subject's privacy than if their personal data were recorded.

In its decision, however, the Authority established that sound recording through the IP cameras was unlawful, because the processing was not proportionate to the purpose to be achieved, and the controller failed to verify the need for it in the course of the procedure. Sound recording cannot be regarded as a generally established practice in the case of video surveillance for asset protection, hence

in the absence of information, the data subjects could not expect that the cameras would record their voice and their conversations in addition to their images . In connection with the camera located in the dining room, the Authority established that the processing was not proportionate to the purpose to be achieved and it is contrary to guest expectations to monitor them during rest and while having a meal. The Authority underlined the same in relation to the camera surveying the Jacuzzi and the internal courtyard stating that based on the camera recordings available, data subjects were not aware that they were monitored while using the Jacuzzi and that recordings were made of them, while in intimate situations. The Authority accepted the need for processing by way of the camera above the reception desk, in view of the fact that based on the recordings that is where cash was paid and the cash box was placed in a cabinet within the viewing angle of the camera.

In addition to this, the Authority established that the controller failed to provide transparent and, easy-to-access information to the data subjects on processing through the surveillance system and that the information communicated was erroneous and misleading.

Based on all this, the Authority ordered that the cameras located in the dining room and those aimed at the internal courtyard and the Jacuzzi were dismounted, and also ordered the controller to cease and desist and ordered it to pay a data protection fine of three million forints. (*NAIH-5114/2022*)

3. The Authority received several notifications, in which the notifiers objected to the operation of cameras in a *beauty parlour*, where facial and body treatments and medical aesthetic procedures are carried out in every room (office, treatment room, corridor, reception), through which both employees and guests are intercepted. Although the company running the beauty parlour informs data subjects about the video recording, but they do not provide any information on sound recording and the genuine purpose of the surveillance. According to the notifications, the purpose of making the sound recordings was to control the employees providing treatment and to obtain information about the guests and, on that basis, sell them even more kinds of treatment and facial care products. The notifications received by the Authority also included that the company carries out a promotion practice, in the course of which they request guests to provide the names and contact data of their acquaintances and using these data they then offer free treatment to the data subjects contacted in this manner.

In this case, the Authority launched an authority audit, in the course of which it held an onsite inspection in the beauty parlour, and based on the experiences, it launched an authority procedure for data protection ex officio. The Authority examined the recordings made by the cameras in the beauty parlour and the guest database and called upon the company running the beauty parlour to make statements on several occasions; because of the breach of the duty of cooperation and obstruction of the investigation into the facts of the case, the Authority was forced to impose a procedural fine on two occasions on the company.

Following the clarification of the facts of the case, the Authority established that the company surveyed both the employees and the guests unlawfully, its processing was flagrantly in violation of the law, inter alia, the company did not have a legal basis for sound recording, the use of the video recordings by the employees and the mode of access and its internal regulation were inappropriate. When examining the purposes and legal basis for processing the personal data of the guests, it was found that the company's processes were untransparent; in addition, the company was unable to verify the legal basis of processing in the cases of several thousand entries in its database. In order to process the data of its guests for marketing purposes, the beauty parlour neither provided adequate information to the data subjects nor justified the existence of the legal bases invoked by it. The Authority also established that the practice of customer recommendation was inacceptable, too. The company was also reprimanded by the Authority because it unlawfully processed special health-related data on the consultation forms and in its database.

Because of the infringements found, the Authority imposed a data protection fine of 30 million forints, prohibited video surveillance in the treatment rooms, the diagnostic and examination rooms and ordered the erasure of video recordings, health-related data and the data generated in the course of customer recommendation. (*NAIH-2732/2023*)

4. In another notification, the notifier objected to the unlawful video surveillance of employees and patients in a dental surgery by her employer, the owner of a dental surgery in its office and two branch offices; the patients were monitored not only while waiting for treatment, but also during treatment without their consent.

Based on Article 57(1)(f) of the General Data Protection Regulation and Section 38(3)(a) of the Privacy Act, the Authority launched an inquiry procedure and based on the answer sent by the notifier to the questions to clarify the facts of the

case and the enclosed photos it was found probable that the owner of the dental surgery infringed the provisions of the General Data Protection Regulation, hence in view of Section 60(1) of the Privacy Act, the Authority decided to launch an authority procedure for data protection, in the course of which it ordered an onsite inspection without sending preliminary notice.

In the course of the onsite inspection, the Authority noted that there was no pictogram on the entrance door to the surgery; according to a later statement of the owner of the dental surgery, this was because of the replacement of the door a few years ago. Two cameras operated in the waiting room to the surgery. The waiting room was used jointly by a laboratory and a dermatological surgery. There was a warning sign about the video surveillance in the waiting room and the privacy notice was also placed on the wall next to the door of the surgery. According to the statement of the owner of the dental surgery made on site, these two cameras were mounted for the purpose of protecting assets and persons. There were also two cameras operating in the treatment room, of which the viewing angle of the camera on the wall covered the entire treatment room, while the other was positioned above the assistant' desk and was aimed at the monitor on the assistant's desk. A PC and a DVR video recording unit were on the assistant's desk. Among other things, the live images of the cameras could be followed on the monitor. During treatment, the person treated was not seen on the recordings only when the treating dentist covered the patient. The live images of the cameras could also be seen on the PC in the treatment room. The assistant working in the surgery could only see the live images, she had no access to the other settings of the camera system, which was also confirmed by the IT expert of the Authority. According to the statement of the owner of the dental surgery made on site, only he was authorised to access the recordings.

As a result of the onsite inspection and the clarification of the facts of the case conducted in an authority procedure, the Authority found the following: in view of the fact that the cameras examined in the course of the onsite inspection were located and their viewing angle was set so that they also monitored employees, the rules of workplace video surveillance must be taken into account in this case. The camera system under investigation was capable of making and storing recordings, which were inspected by the representatives of the Authority in the course of the onsite inspection.

The controller cited the legitimate interest of the controller or a third party as the legal basis of video surveillance and the protection of physical security, personal freedom, the safeguarding of hazardous materials, the protection of business secrets and of assets as its purpose. In the context of video surveillance in the waiting room, the Authority found in the course of its onsite inspection that in addition to patients waiting for dental care, patients waiting for the laboratory and dermatological care were also within the viewing angle of the cameras operated by the controller. Recordings of patients arriving for other medical examinations can by themselves provide sensitive data on the health condition of patients, disclosing information on the persons through the fact that they may refer to the kind of medical care they were waiting for. During the onsite inspection, the Authority did not observe any valuable object in the waiting room – drinks dispenser, external reception desk, computer, painting, furniture, etc. –, which would be considered as being in line with the asset protection purpose and for which reason the cameras would be aimed at the assets to be protected. According to the controller's statement, physical atrocities warranted the video surveillance for the purpose of "protection of physical security and personal freedom", but in view of the fact that patients waiting for the other type of care in the waiting room were also within the viewing angle of the camera, the Authority did not perceive adequate reasons for the controller's interest taking precedence over the data subjects' right to the protection of their personal data. The Authority did not find the video surveillance of the entire waiting room acceptable.

Also in the case of surveillance in the treatment room/surgery, the Authority has previously stated that the camera must not show/record the patient during treatment in an identifiable manner, except with the patient's explicit written consent, e.g. for scientific or educational purposes. Patients can be recognised and identified from the moment of entering the treatment room to the end of the treatment; at best they are not seen when the treating dentist covers them, but even then they can be identified. In view of the fact that this is a medical intervention, the consent as legal basis can be questioned from the viewpoint that it is hard to imagine what a patient can do, if during dental treatment he or she would like to withdraw his/her consent to the surveillance, e.g. by stopping the camera in practice, except for scientific-educational purposes. Based on what was experienced by the Authority, asset protection and personal security set as purposes substantiating the employer's legitimate interest are not justified in the treatment room. During surgery hours, surveillance for the purpose of asset protection may be aimed only at the place where cash is handled or stored; it is unrealistic to have higher value dental equipment stolen during surgery hours. The processing purposes substantiating the legitimate interest of the controller are not warranted, the video surveillance of data subjects concerned – patients and employees – disproportionately affects the fundamental rights and freedoms, primarily of the employees monitored during the entire day. The viewing angle of the cam-

era in the treatment room covered not only the reception desk where cash was handled or the cabinet containing hazardous materials, but the entire room providing an opportunity for the unjustified and constant observation of patients and employees.

The Authority did not observe any high value objects either in the waiting room or in the treatment room that could be likely and realistically be stolen, whose safeguarding would have justified continuous video surveillance. Prior to the commissioning of a camera system, the controller must survey where and when cameras are absolutely necessary. The payment for dental treatment and the safekeeping of cash may indeed warrant video surveillance, but in such a case, the protection of assets would be acceptable as a lawful purpose only if the viewing angle of the camera was really directed at the place where cash is handled and where it is stored.

The viewing angles of the cameras were not set so as to be in line with the exclusive purpose of surveillance to protect persons and assets as emphasized by the controller several times and to focus only on those areas. The viewing angles of the cameras installed in the waiting room and the treatment room were suitable for the unjustified and constant monitoring of employees and not only those who were employed by the controller; according to the findings of the Authority, the entire day activity of employees could be checked based on the recordings; because of this, the controller infringed the principle of purpose limitation according to Article 5(2) of the General Data Protection Regulation.

In the context of the individual cameras, the controller did not specify the position of the individual cameras and their purpose with regard to the employees in any document whatsoever, why there was a need for constant and continuous video surveillance, he did not provide appropriate information on processing to the employees and thereby infringed Article 13(1)-(2) of the General Data Protection Regulation.

By operating the set of cameras under investigation, the controller kept employees under continuous control and total surveillance, observing their activities throughout the day whereby he infringed the principle of fair processing according to Article 5(1)(a) of the General Data Protection Regulation.

In its decision, the Authority ordered the controller to terminate video surveillance in the waiting room, or to set the viewing angle of the camera so that it is aimed exclusively at the door of the dental treatment room. The controller was

also ordered to terminate the video surveillance system installed in the treatment room, or to set the viewing angles of the cameras so that they should not be suitable for the unjustified, continuous surveillance of patients and employees and to amend the privacy notice concerning the video surveillance of employees. The Authority imposed a data protection fine to an amount of five-hundred thousand forints in the case. *(NAIH-903/2022*)

5. During the Authority's inquiry procedure for data protection, a legal entity keeping an office building and its vicinity under continuous video surveillance stated that in its position it has no obligation to comply with the requirements of the General Data Protection Regulation as *it only carries out real time monitoring*, thus its activities are not subject to the scope of the regulation. They also argued that in their view processing takes place only if recordings are made. In line with Guidelines 3/2019 on processing of personal data through video devices of the European Data Protection Board, the Authority declared that in some cases real-time monitoring may be more intrusive into privacy than the storage of the recordings and their automatic deletion after a restricted period, which means that this activity is a processing operation subject to the scope of the General Data Protection Regulation, even if the right to erasure cannot be exercised by the data subjects. *(NAIH-2929/2022)*

6. In cases involving video devices, it occurs that the controller *disputes or even denies the fact of processing of video surveillance*. With regard to processing through video devices in a shop, the Authority – based on the protocol made out of the onsite inspection conducted by the municipal executive – found that even though the petitionee did not acknowledge the fact of processing through video devices, it was not realistic to install a complete and functional set of cameras, including full cabling at a relatively high cost, and to use them only as pseudo cameras by cutting the cables, because mounting pseudo cameras can be carried out at substantially lower costs and labour. The entrepreneur subject to the petition did not acknowledge processing through video devices, hence it did not cite a legal basis either and, furthermore, violated the principle of transparency as it failed to provide information on processing through video devices to the data subjects. (*NAIH-197/2022*)

In the same case, a dissatisfied customer of the company also complained about the information provided on processing related to online sale of products, which leads us to a different topic, that of marketing related processing, another area where infringements continue to be frequent.

II.1.4. Marketing related processing

1. In the case referred to in the preceding subheading, the Authority established that the company running a webshop also infringed the principle of *transparency*, because it failed to indicate the source of personal data in its privacy notice and failed to separate the privacy notice from the rules containing its general terms and conditions of contract and, furthermore, failed to provide information on the most important circumstances of its processing of personal data.

The petitonee also failed to provide adequate information in the sense that the data subject's consent was wrongly indicated as the legal basis for the processing in the contested privacy notice, despite the fact that, according to its statement sent to the Authority, it does not process personal data solely on the basis of this legal basis; moreover, it did not provide clear information on all data subjects' rights and the right to apply to the supervisory authority. (*NAIH-197/2022*).

2. According to the facts of another case, a company marketed collector's coins issued by itself. The procedure focused on the way in which the company obtained the personal data of its new customers and the information it provided to data subjects. The source of the data is a *brochure sent as a supplement to several newspapers*; the products can be ordered by completing the brochure, which also included their consent to processing. Orders can be made by sending the brochure by mail, or by phone calling the phone number in the brochure or online. If ordering by mail or phone, the information provided did not include the elements set forth in GDPR. The brochure did not provide information to those interested that not all of the address, phone number and e-mail address were required and only each of these modes of contact could be consented to together when using the phone.. The information did not mention that the e-mail addresses processed for the purpose of maintaining contact are transferred to the operators of Google and Facebook for the purpose of targeted advertisements, and there was no separate opportunity to consent to this.

The legal basis cited by the controller, the consent of the data subjects [GDPR Article 6(1)(a)] is rendered invalid by the absence of informed consent and the circumstance that consent to future processing for marketing purposes and ordering the product takes place by ticking of the same box. Because of this, the Authority ordered the controller in its decision to bring its processing for the purposes of direct marketing in line with GDPR, i.e. to continue its data collection by mail and by phone only if it enables data subjects to give their consent separately for the individual processing purposes and separately from the order (such as contact by e-mail, contact by phone and contact by mail) and to provide adequate preliminary information to the data subjects. In addition, the Authority imposed a data protection fine of HUF 30,000,000, in view of the severity of the infringement, the full absence of transparency, the very high revenues and profit maximization as the purpose of processing to be achieved. (*NAIH-2501/2022*)

3. Similarly, severe infringements were found because of processing by a company specialised in audiometric testing related its *letters addressed to specific names by mail inviting persons to audiometric testing*. The company requested the Ministry of the Interior (Registry of personal data and residential addresses) to provide the names and residential addresses required for contacting potential customers – largely persons in the elderly age group – to contact them by mail. The company relied on legal basis of contacting the data subjects by mail on that, in their view, the consent of citizens in the personal data and residential address registry can be regarded as automatically given, if they made no provision to prohibit the issue of their data. The Authority, however, established that consent cannot be a lawful legal basis for contacting people by mail, because all of its conceptual elements – a clear, voluntary, specific expression of consent by the data subject based on appropriate information – were missing.

The Authority also established the infringement of the principles of purpose limitation and fair procedure, because the company, in order to comply with the legal regulations amended in the meantime, indicated market research as the purpose of processing instead of direct marketing as stated earlier, although this was inaccurate, and continued to send its letters to the data subject with the previous content and offering an opportunity for free audiometric tests and sending the invitations to the data subjects by mail continued for the purpose of selling their product. According to the position of the Authority, the company's purpose of market research was not verified and the company misled both the data subjects and the Ministry of the Interior of the true purpose of its processing. Furthermore, the Authority did not regard the content of the privacy notice included in the invitation sent by mail as adequate, because it was not full, unambiguous, appropriate and accurate. (*NAIH-5802/2022*)

4. Compliance of c*ookie consent management systems* (hereinafter: CMS) with GDPR was at the focus of the procedure in the case, in which the media content made accessible to the public on websites operated by a media group also displayed advertisements. In the first CMS case, the Authority established the client's role as controller, the absence of appropriate preliminary information and in relation to this, the absence of a legal basis, as well as the lack of transparency

and fairness in the mode of consent to data transmission to the partners (several hundred partners). Once the first CMS is set and saved, a new, different type of setting panel pops up on the website to manage consent, which is confusing for the users of the website. In addition, after requesting separate consent, the second panel tells the data subject refusing to consent that it is not possible to refuse consent, or in the event of refusal it blocks access to the content of the website as a so-called cookie wall. The Authority also found that some cookies used by the websites were suitable for identifying, tracking and profiling individual users of the website, and the information provided on them did not include all the minimum information according to GDPR Article 13 and the small amount of meaningful information was accessible to data subjects with a great deal of difficulty through an insufficiently transparent interface in a manner that was not suitable to provide real information. The controller acknowledged the faults of its system and promised to rectify them, which, however, it did not do in substance, the minor formal alternations did not change the essence of the infringement. The Authority ordered the controller to continue the processing of personal data on the websites only if it can guarantee compliance with GDPR and imposed a data protection fine of HUF 10,000,000. (*NAIH-3195/2022*)

II.1.5. Processing of health-related data

Unfortunately, there were several cases this year in which the Authority had to establish severe infringement in relation to the processing of health-related data.

1. In a gynaecology case, a gynaecologist provided pregnancy care to the petitioner as part of private health care. Following the death of the foetus, the petitioner requested the issue of a copy of her entire health documentation in writing on several occasions; however, the gynaecologist would not even accept the requests. Based on domestic regulation, the service provider has an obligation to keep documentation and it should have provided a copy of it pursuant to GDPR.

The Authority found that the gynaecologist providing care did not ensure that anyone should receive the mail arriving at the premises of the surgery he rented, so he did not receive the data subject's request. It was proven in the course of the procedure that the gynaecologist did not produce any kind of documentation on the care of the pregnant woman, he did not give any paper-based findings to the patient, he failed to meet his mandatory obligation set forth in legal regulation to electronically upload findings, so the Authority was unable to order the issue of a copy of the documentation. In the course of the Authority procedure, the gynaecologist made contradictory statements, his privacy notice provided to data subjects contained inaccurate information as he informed them of keeping electronic and hard copy documentation and meeting his legal obligation to upload information, hence the Authority established that the gynaecologist's processing was not transparent and imposed a data protection fine. (*NAIH-4137/2022*)

2. A dental surgery as controller was requested by a patient to let him have a copy of his X-ray findings by e-mail. An earlier similar request of the data subject had already been met by the controller; however, their relationship deteriorated later and the controller would not fulfil the later request. He justified the decision by stating that he was unable to identify the data subject and so would not fulfil the request by e-mail, instead he would send the requested findings on CD by mail. The controller also offered an opportunity for data reconciliation underlining that if it is met, he would send the findings by e-mail. The data subject notified him that he would not be able to meet the conditions of data reconciliation because of his health condition, and he would not be able to access his mail as he will not be accessible at his postal address for an extended period of time, and in any case, he did not have a CD player, so he insisted on receiving the data by e-mail. The data subject also notified the controller that his X-ray findings were needed for his emergency care and because of his oncological disease, under the given circumstances, a repetition of the X-ray examination would entail the risk of being detrimental to his health. Finally, the controller sent the findings on CD by mail to the patient. Handing over the copies on CD in itself would not have violated the data subject's right to access, but under the given circumstances, the chosen mode was detrimental to the data subject, while he had a recognisable interest in the requested mode of receipt. Thus, the controller breached his obligation to facilitate the exercise of the data subject's rights by choosing the postal route instead of e-mail, without having any justifiable reason to do so. The controller could identify both the e-mail address and the residential address of the data subject, in addition, in the given situation the controller had no reason to hope for a higher degree of data security from delivery by mail.

According to the Authority, both appropriate information about processing and a reliable data reconciliation procedure are important, primarily because these were health-related, i.e. special category data, whose processing may take decades. In this case, the designed mode of data reconciliation was, on the one hand, unreliable, and on the other hand, the document processing practice, which became known in respect to it, was unlawful, furthermore, the information provided was deficient. A Hungarian language privacy notice was only available in the surgery. The controller failed to publish the privacy notice on its non-Hun-

garian website and he did not have a Hungarian website. The document was not suitable for providing information, partly because of its erroneous content and partly because it was hard to access. At one point of the correspondence between the parties, the controller wrote that in the light of the conflict, he would consider whether to fulfil the data subject's request. The Authority stressed that compliance with controller obligations is not up a matter of consideration, but an objective obligation. Although the data subject need not justify his request for the issue of copies, it was clear that he had an overriding interest in having his findings sent as soon as possible. This conduct was clearly unfair, particularly in view of the data subject's underlying medical condition and his interest in emergency care. (*NAIH-132/2022*)

3. In another case, the controller was a company providing physical well-being services as its main activity. A customer of the controller (the data subject) made use of the controller's services in relation to his oncological condition, but when he asked for the copies of the results of the measurements carried out as part of the service, the controller refused to issue them. The controller did not include any justification of substance in its decision, nor did he make any statement whether it would satisfy the request in another way or under specific conditions; in fact, it made the exercise of data subject's rights in relation to the requested results of measurement essentially impossible. In that situation, the data subject did not have access to the requested measurement results, while the controller was aware of the data subject's severe disease and his outstanding interest in accessing the data. The controller acquiesced in the disadvantage caused, without taking any steps at all to facilitate the exercise of the data subject's rights.

The controller did not publish any information on the processing in question, while it did have a privacy notice published on its website in relation to its other activities. In the absence of a privacy notice, the data subject did not have an insight into the ongoing processing of his personal data, his data subject's rights, the possibilities of legal remedy and he received no information on these issues even in the answer to his data subject request from the controller.

In relation to this processing, transparency was breached to such an extent that the data subject could reasonably believe that he was making use of some health care service (in relation to which, the data subject lodged complaints with other authorities, too).

During the procedure, the controller made contradictory statements also in relation to the purpose of the processing under investigation. It explained that according to its general administrative procedures, measurement documents are retained until clients requested deletion and they are retained for the purpose of enabling it to issue requested copies of the document. It should be stressed that this is not a purpose of processing, but a right of the data subject related to processing carried out for the given purpose. At the same time, even the "purpose" cited was thwarted in the course of its administration because it failed to issue the copies. Also, the controller made contradictory statements concerning the range of data processed and the processing operations carried out using the measuring devices, through which the Authority established an infringement of the principle of purpose limitation. (*NAIH-1433/2023*)

4. According to a complaint, a private health care provider wanted to charge a fee even for the first copy of health care documentation, claiming that the patient would receive the findings at the end of treatment, so any additional copy would qualify as a copy subject to the payment of a fee. This would have cost tens of thousands of forints owing to more than ten years' treatment of the data subject. The Authority declared that based on the sectoral legal regulation, the issue of findings, which is an obligation of the service provider, is independent of the exercise of data subject's rights set forth in the General Data Protection Regulation. Receipt of the findings based on sectoral requirements does not, in any way, qualify as the exercise of the data subject's data protection right; the data subject's request for a copy submitted for the first time is to be fulfilled free of charge. In addition to analysing access as the purpose of the data subject's right, the Authority also established that if his findings and documentation are accessible to the data subject in the service provider's own electronic system, that may comply with ensuring the right of access, so the Authority ordered the controller to provide copies of the documents free of charge to which the data subject did not have access in the service provider's system. (*NAIH-3849/2022*)

II.1.6. Other important cases subject to the General Data Protection Regulation

1. Aptitude/IQ testing of children in specialised care

The Authority launched an inquiry based on the notification of an NGO in a case also published in the press, in which the president of the National Specialised Service for Child Protection (hereinafter: OGYSZ) issued an individual instruction in relation to the implementation of the aptitude/IQ testing of children in specialised care. According to the instruction, children aged 6-18 in childcare protec-

tion had mandatorily to undergo testing with the collaboration of their guardians and they had to complete the test accessible on the website https://testometrika.com. The guardians received the order to perform the testing, if they were prevented, the test was to be carried out by the deputy guardian, the foster parent or a teacher of the children's home/residential home. At the end of completing the test, the child received a unique identifier and the result had to be sent together with the identifier to the county/Budapest territorial specialised service for child protection.

The Authority reviewed the website referred to and carried out a test registration, in the course of which it found that on the Russian website consent to processing had to be given unconditionally, the website could process the data even after the withdrawal of consent, if the Russian law so provides, and the data of the website's user were automatically transferred to Google and Yandex as third parties providing web analysis cookies for the online platform.

According to the position of the Authority, the above constituted a direct threat of infringement from a data protection point of view with regard to the fact that children under child protection were required to complete the test in the website mentioned, in the course of which the data landed outside the Hungarian jurisdiction through transfer to unsafe third countries,, particularly as this took place in the course of processing related to the performance of public duties, hence the Authority ordered OGYSZ to terminate the processing ordered in the instruction. OGYSZ complied with the order.

In addition to issuing the order, the Authority investigated processing related to the children's test results ex officio. In the course of the investigation, it was found that the participation of the guardian in completing the test ordered by an instruction received within the framework of his/her employment relationship, the processing and the forwarding of the test results and the processing of the data set organised into a structured database covering the entire range of data subjects differs from the range of data generally processed by guardians and guardians' organisations based on authorisation by legal regulation, hence processing aimed at this qualifies as independent processing, for which OGYSZ had neither authorisation based on legal regulation, nor any other legal basis. The purpose of processing indicated by OGYSZ was the determination of strategic and developmental directions, i.e. a general goal that is not unique to a child, as a result of which the processing of personal data was not at all justified in the Authority's view. As no individual goal was specified as the purpose of processing, the Authority is of the opinion that, had the data otherwise been lawfully

collected, the pseudonymised data set should have been anonymised after the receipt of the results both for OGYSZ and the territorial specialised services so as to prevent the identification of the data subjects in any way.

Through the experiences of the test registration, the Authority also established that the test did not give accurate results of the intelligence level of the children for several reasons, so it could be suitable at best to map out rough and ready magnitudes; it is, however, dubious whether the results of a 'recreational' test, which in many cases are not even accurate, could serve as a reference for a budgetary organ at all, while the results obtained could be attributed to the individual children.

The Authority also established that neither the guardians, nor the children received preliminary information on processing and also that OGYSZ as a result of the nature of its activities and the range of data subjects should proceed with particular attention in analysing risks in every case when it intends to pursue new processing activities. (*NAIH-7237/2022*)

2. The processing of a sound recording in the course of a guardianship procedure

A divorced father requested the Authority to establish that the local family assistance centre unlawfully processed and forwarded a sound recording containing his personal data to another child welfare centre in the course of a guardianship procedure and unlawfully refused to comply with his access request. The family assistance centre first stated that the requested sound recording was not part of the documentation and later that it was physically not part of the documentation as it was not sent to it on a tangible medium and it alleged to have erased the sound recording once it forwarded it electronically to the other child welfare centre.

In the course of the procedure, the Authority established that as the petitioner requested a copy of the sound recording by reference to the General Data Protection Regulation in its request submitted to the family assistance centre, these requests qualify as access requests under Article 15(3) of the General Data Protection Regulation. The Authority also established that the family assistance centre was in possession of the sound recording at the time of the submission of the data subject's request, in contrast to their answers to the father and their statements, i.e. their statements were untrue. Hence, they should have

made a copy of the sound recording available to the petitioner as that was his personal data. As the family assistance centre provided inaccurate information on the fact of processing and its essential circumstances and it did not ensure the transparency of its processing for the petitioner, and as it denied that the sound recording was available to it, the Authority ex officio reprimanded the controller. (*NAIH-13/2022*)

3. The processing practice of a retail chain in relation to the purchase of alcoholic drinks

The Authority received several complaints concerning the processing practice of a retail chain in relation to the purchase of alcoholic drinks in August 2022. According to the information provided by the notifier, in the event of purchasing alcoholic drinks in the shop of the chain, the birth date of the buyer is recorded based on statement at the cash desk and according to another complaint by requiring the presentation of an ID card with photograph, even if the buyer was aver 18 years of age. According to another complaint, the cashier was unable to provide information on the purpose and legal basis of recording the data, while the regional manager notified the shop manager that the recording of the data of the ID card was not necessary, if the buyer's being of age could be established in other ways; however, buyers were not informed about this fact. A notifier complained that he was visibly over the age of 70, yet he had to verify his age. As alleged by the notifiers, privacy notices were not handed over to the data subjects even if they requested them, and the cashiers did not have them, hence the legal basis of processing and its duration was not known in relation to the recording of the birth date.

The Authority launched an authority procedure for data protection ex officio in relation to the processing complained against and carried out onsite inspections without prior notice in the shops of the controller on two occasions. In the course of the inspection, the Authority saw processing practices confirming the complaints and it was established that there was no accessible privacy statement on the site of the data collection when requiring the presentation of an ID card and recording the birth date.

Following the launching of the authority procedure for data protection, the controller terminated the practice of requiring the verification of the birth date uniformly from all those purchasing alcoholic drinks.

As the legal basis of processing, the controller identified Section 16/A(1) and (4) of Act CLV of 1997 on Consumer Protection as a legal obligation applicable to it, according to which prior to the purchase of alcoholic drinks "*the undertaking or its representative, in case of doubt, shall ask the consumer to provide credible proof of his/her age*". As opposed to that, the Authority found that, contrary to the processing required by the law, the controller went beyond it by requiring its employees working as shop assistants to mandatorily check the age of every person wishing to buy any alcoholic drink not only in the case of doubt, but in general. In the course of the procedure, it was also established that the birthday recorded by the staff of the controller was used by the point-of-sale system not only to calculate the age of the buyer, but it was also stored as part of the log files for 180 days and the processors of the retail chain also had access to it.

In its decision, the Authority established that the processing practice of the retail chain infringed the principles of transparency and data minimisation according to Article 5(1)(a) and 5(1)(c) of the General Data Protection Regulation, Articles 12-13 of the General Data Protection Regulation in the context of informing data subjects; it failed to verify a legal basis according to Article 6 for processing and, furthermore, it failed to apply data security measures compliant with Article 32(1) and (4) in the course of processing.

On the grounds of the established infringements, the Authority ordered the retail chain to pay a data protection fine of HUF 95 million, to review its age verification practice and to display a privacy notice with regard to processing carried out at its premises. *(NAIH-6989/2022, NAIH-3227/2023)*

4. Violation of data subjects' rights in relation to querying vaccine registration (vakcinareg.neak.gov.hu)

The Petitioner stated in his petition that he noted that the National Health Insurance Fund Manager (hereinafter: Obligee) "published" the information that the Petitioner registered for the vaccine against Covid-19 on the website https://vakcinareg.neak.gov.hu. By providing the social security number and the birth date, anyone who knows these data may query the validity of the data subjects' registration on the Obligee's site. On 25 March 2021, the Petitioner objected to the processing of his personal data on a website by sending a simple e-mail to the Obligee; however, he did not receive any answer at all from the Obligee.

Because of this, the Petitioner sent an e-mail again to the Obligee, including the antecedents and he stated in that e-mail that he wished to exercise his right of

access according to Article 15 of the General Data Protection Regulation concerning which IP addresses queried the fact of his vaccine registration. The Petitioner still received no answer from the Obligee. In view of this, the Petitioner requested the Authority to conduct an authority procedure for data protection and asked the Authority to establish the infringement by the controller, order it to provide the information it had to do, order it to take his right to object into account and to terminate the accessibility of his personal data on the Internet, once the period open for responding according to the General Data Protection Regulation expired.

In order to clarify the facts of the case, the Authority sent an order to the Obligee but received no answer. In doing so, Obligee obstructed the investigation of the case and failed to inform the Authority of the reason for the delay and when an answer of merit could be expected. The Authority repeatedly called upon the Obligee to clarify the facts of the case and expressly called its attention to the possible legal consequences of the omission. The Obligee verifiably received the repeated order, yet failed to comply with it. In view of this, the Authority imposed a procedural fine of HUF 250,000 on the controller in its order.

As the Obligee continued to fail to meet its obligation to clarify the facts of the case, and it failed to pay the procedural fine despite the above, the Authority carried out an onsite inspection at the registered offices of the Obligee. In the course of the inspection, by way of examining the electronic information system of the Obligee and test querying, it was found that the Obligee logged the data requests through its query interface in accordance with its published privacy notice and had the data concerned in the access request of the Petitioner.

Based on this, the Authority established an infringement of Article 12(3)-(4) of the General Data Protection Regulation. The Authority rejected the rest of the Petitioner's petition because he sent his requests to the Obligee for exercising his data subject rights in an unidentifiable manner, by simple e-mail; however, according to the information sent by the controller as a result of the Authority's procedure, the Petitioner could now submit his data subject request in accordance with the Obligee's procedures in a manner suitable for identification and exercise his data subject rights, so in this respect his rights were not violated.

Based on the above, the Authority also established that the Obligee – irrespective of whether it regarded the request received as an access request according to Article 15 of the General Data Protection Regulation – should have evaluated

the request in merit and with the content according to Article 12(4) within the period open for this according to paragraph (3).
In clarifying the facts of the case, the Authority investigated ex officio the information provided to data subjects when registering on the website vakcinainfo.gov.hu, the Privacy Statement on the Obligee's website and the Privacy Statement accessible on the query interface concerned in this case. Neither of these Privacy Statements included information on how data subjects can identify themselves to the Obligee controller in the course of exercising their data subject's rights, nor did they state that they would not answer requests received from unidentified data subjects. In view of this, the Authority established ex officio the infringement of the principle of transparency according to Article 5(1)(a) of the General Data Protection Regulation.

In addition, the Authority also established ex officio that the Obligee failed to meet its obligation to cooperate according to Article 31 of the General Data Protection Regulation because of the deficiencies of its internal organisation by failing to provide the information requested to be enclosed in the course of the inspection conducted by the Authority and on that basis imposed a data protection fine on the Obligee to an amount of HUF 500,000. *(NAIH-6484-2/2022)*

5. Processing by fuel stations related to reading the barcode on vehicle registration certificates

According to notifications received by the Authority, a fuel provider read the barcode in the vehicle registration certificate and recorded it in its system at its fuel stations selling fuel at official prices. According to press reports, the service provider, in addition to establishing the entitlement to buy fuel at official prices and verifying the lawfulness of the sale in the course of an eventual tax audit, also stored the data in order to restrict the quantity of fuel available at official prices in the network of fuel stations and to monitor the quantity purchased in its national network of fuel stations. There was no Privacy Statement available to the data subjects on processing at the fuel stations; according to one complaint, staff at the fuel stations was unable to provide even oral information on the purposes and most important characteristics of the processing. Based on the notification, the Authority launched ex officio investigations and contacted the largest fuel station networks operating in Hungary.

In addition, the Authority published a communiqué concerning processing[3] in which it addressed the obligation of controllers to provide appropriate preliminary information to data subjects and the restricted extent of the mandatory processing required by the legal regulation on official fuel prices.

The Authority found that the fuel stations failed to provide appropriate preliminary information to the data subject even though they carried out processing subject to GDPR through inspecting the registration certificates and recording their barcodes. However, as Section 1/A of Government Decree 94/2022. (III. 10.) on the different application of Act CXXX of 2021 on Certain Regulatory Issues Related to the Emergency Situation lost its effect on 6 December 2022, the obligation to process data required by it ceased, data are no longer collected, thus the Authority, in addition to establishing the infringement, terminated the procedures because of the elimination of the circumstance giving rise to the procedure. *(NAIH-7020/2022, NAIH-7081/2022, NAIH-7082/2022, NAIH-7083/2022, NAIH-7084/2022, NAIH-7085/2022, NAIH-7086/2022)*

6. Obligation to verify identity in pharmacies

The notifiers objected to processing by various pharmacies, according to which the issue of medications on electronic prescriptions via the e-recept system was subject to the joint presentation of an official certificate suitable for the verification of identity, the social security card and the address card. In view of Section 20/A(1) of Decree 44/2004 (IV.28.) ESzCsM on the prescription and issue of medications for human use, the processing of personal data related to the issue of medications in the case of electronic prescriptions is mandatory processing. With regard to these notifications, the Authority established that processing has the appropriate legal basis, thus provided that appropriate information is provided on the processing, rights are not breached. In view of the number of such notifications, the Authority published general information[4] on its website among the data protection statements. *(NAIH-5678/2022)*

7. Data protection issues of the organised postal replacement service

3 https://www.naih.hu/dontesek-adatvedelem-tajekoztatok-koezlemenyek?download=545:a-nemzeti-adatvedelmi-es-ia-hatosag-kozlemenye-az-uzemanyagtolto-allomasok-forgalmi-engedelyen-szereplo-vonalkod-leolvasasahoz-kapcsolodo-adatkezeleserol

4 https://www.naih.hu/adatvedelmi-allasfoglalasok/file/531-szemelyazonossag-igazolasanak-kotelezettsege-gyogyszertarban-veny-recept-kivaltasa-soran

The Authority was requested to make a statement concerning the lawfulness of processing by NGOs providing “postal replacement point services” on account of the closure of certain post offices.

The Authority stressed that the service provider at the post replacement point has to be able to determine based on the actual activities, which person or persons (the NGO or its certain members) carry out processing activities with regard to the service, and whether the individual persons carry out the tasks of the controller, joint controller or processor with regard to processing. Guidelines 07/2020 on the concepts of controller and processor in the GDPR of the European Data Protection Board may assist with this. In relation to the issue of authorisation with regard to the procedure and the provision of the service, personal data are processed, hence the provisions of GDPR are applicable. The Authority stated that the controller is responsible for providing appropriate information to the data subjects on the processing activity. *(NAIH-8866/2022)*

8. Processing by accommodation service providers related to the scanning of documents

The Authority received several notifications from data subjects, who complained that to be allowed to use accommodation, the service provider asked them for their ID cards and their official certificate verifying their personal identification number and address, of which they make copies. The Authority informed the notifiers that Section 9/H(1)-()2) of Act CLVI of 2016 on the Public Tasks of the Development of Tourist Regions requires accommodation service providers to carry out processing, i.e. they have to record the data of the persons using the accommodation service for a purpose specified by the law under storage space provided by the hosting provider designated in the Government Decree.

In relation to the recording of the data, the Authority also called attention to the provisions of the Government Decree, according to which “*the accommodation service provider shall record the data of the document suitable for the verification of identity in the accommodation management software through the document scanner. Data whose recording is not possible via the document scanner can be manually recorded by the accommodation service provider in the accommodation management software. If, in addition to the data of the document suitable for the verification of identity, the scanner also records the image of the document, the accommodation management software shall immediately erase the image data of the document.”*

The Authority called the attention of the notifier to the fact that the legal regulation does not create a legal basis for the accommodation provider to make copies of the documents presented or to process the copies of the documents. *(NAIH-6291/2022)*

II.1.7. Recommendations issued by the Authority

In relation to certain problems, the Authority turned to the legislator and made recommendations to settle detrimental situations.

1. Employee witnessing on financial contracts

A notifier complained to the Authority that a bank compels its employees to be witnesses to contracts, which are handed over to clients and the documents show their names and addresses. The notifier presented that over the past years, several employees requested the bank to have the address of the registered offices/branch of the bank displayed on these documents instead of their home addresses, however, the bank disallowed these employee requests.

In its statement, the bank presented that for the vast majority of contracts concluded by the bank or statements needed at the bank, the address of the bank branch and the number of the employee's certificate suitable for identification suffice on bank documents to be signed by two witnesses; however, there are certain exceptions. The relevant legal regulation sets out as a dispositive rule that the contract concluded by financial institutions and their clients qualifies as a private deed of full probative force, even if the witness is an employee of the financial institution and, instead of his place of residence or stay, the address of the employer (registered office or branch), and the type and number of the official certificate suitable for identification are show on the private deed.

In view of the principle of data minimisation, the Authority initiated an amendment to the legal regulation at the competent ministry, recommending that when an employee witnesses contracts of a financial nature showing the bank identifier, which –similarly to a certificate issued by an authority – is a unique identifier consisting of letters and/or numbers on the basis of which the employee concerned is uniquely identified and registered in the bank's system, should suffice for identification. In addition, the legal regulation should specify as a cogent rule that the employee should not enter either his own or the employer's address when witnessing documents, but only the employer's address on the documents. (*NAIH-4008/2022*)

2. Exercise of data subject's rights with regard to the eKRÉTA system

In a case related to education, the mid-term history assessment of a primary school child, who is the petitioner, changed in the second term in the eKréta system. The child and the child's parents would have liked to learn from the school who modified the mark retroactively and when, but the school told them that they were unable to disclose this to them as they did not have this information either. The procedure found that the institution indeed did not have the requested information, the data were located in the log files of the company operating the eKRÉTA system (the processor). However, the company erroneously informed the school that these data were not available to them and later on, only after lengthy correspondence with the operator, was it able to provide information on who and when the child's mid-term assessment was changed retroactively.

The Authority made a recommendation to the ministry in charge of public education because of the practice of eKRÉTA Zrt., according to which the operator provided access to the data stored in its system only after lengthy and contradictory statements and not to the processor institution of public education. In its recommendation, the Authority requested to clarify that irrespective of the form of operation, when it comes to the exercise of data subject's rights, it is the responsibility of the processor institution to ensure the exercise of data subject's rights and not of the operator, for which the processor has to provide assistance to be regulated by a contract or other legal act according to Article 28 of the General Data Protection Regulation. In addition, the information on processing must be adjusted to the above requirements, taking into account the fact that children are concerned and it has to extend to the mode of the enforcement of data subjects' rights. (*NAIH-7667/2022*)

3. *Recommendation to amend a legal regulation in relation to the registration of the personal data and the residential addresses of citizens*

The Authority put forward a recommendation to amend the legal regulation concerning the registration of the personal data and residential addresses of citizens in order to clearly ensure the authorisation of the Authority to access the data of the registry even on the basis of fragmented or deficient data with a view to be able to investigate every notification in merit. Based on the recommendation, the Act on the Registration of the Personal Data and Residential Addresses of Citizens was amended, authorising the Authority to request the data in the registry. (*NAIH-3424/2022*)

4. Processing of children's coronavirus vaccination records in schools

In the spring and also in September 2022, the Authority received several notifications about the fact that the institutions of public education collected the data of children in a legal relationship with the given institution concerning their vaccination against SARS-CoV-2 coronavirus (hereinafter: coronavirus) without indicating an express legal requirement. Based on the notifications received by the Authority, the mode of data collection was not uniform – teachers requested that the health-related data are sent to their private e-mail addresses, or through the messaging application of a community website, moreover, even the oral statements of minor students in front of their classmates were solicited on whether they were vaccinated.

The investigation found that issues related to the processing were not regulated, hence the Authority made a recommendation to the Ministry of the Interior in charge of public education and health care and therefore empowered to legislate in relation to public education and healthcare and to issue regulatory instruments for the organisations under public law. The Authority has taken the initiative that the Ministry specify the public task of institutions of public education, which may create a legal basis for processing in relation to the assessment of the vaccination status and elaborate detailed rules of processing related to protection against the epidemic in line with data protection principles and data security requirements, as well as uniform procedures to be followed by institutions of public education with a view to avoiding breach of rights.

In its response, the Ministry informed the Authority of its acceptance of the recommendations and stated that by inserting Sections 74/Q-74/S into Act CLIV of 1997 on Healthcare in December 2022, it settled the purpose and period of storing health-related data related to the verification of vaccination against a possible future infectious disease, the range of persons authorised to access the data, the mode of data collection and the related requirements to provide information. *(NAIH-2880/2022)*

II.2. Procedures related to the processing of personal data for the purposes of law enforcement, defence and national security (procedures subject to the Privacy Act)

II.2.1. Investigation of the Szitakötő (Dragonfly) system

The goal of the Dragonfly project was to set up and operate a video surveillance system for the intensive and mass surveillance of persons in public areas, traffic participants, those travelling by public transportation and those using banking and financial services, in every settlement of the country, organised into a single centralised system. The Authority provided its opinion on the package of laws concerning the amendment of certain acts on internal affairs and related acts, which laid the foundation for the implementation of the Dragonfly project by amending several acts in 2018.

One of the important elements of the project was the continuous collection of images from 35,000 cameras in operation or to be put into operation in the country in a single central depository, so that the controller is not the organ operating the central storage space, but the organisations required to upload the video files. The hosting provider only played the role of processor in processing the huge volume of image data for monitoring purposes. Primarily, Sections 73/A-E of Act CCXXII of 2015 on the General Rules on Electronic Administration and Trust Services (Electronic Administration Act) provides for this, but several acts (such as the Police Act, the Act on Public Area Supervision, the Asset Protection Act, the Act on Road Traffic) contain related rules following the amendment enacted in 2018.

The Authority launched the investigation of the project ex officio based on Section 51/A(1) of the Privacy Act in 2021 and closed it in 2022. The goal of the investigation was to explore how processing at the central depository operates in practice, how data processing is carried out and what opportunities and rights the individual actors have in the course of processing. Another goal was to examine whether all this is in line with legal regulation in force and whether the data protection safeguards specified therein are implemented.

The audit was carried out based on the answers given by the organ subject to the investigation to the questions posed in advance in writing and by conducting onsite investigation involving the following organisations:

- NISZ Zrt.
- GVSX Kft.
- Budapest Police Headquarters (BRFK)
- Policing Directorate of the Municipality of Budapest (FÖRI)
- Budapest Közút Zrt.

As the operation of the system subject to the investigation is closely related to the Integrated Traffic Management and Regulatory System (IKSZR), to avoid confusion, it is important to clarify that currently the term “Dragonfly System” is used to refer to the operation and processing of a copy of IKSZR by NISZ Zrt. and the Governmental Data Centre (KAK

IKSZR was developed by GVSX Kft. and used first by Budapest Közút Zrt., while it was run by GVSX Kft. Initially, Budapest Közút Zrt. used IKSZR for traffic management, e.g. (with many other functions) to operate variable message boards (VJT). The operation of the VJTs (in certain traffic junctions, for information purposes, they display how long it takes to reach the next junction under the current traffic conditions) is based on number plate recognition. In practice, the way this works is that the software selects a car, detected at both junctions in question and then calculates the time between the two detections. According to the information received, a user cannot obtain data on number plates in the course of this type of IKSZR usage. The basis of IKSZR operation is the 188 number plate recognition and 300 scan cameras installed in Budapest by Budapest Közút Zrt., which monitor road traffic.

Currently, in addition to Budapest Közút Zrt., BRFK, FÖRI and NISZ Zrt. also have a copy each of IKSZR, each of which is operated by GVSX Kft. In June 2017, Budapest Közút Zrt. entered into a contract with FÖRI, providing the right of use for the basic component of IKSZR and subsequently for its further development. In 2019, BRFK concluded an agreement with FÖRI that is how they have been able to access the data files ever since.

Currently, these four organisations have access to the centrally stored data using the camera images and metadata generated in IKSZR. According to their statements, these organisations exercise their right to use the complex system independently of one another. In every case, the data source includes the images of a total of 488 cameras, which are first sent to the servers of Budapest Közút Zrt., then to their office of Szabó Ervin tér where they are mirrored and forwarded to the other three organisations.

The Dragonfly system was established by a public procurement procedure at NISZ Zrt. in November 2019; in actual fact, however, it has only been operational since 1 February 2022, for which NISZ Zrt. provides the infrastructure (storage space and server capacity), and GVSX Kft. has an exclusive right of operation and further development. Incoming images are recorded and stored for 30 days.

Currently, based on an agreement, BRFK uses the IKSZR copy purchased by FÖRI, developed and operated by GVSX Kft., for number plate monitoring. For this, they use the images of approximately 188 number plate monitoring cameras operated by Budapest Közút Zrt. BRFK regards itself as the controller in this processing, which is reflected also by the agreement concluded with FÖRI, as well as the related BRFK measure.[5] Hence, processing carried out by BRFK is not part of the Dragonfly system. Although it was raised that BRFK might also use the IKSZR copy of NISZ Zrt., based on a study of the legal environment in force, BRFK, however, arrived at the conclusion that for the time being they do not have the possibility to use it in compliance with the Electronic Administration Act, and the system they use meets the needs of their current tasks. As no agreement was signed, BRFK currently uses only the IKSZR copy of FÖRI.

The investigation revealed that the Dragonfly system in its current form is far from fulfilling the role or performing every function, for which it was established according to the original plans. One, but not the only, reason for this is that the legal regulation (which is incidentally not flawless from a data protection point of view) is far ahead of technical implementation.

The relevant legal regulations in force would enable the implementation of all that the Dragonfly project was about – i.e. channelling all the area surveillance cameras and other image recording cameras (used by banks, public transport, etc.) to the Dragonfly system operating in KAK. According to the Electronic Administration Act:

Section 73/A(1) An organ designated by the Government in decree (hereinafter: storage provider) shall ensure the storage of image, sound and audio-visual recordings (hereinafter: recording) produced by

5 BRFK measure 37 (IX.2) on the rules related to the application of the policing module of the Integrated Traffic Management and Regulatory System

a) road operators,
b) the police in the course of traffic policing measures,
c) image recorders deployed by the police,
d) image recorders deployed by a public space supervisory authority,
e) entities pursuing personal and property protection activities for the protection of private areas open to public, or entities providing financial services or supplementary financial services that are necessary for their tasks,
f) a service provider within the meaning of Section 8(1) of Act XLI of 2012 on passenger transport services,
g) toll collectors within the meaning of the Act on toll to be paid for using highways, motorways and the main roads proportionate to the distance travelled (hereinafter: jointly "mandatory central storage user")
by providing information technology applications and central storage space

(2) The storage provider shall ensure the storage of data recorded by the service provider referred to in Section 16/A(e) of the Act on the Local Governments of Hungary by means of providing information technology applications and central storage space.

(3) The activities of the storage provider shall be limited to storing recordings and data at its central storage space and providing the information technology application specified in Section 73/B; it may not access or perform any data processing operation with any recording or data stored at its central storage space.

(4) Mandatory central storage users shall cooperate with the storage provider as required under a Government Decree and where the conditions laid down in a Government Decree are met, they shall use the central storage space provided.

(5) Mandatory central storage users may use the central storage space under terms and conditions laid down in the Government Decree referred to in paragraph (4).

However, the Government Decree referred to in paragraphs (4) and (5) has not been drafted to this day, hence the regulatory environment is not in place for using the central storage space. The absence of a Government Decree defining the conditions for data processing is a fundamental obstacle to the operation of the Dragonfly system. This is also the reason why only the camera images of Budapest Közút Zrt. are now channelled to KAK.

From a legal point of view, another condition of operation would be the amendment of Decree 7/2013. (II.26.) NFM on organisations using centralised IT and electronic communication services based on individual service agreements and IT system operated or developed by the central service provider, which would take care of the designation of the operator.

However, more is missing from an IT point of view; according to the information available to the Authority, technical conditions are not in place for the processing of such an enormous volume of data: there is not enough server capacity, which would be sufficient for the storage and processing of the gigantic amount of incoming camera images. In addition, it is also a fact that, precisely because of the gigantic server capacity requirements needed to run such systems, currently technical development is moving towards the use of the so-called 'embedded' endpoint analytics usage running as a shared resource on the image recording device.

All in all, it can be established that the concerns formulated by the Authority in the course of the preparation for legislation have not been settled in a reassuring manner. The concerns of the Authority were primarily related to the disorganised nature of the conditions of processing, to the fact that it was unclear what organ would have what responsibilities, which will in fact have disposal over processing and whether it is possible to have several entities disposing over the same data in parallel. (*NAIH-4790/2022.)*

II.2.2. Unlawful processing of personal data in a decision made by a police station in the course of a criminal procedure

Upon request, the Authority conducted an authority procedure for data protection with regard to personal data shown in a decision brought in a criminal procedure and communicated by means of the decision. In the course of the criminal procedure conducted against the Petitioner, the Petitionee send a decision to 18 addressees, including 16 natural persons – 14 persons with name and address, and 2 persons with name only –in the decision. In this way, the addressees were informed of one another's names and addresses. The natural persons listed in the decision were the injured parties to the criminal procedure, while the Petitioner was the subject of the investigation and, subsequently, the accused. The Petitioner also objected to the fact that the decision included his place of stay (abroad) established in the course of the procedure.

The Petitioner's representative requested the Petitionee to amend the decision because according to his position it failed to comply with the provisions of the Privacy Act and the rules applicable to the Petitionee under Instruction 39/2019. (XI. 19.) ORFK. Based on Section 17 of the Privacy Act, he also requested information as to what was the purpose and legal basis of forwarding his place of stay to the addressees; furthermore, whether it was forwarded to persons other than the addressees and requested information whether there was any data breach in relation to these personal data and as to what data subject rights the Petitioner is entitled to.

According to the Petitioner's position, by its procedure as described above, the Petitionee violated the principle set forth in Section 4 of the Privacy Act, the disclosure of his place of stay in the decision went beyond the necessity and expediency of identification, hence it violated the principle of purpose limitation. He also requested an evaluation whether the Petitionee lawfully forwarded the data of his place of stay in the decision to the addressees. He also complained that the Petitionee did not adequately ensure his right of access and pointed out that the rights of the parties to the procedure were breached by the communication of the decision.

Enforcement of the Petitioner's access right:

The Authority found that the Petitionee infringed the Petitioner's right to access by failing to answer all of the Petitioner's questions in relation to it. Its answer did not include whether there was a data breach concerning the Petitioner's personal data, it did not make a statement on who else the personal data of the Petitioner were forwarded to, and cited a non-existent legislation – *Section 363(1)(d) of the Code of Criminal Procedures* – as legislation laying the foundation for the content of the decision.

Showing the personal data of the addressees in the decision and failure of confidential processing

Showing the name and delivery address of the addressee (excluding the name of the Petitioner) in the decision violates the principle of purpose limitation because showing these is absolutely unnecessary, it could only have administrative reasons. The Authority established that it would have been appropriate to include the delivery data of the addressees (name and address) in a separate delivery clause.

In the course of the procedure, the Authority ex officio noted that the Petitionee indicated the name of an injured party in the decision, who requested the confidential processing of all his personal data, including his name in the course of his witness hearing. It was also found that the minutes of the witness hearing among the documents of the investigation also included the name and signature of the witness requesting confidential processing of his personal data. Through this, the Petitionee failed to process the personal data of the witness in accordance with the request of the data subject and the relevant data protection rules of the Code of Criminal Procedures, including the provisions of its Sections 99[6], 100 and 102.

The Petitionee disregarded the motion for confidential processing in the case of one data subject aggrieved party by negligence. At the same time, the Authority took into account that only his name and signature was disclosed to the Petitioner and the Petitioner's representative from the minutes of the hearing and the decision. Because of the nature and the circumstances of the criminal act, of which he was accused, the Petitioner had to know the name of this data subject aggrieved party. The case documents reveal that the Petitioner and the aggrieved party were personally known to one another, they had met earlier, in the course of which they entered into a contract under civil law in writing. In response to the Authority's question, the Petitionee declared that the other parties to the proceedings did not get to know one another and the aggrieved parties' data set forth in the decision and only the Petitioner and his representatives had access to the case documents.

A data breach was established, which did not qualify as being of high risk. The Authority pointed out that with the exception of the data subject, who requested the confidential processing of all his personal data, no data were transferred,

6 *Pursuant to Section 99(1) of the Code of Criminal Procedures, the investigating authority shall order upon a motion the name, birth name, place and date of birth, mother's name, nationality, ID number, home address, contact address, the actual place of residence, service address, electronic contact details of the aggrieved party to be processed confidentially (hereinafter: confidential data processing). On Section 99(6) of the Code of Criminal Procedures, the investigating authority shall ensure that no confidentially processed personal data may become known based on any other data of the proceeding. Pursuant to Section 102(1) of the Code of Criminal Procedures, the investigating authority shall handle case documents specified in this act confidentially and separately from other case documents. According to Section 102(3), if a case is handled confidentially, the investigating authority shall ensure*

a) that the case document handled confidentially or its content is not revealed in other case documents or data of the proceeding,

b) the inspection of case documents in such a manner that prevents case documents handled confidentially from being revealed.

which the aggrieved parties and the Petitioner would not have had access to in the course of the criminal proceedings[7].

The Authority partially upheld the request and established the infringement of the principles of data minimisation and purpose limitation, because the decision unnecessarily contained the Petitioner's delivery address. Furthermore, the Authority ex officio established that the decision unnecessarily contained the names and delivery addresses of the aggrieved parties.

In accordance with Section 61(1)(b)(ba) of the Privacy Act, the Authority also established ex officio that the Petitionee unlawfully processed the personal data, violating the data security requirements, by including the confidentially processed data of the witness in the decision and not ensuring the confidential processing of the data of the data subject aggrieved party/witness in the minutes of the hearing.

Transferring the data concerning the Petitioner's place of stay to the addressees:

In view of the fact that the Authority did not receive any evidence to the contrary in the course of the clarification of the facts of the case, the Authority accepted the Petitionee's statement substantiated by a document, according to which the decision was delivered to nobody else but the representative of the Petitioner.

At the same time, the Authority found that according to its original intention, the Petitionee wished to deliver the decision without any legal basis to the addressees shown on it. The argument of the Petitionee that the decision contains direct provisions also for the other addressees other than the accused is obviously erroneous. There is no doubt that the aggrieved parties have a right to be informed of the course of the criminal proceedings, however, in this regard the delivery of the decision providing for the continuation of the suspended investigation would be warranted. Section 397(2) of the Code of Criminal Procedures requires this, and only this, as a separate obligation of communication. Here it is necessary to invoke the relevant part of the commentary to the Code of Criminal Procedures:

"As a main rule, a decision shall be served on those who are directly affected by one of its provisions. Being directly affected must be stated by the introductory part; the decision itself contains to whom its provisions apply, thus for instance a decision concerning the advance payment of the fee for a defence attorney concerns the defence attorney, the decision extending the period open for the investigation against him concerns the accused, a decision rejecting a motion concerns directly the maker of the motion, while the decision ordering unification, separation or transfer does not affect a person directly involved in the criminal proceedings. Exceptions from the main rule of the communication obligation can be divided into two groups; in the first one, the decision may not be communicated to the person concerned, even if a provision directly applies to him, thus for instance in view of Section 250 of the Code of Criminal Procedures, communication of a permit to apply covert means is excluded to the person concerned in the permit. In the other one, the decision is to be communicated also to those who are not directly affected, which may be based on general provisions, such Section 42(3) of the Code of Criminal Procedures, a decision communicated to the accused shall also be communicated to the defence attorney based on Section 72(2), a decision communicated to the defence attorney shall also be communicated to the legal representative of the accused, but the Code of Criminal Procedures specifies communication obligations also in relation to certain decisions, such as in the case of Section 350(2) for transfer, Section 381(2) for the dismissal of a criminal report, Section 397(2)-(3) for the suspension of proceedings and Section 401 for the termination of proceedings, which provide for who is to be served with the decision on the given issue."

At the same time, according to the position of the Authority, the recording of the Petitioner's place of stay abroad in the decision is warranted in view of Section 393(4) of the Code of Criminal Procedures. It qualifies as a significant fact established by the investigating authority because it was on this basis that the arrest warrant was withdrawn and the continuation of the investigation was ordered.

According to the Authority's position, in this respect the fact that the accusation was not communicated to the Petitioner when the decision was made – obviously because he was staying at an unknown place – has no decisive significance. In contrast to the law currently in force, the Code of Criminal Procedures then in force did not yet include a person under the suspicion of committing a crime as a person involved in the criminal proceedings; however, the introduction of this role – as revealed by the justification of the law in force – was in line with previous legal practice.

In this respect, the Authority rejected the request.

7 *According to Section 100 of the Code of Criminal Procedures*

Legal consequences:

Based on Section 61(1)(b)(bf) of the Privacy Act, the Authority called for supplementing the information provided to the Petitioner by the Petitionee, adding whether a data breach took place and to whom the decision was communicated. Based on Section 61(1)(b)(ba) of the Privacy Act, the Authority found that the Petitionee infringed Section 4(1)-(2) and (4a) of the Privacy Act by unnecessarily recording the names and delivery addresses of the natural person data subjects as aggrieved parties and the delivery address of the Petitioner in the decision without a lawful purpose. Also, based on Section 61(1)(ba) of the Privacy Act, the Authority ex officio established that by omitting to comply with the relevant security requirements in the course of its proceedings, the Petitionee infringed Section 25/I of the Privacy Act as it failed to ensure the security of the confidentially processed personal data of the witness.

Based on Section 61(2)b) of the Privacy Act, the Authority also ordered the publication of its decision together with the identification data of the Petititonee. The Petitionee complied with the provisions of the Authority's decision and supplemented the information provided to the Petitioner upon his access request. *(NAIH-462/2022)*

II.2.3. The issue of access to psychological opinions on prisoners in penitentiary institutions

Upon request, the Authority carried out an inquiry against a penitentiary institution (hereinafter: Penitentiary) on the exercise of the right of access to psychological opinions on the notifier.

The Notifier requested the Health Department of the Penitentiary to issue the psychological opinions and reports made on him by the psychologists of various penitentiary institutions over the preceding five years. According to the response of the Health Department sent to the Notifier, the health-related documents of the Notifier did not include any psychological report. According to the position of the Notifier, psychological opinions were drafted on him on an ongoing basis, that is why he wished to learn from the psychologist of the Penitentiary how he could request to see these and from what organ. According to him, the psychologist acknowledged the existence of these opinions, but informed him verbally that they would not be issued to him as he was not entitled to have access to them.

In penitentiary institutions, the activities of psychologists related to the detainees are regulated by Act CCXL of 2013 on the Execution of Sentences, Measures, Certain Coercive Measures and Detention for Misdemeanours (hereinafter: Bvtv.) and Decree 16/2014 IM on the detailed rules of the execution of imprisonment, detention, pre-trial detention and detention in lieu of a fine (hereinafter: IM Decree), Act CLIV of 1997 on Healthcare and Act LXXXIV of 2003 on Certain Issues of Performing Healthcare Activities. Act CVII of 1995 on Penitentiary Organisation also includes rules affecting data processing while executing a sentence (hereinafter: Bvsztv.). According to the practice of the Penitentiary subject to the inquiry, a psychological opinion is drafted upon the admission of a detainee; if it was already prepared in another Penitentiary, then the receiving penitentiary reviews it and supplements it, if necessary. Such reviews were carried out on several occasions in the case of the Notifier.

The Penitentiary investigated by the Authority declared that it has health-related and other documentation (psychological review opinion) only for the period of detention in the penitentiary. The detention of the Notifier in the Penitentiary ceased after his request and his health-related and detention-related documents were sent to the penitentiary organisation currently detaining him, so following his transfer, the Penitentiary no longer processed any psychological opinions or other health-related data on the Notifier, according to their statement. As stated by the penitentiary, the central registry is accessible to all the authorised members of penitentiary institutions, but only with a view to discharging their official duties; the central registry logs any querying of data, so any processing can be subsequently audited. According to their position, as a former institution detaining the person, they were no longer authorised to query the central registry in the absence of an official duty.

Access to the documents subject to the inquiry is excluded by Bvtv. Section 26(4)(a) and (b), in view of the fact that the right to access does not extend to drafts supporting decision-making and the risk assessment summary report. According to Bvtv. Section 26(4)(h), the right to access does not extend to documents to which the Petitioner is not entitled by law to have access.

The reasons for drafting a psychological opinion include preparing for a decision concerning appropriate accommodation, ensuring the security of detention and the risk assessment of detainees.

Pursuant to Section 29(1) of the IM Decree, the penitentiary develops and operates a Risk Assessment and Management System (hereinafter: KEK system) specified in Bvtv. Section 82(3) with a view to assessing the recidivism and detention risk of convicts, the mitigation of such risks and the facilitation of successful reintegration into society. Pursuant to Section 29(3) of the IM Decree, risk analysis is a professional activity of penitentiaries, in the course of which the risk value of the risk groups specified in this decree are assessed and evaluated with regard to the convict. Pursuant to Section 29(6) of the IM Decree, the convict is obliged to cooperate in the course of the procedures assessing the risks of recidivism and detention.

According to Bvsztv. Section 30(3), the detainee may not have access to data affecting the security of detention generated in relation to measures, which the detainee is required to tolerate by force of legal provision. When released from the penitentiary, the detainee may have access to these data – upon request – with the exception of classified data. Pursuant to paragraph (4), the detainee's right to have access to his data may not jeopardise the enforcement of public interest in the use of data required for the operation of law enforcement and judicial organs and the performance of public and municipal tasks.

According to Bvsztv. Section 30(1), the penitentiary and the organs, organisations and citizens requesting information on the detainee's data may use such data exclusively for the lawful discharge of their duties specified in legal regulation and the enforcement of the right mentioned in the request. With regard to the processing under investigation, the legal basis for processing is created by Bvsztv. Section 28 and Bvsztv. Section 76. The legal provisions concerning processing in the course of detention in a penitentiary and access to these data contain special rules relative to those in Act XLVII of 1997 on the Processing and Protection of Health and Related Personal Data. Pursuant to Section 17(3) of the Privacy Act, the controller may restrict or reject, proportionately to the desired objective, the enforcement of the data subject's right to access, if this measure is absolutely necessary for securing an interest specified in Section 16(3)(a)-(f).

At the time of the submission of the request, the detaining penitentiary as controller should have refused to provide information on the psychological opinion as personal data under the right of access based on Section 17(3) of the Privacy Act with reference to the relevant point of Section 16(3) of the Privacy Act, or if it assesses the request after the detainee is transferred, it should inform the notifier of the identity of the organ authorised to fulfil or reject the request (the current detaining institution). Bvsztv. Section 30(3) and (4) as referred to above create the legal basis for rejecting the provision of information.

With regard to the processing of personal data for law enforcement purposes, the Privacy Act transposes Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and on the free movement of such data and repealing Council Framework Decision 2008/977/JHA (hereinafter: Law Enforcement Directive) into Hungarian law. This means that processing for law enforcement purposes is subject to the scope of this Directive. Under Recital (39) of the Law Enforcement Directive in order to enable data subjects to exercise their rights, any information to the data subject should be easily accessible and easy to understand using clear and plain language. Such information should be adapted to the needs of vulnerable persons.

Based on Recital (40), modalities should be provided for facilitating the exercise of the data subject's rights, including mechanisms to request and, if applicable, obtain, free of charge, in particular, access to and rectification or erasure of personal data, and restriction of processing. Detained person qualify as a vulnerable group in terms of information provided to them and access to information.

The response of the Penitentiary, according to which the health-related documents of the notifier did not include any psychological records, suggested that such documents were not drafted on him in relation to his detention and such documents were not accessible either in the Penitentiary or in the central registry. Furthermore, the response kept quiet about the fact that according to the relevant legal provisions, these personal data are not accessible to the data subject during their period of detention.

The Authority established that the processing by the Penitentiary infringed Section 14(b) and the provisions of Section 17 of the Privacy Act as it failed to fulfil the request and did not delay, restrict or waive the fulfilment of the request citing the conditions according to Section 17(3) of the Privacy Act and with content according to paragraph (4) and it failed to provide transparent information about the fact that these data were no longer processed by the Penitentiary, but the penitentiary, which subsequently detailed the data subject and they are contained in the central registry, which is authorised to assess the request.

Based on Section 56(1) of the Privacy Act, the Authority called upon the Penitentiary to respond to the data subject's access request in accordance with the provisions of Section 17(3) of the Privacy Act and, if it is not authorised either to query the requested data on the data subject from the central registry or to reject the request, provide information to the data subject on the identity of the controller penitentiary authorised to answer or reject the request or on the mode of determining its identification (e.g. at the time of the response, the organ carrying out the detention), with a view to the enforcement of the right to access. The Penitentiary complied with the call.

In the course of the investigation, the Authority also underlined that as of 1 January 2016, pursuant to Bvtv. Section 92(3), the convict shall be informed of the content of the risk assessment summary report drafted partly using the psychological opinions, which include the healthcare, psychological, security and reintegration tasks necessary for mitigating the risks of recidivism and detention for the convict, which the penitentiary has to take into account in the course of its reintegration activities, and the convict shall also be informed of the availability of recommended reintegration programmes to mitigate the risks of recidivism and detention. According to the justification of the act, this information is to be provided to the detainee primarily by the staff of the Central Examination and Methodology Institute (hereinafter: KKMI) (professional team) on site and not in the admission unit of the penitentiary designated for execution in view of the fact that they are professionally competent to provide professional justification in case the convict has any questions. This provision and the justification reveal that the request to have access to the content of the risk assessment summary report may not be rejected either by KKMI or any other penitentiary authorised to process it, and the detainee has a right to access the content of this report.

In view of the fact that the Authority received another request for consultation concerning the determination of the penitentiary authorised as well as obliged to respond to requests for psychological opinion, in which the notifier objected to the different practices of the various penitentiaries, the Authority also contacted the National Command of Penitentiaries (hereinafter: BVOP) as the supervisory organ of the individual controllers in penitentiaries.

BVOP informed the Authority that, according to their position, the respective detaining/registering penitentiary qualifies as controller where the detainee is currently being held and the detaining penitentiary is entitled to query sectoral data from the central electronic registry, even if the queried data were generated in another penitentiary. After this, the Office of BVOP sent a circular to the heads

of the penitentiary agglomeration centres and called their attention to the appropriate practice of accessing psychological opinions on the detainees, including that the currently detaining institution qualifies as controller, thus the decision concerning access may not be shifted onto another organ. *(NAIH-5478/2022.) (NAIH-1204/2022.)*

II.2.4. The processing of health-related personal data of detainees by penitentiaries

Based on a notification, the Authority investigated the processing practice of penitentiaries related to the records of health-related personal data of detainees. Pursuant to Bvtv., penitentiaries process the health-related personal data of detainees until they complete their sentences, or until such time as they cease to be enforceable. The processing of health-related personal data records of detainees by penitentiaries is processing for law enforcement purposes, to which the provisions of the Privacy Act apply.

In the course of the investigation, the Authority found that the records of the penitentiaries (hard copy and computer records) contain the health-related personal data of the notifier on his medication inaccurately and deficiently. The data of the hard copy and computer records do not correspond and it is not possible to clearly establish from the health-related personal data in the records what medication was given to the notifier and with what frequency during the period under investigation. The Authority established that processing by the penitentiary complained against infringed Section 4(4) of the Privacy Act, because the institute failed to ensure the accuracy and correctness of the health-related personal data of the notifier processed during the period under investigation.

In view of this, the Authority wrote a recommendation to the National Command of Penitentiary Institutions as the supervisory organ of the controllers based on Section 56(3) of the Privacy Act concerning the transformation of the processing practices of penitentiary institutions related to the records of the health-related personal data of detainees using technical and organisational measures to guarantee the accuracy and correctness of the processed data and the correspondence of data on hard copies and in the computer records.

The National Command of Penitentiary Institutions informed the Authority that, with a view to avoiding similar administrative problems, they called the attention of the penitentiaries to primarily record documentation in the medical system

(Főnix Healthcare Sub-module) in the course of healthcare activities provided by the penitentiary organisation, or if that is impeded, record the data in the electronic system subsequently after the cessation of the impediment based on the hard copy documentation. *(NAIH-4930/2022)*

II.2.5. Opening an official document for a detainee in a penitentiary

A notifier objected to processing by a District Prosecutor's Office (hereinafter: Prosecution) because in the course of his correspondence with the Prosecution, the Prosecution addressed letters sent to him to the Penitentiary where he was detained, which was injurious to him. Based on the notification, the Authority carried out an inquiry. The Authority examined all the relevant data of the Prosecution's measures served on the notifier. According to the Prosecution's statement, service was always done in accordance with the office instructions of the prosecutor authorised to take the given action recorded on the retained copy of the measure.

The Prosecution informed the Authority that the County Prosecutor's Office also investigated the mode of service objected to in the notification, according to which the prosecutor's address letters for the notifier to the penitentiary, hence the institution opens them.
The County Prosecutor's Office issued guidelines concerning service to persons detained in penitentiaries, according to which: *"The expedient practice is to send official documents in a closed envelope to the commander of the penitentiary, requesting him to deliver the closed envelope to the detainee. In this way, it can be avoided that an employee of the penitentiary should have unwarranted access to the content of the official document."*

According to the gist of the information provided by the Prosecution, service of documents to be sent to the notifier and other accused persons in detention will, in the future, be done in accordance with the guidelines issued by the County Prosecutor's Office.

The Prosecution also informed the Authority that Section 131(6) of the Code of Criminal Procedures provides that: *"If the addressee is detained, the document shall be served on him through the commander of the detaining penitentiary institution."*

The Authority established that the Prosecution did not act appropriately when it did not, in each case, ordered the delivery of the official document in a closed envelope to the notifier in the action clause. Although the name of the notifier was shown on the official document below the name and address of the penitentiary institution in order for the penitentiary to be able to determine which detainee the official document was sent to by the Prosecution, the penitentiary institution had to open the envelope thus accessing the content of the official document addressed to the notifier.

The Authority established that the Prosecution did not act appropriately from the viewpoint of the protection of personal data when – although forwarding the official document for the notifier in a closed envelope in the penitentiary –, they informed the commander of the penitentiary in the cover letter addressed to him of the content of the official document for the notifier and requested the penitentiary institution to deliver the closed envelope containing the official document to the notifier.

Bvtv. Section 174 provides for the rules of correspondence. Under Bvtv., the detailed rules at the level of an implementing regulation are specified in Decree 16/2014. (XII. 19.) IM.

According to Bvtv. Section 174(4): *"The content of correspondence of the convict with the authorities, with international human rights organisations, with relevant competence as acknowledged by international convention promulgated by law, the commissioner for fundamental rights, the organisation or staff member of the national mechanism for prevention and the defence attorney may not be checked. If there are reasonable grounds to suspect that the letters either received or sent by the convict do not come from the authority, international organisation or the defence attorney as indicated on the envelope, or are not for the addressee, the letter shall be opened in the presence of the convict, which shall be recorded in minutes simultaneously. Checking can only serve the purpose of identifying the sender."*

The Authority informed the Prosecution that Section 131(6) of the Code of Criminal Procedures provides for the mode of service and not for informing the commander or any employee of the penitentiary of the content of an official document for a detainee.

The Authority drafted data security measures compliant with Section 25/I(1), (2) and (3)(b) of the Privacy Act for the district prosecutor's office as controller;

1.) By showing the name of the detainee on the external cover of the letter sent to the address of the penitentiary, but addressed to a detainee, the opening of the letter received from the authority by the penitentiary in order to ascertain which detainee the letter is for could be avoided.

2.) Service according to the guidelines of the County Prosecutor's Office is also appropriate, according to which official documents intended for persons in penitentiary institutions are sent in a closed envelope to the commander of the penitentiary institution requesting him to deliver the closed envelope to the detainee. However, this way of sending the document is appropriate from a data protection point of view only if the cover letter enclosed with the letter for the notifier forwarded in a closed envelope does not inform the commander of the penitentiary institution of the content of the official document in the closed envelope.

The Authority established that an infringement related to the processing of the notifier's personal data took place and called upon the prosecution to transform its processing practice with regard to service to detainees in closed envelopes in line with the relevant legal regulations in accordance with either of points 1 and 2 above.

In their response, the Prosecution informed the Authority, inter alia, of the fact that they agreed with the Authority's call in relation to the Prosecution's processing practice. The senior district prosecutor modified the rules of service on persons in penitentiary institutions, taking into account the Authority's call in accordance with the guidelines of the county prosecutor's office concerning the delivery of official documents to penitentiary institutions and in the future they will refrain from making references to the content of the document in the course of delivery. With a view to data security, the name of the detainee will be indicated also on the external cover of the letter addressed to the detainee. The rules of delivering official documents to penitentiary institutions in compliance with data protection regulations were communicated to all the assistant prosecutors and the senior district prosecutor issued an instruction for compliance with these rules. (*NAIH-5512/2022.)*

II.2.6. Packaging evidence of crime

The Authority received a notification, according to which police officers on the staff of a police station carried out a search and seizure operation under a criminal procedure at the place of stay of the data subject. According to the notification, the police officers taking action violated the legal regulations when they seized the electronic devices in the possession of the data subject, his workplace mobile phone, which was not his property, together with 2 SIM cards, and his computer. The notification stated that the seized devices were not given evidence numbers as evidence and they were not packaged in accordance with the rules, thus their integrity and protection from alteration were not ensured; on the other hand, the data subject did not receive specific or correct information on the place where they were kept. The notifier explained that the seized computer contained also his personal data, the seizure of the computer and of the mobile phone were unnecessary; furthermore he did not receive a protocol on the procedural act.

In view of the notification, the Authority conducted an inquiry in the case based on Section 38(3)(a) of the Privacy Act. The Authority found that the investigator carried out the seizure without the participation of a forensic technician, thus, the required packaging materials were not available onsite; because of this, the police officer taking action called upon the subject of coercive measure to hand over his IT devices switched off. The evidence was packaged in the building of the police station.

According to Section 25/I(1) of the Privacy Act, for the purpose of ensuring the appropriate level of security for the personal data processed, the controller and the processor shall implement technical and organisational measures to reflect the level of risks, resulting from the processing, to the enforcement of the data subject's fundamental rights taking into account, in particular, risks entailed by any processing of the sensitive data of the data subjects. Paragraph (2) of the same section stipulates that in the course of developing and implementing the measures specified in paragraph (1), the controller and the processor shall take all circumstances of the processing into account, in particular the state of the art, the cost of implementing measures and the nature, scope and purposes of processing, as well as the risks of varying likelihood and gravity for the enforcement of the rights of data subjects posed by the processing. According to Section 25/I(3)(b) of the Privacy Act, the controller and, within the limits of its activity, the processor shall ensure through the measures specified in paragraph (1) the prevention of unauthorized reading, copying, modification or removal of data storage media.

Based on the above, the Authority established that the police officers failed to comply with the data security measures according to the Privacy Act in the

course of the procedure under investigation. According to the position of the Authority, the fact that a forensic technician cannot be present at the site of the procedural act should not result in the omission of the packaging of the evidence; it is necessary to provide the appropriate packaging materials for the procedural act and in the absence of a forensic technician, the police officer taking action has to carry out the necessary packaging. The Authority's inquiry did not find a data breach; according to the controller's statement its possibility did not arise, nor did the notifier regarded it probable.

Based on Section 56(1) of the Privacy Act, the Authority called upon the Police Station as controller to carry out its acts in full compliance with the data security measures in the future. They should package the seized data storage media onsite in accordance with the rules in every case, to ensure their integrity and inaccessibility by any unauthorized person. The fact that the data storage media is switched off and password-protected is not in itself sufficient. A good example is having the inputs of the data storage media sealed off, stamped and signed by the subject of the coercive measure and then documenting their opening to unambiguously verify that no unauthorized person had access to it. (*NAIH-267/2022*)

II.2.7. Transfer of person data, the principle of purpose limitation

In an Authority procedure for data protection launched upon request, the Authority investigated the lawfulness of the procedure of the Airport Police Directorate (for the purposes of this heading, hereinafter: Controller) related to the transfer of personal data.

Based on Section 24(4) of Act XXXIV of 1994 on the Police (hereinafter: Police Act), the police patrol on the staff of the Controller subjected the Notifier to mutual identity check. Following the mutual identity check, those requesting the identity check submitted a request to the Controller electronically for the issue of the Notifier's personal data. To substantiate their entitlement to access the personal data of the Notifier, they cited that the ticket inspectors of the Budapest Traffic Centre (BKK) do not allow them to perform their activities lawfully, they are regularly subjected to unjustified checks and, because of this, they wish to take additional legal steps. The Controller fulfilled the request of the persons requesting the identity check and disclosed the identification data (name, place and date of birth, mother's name) of the Notifier.

Pursuant to Section 24(4) of the Police Act, a police station may issue the personal data of a person whose identity was checked to the person requesting the identity check, if the latter verifies his entitlement to the data in a creditworthy manner.

The principle of purpose limitation is one of the most important principles of processing developed internationally, according to which personal data can only be processed for a clearly determined, lawful purpose to exercise a right and to meet an obligation. When the principle is complied with, the controller processes only those personal data, which are necessary for performing its tasks and functions. The requirement of purpose limitation extends to all the stages of processing, including the transfer of data.

In their request submitted to the Controller, those requesting the identity check did not specifically indicate the purpose of using the requested personal data ("*additional legal steps*"), the request does not reveal what sort of legal steps they wished to take, what sort of procedure they wished to launch, in front of which authority and against whom – whether the Notifier or BKK. Even if there is a lawful, clearly specified purpose of processing, only the data indispensable and suitable for the attainment of the purpose of processing can be processed. In the absence of a clearly specified processing purpose, it is not possible to determine the data indispensable and suitable for the attainment of the purpose of processing. It is not indispensably necessary to know the personal data of the Notifier to launch an eventual procedure against BKK, to lodge a report with the police – which presumably was the intention of those requesting the identity check based on their statements – because the Notifier acted as BKK's ticket inspector in the course of the act objected to, not as a private individual. Furthermore, the Notifier made out a protocol on the inspection carried out by it, a copy of which was given to the person subjected to the inspection and requesting the identity check, whereby the name of the Notifier, the name of his employer, his position and the time and place of the act were available. Knowledge of these data is sufficient to initiate an eventual procedure in relation to the act objected to.

In the course of its investigation, the Authority established that the persons requesting the identity check did not verify in a creditworthy manner their entitlement to have access to the personal data of the Notifier in their requests submitted to the Controller. The Controller did not act lawfully when issuing the personal data of the Notifier to those requesting the identity check, because the data were transferred in the absence of a clearly specified, lawful purpose. Based on Section 61(1)(b)(ba) of the Privacy Act, the Authority established the

fact of the unlawful processing of personal data as the Controller violated the principle of purpose limitation set forth in Section 4(1) of the Privacy Act when processing the Notifier's personal data. *(NAIH-3314/2022)*

II.2.8. Investigation of the lawfulness of processing practice, data security requirements

As a result of a notification and based on Section 38(3)(a) of the Privacy Act, the Authority investigated the lawfulness of the processing practice pursued in the building of the National Tax and Customs Administration (NAV) Dél-alföld Criminal Directorate (for the purposes of this heading, hereinafter: Controller). The Notifier stated that when he visited the building of the Controller, he noticed that "a great many folders and documents were lying on the floor" in a ground floor office with glass walls and also "many documents were laid on the open shelves and on the floor" also in another office, which he could have read as he stated. He also enclosed photos made on site to the Notification.

The Authority inspected the photos enclosed by the Notifier and found that the photos did not substantiate that the Notifier would have physically been able to read the folders. Based on the internal investigation conducted by the Controller, unauthorized access to personal data or any data breach could not be verified. The Authority investigated the data security-related provisions of the rules (document management rules, rules of guard security) in force at the Controller at the time of the event, particularly the requirements related to the protection of documents. According to the provisions of the document management rules of the controller, the requirements concerning the physical protection of archives and additional document management rules are contained in the NAV guard security rules (hereinafter: ÖBSZ) and the rules on local guard security of the organs of NAV (hereinafter: local ÖBSZ). The Authority found that the data security measures set forth in the document management rules and ÖBSZ are of a general nature and they did not contain detailed rules taking into account local specificities related to the physical protection of the premises and the reception of external persons, their accompanying and supervision within NAV's buildings. The controller did not have a local ÖBSZ when the event took place.

The Authority established that by failing to create the local ÖBSZ, i.e. the data security requirements taking local specificities into account, it did not comply with its obligation set forth in Section 25/I(1) of the Privacy Act. In view of this, based on Section 56(3) of the Privacy Act, the Authority made a recommendation to the

National Tax and Customs Administration Criminal Directorate General as the supervisory organ of the Controller for the enactment of the local guard security rules of the Controller.

The Controller complied with the recommendation by enacting the local ÖBSZ, in which it specified the requirements related to the physical protection of archives and document management rooms, as well as the mode of receiving external persons, accompanying them and supervising them within the building. *(NAIH-317/2022)*

II.2.9. Authority procedure for data protection based on a request in relation to surveillance using the Pegasus spyware

The Authority launched an investigation concerning the application of the "Pegasus" spyware in Hungary in 2021, in view of the fact that according to the news published by the media, personal data may have been unlawfully processed by using the spyware.

Article VI of the Fundamental Law protects private and family life, home, communication and good reputation, personal data and access and dissemination of data of public interest as the fundamental rights of individuals. The Authority supervises the enforcement of the latter rights concerning information as an independent authority established by a cardinal act. Covert intelligence gathering is an activity, which evidently takes place without the data subject being aware of it, yet it deeply intrudes into the privacy of individuals and has a direct impact on the fundamental rights mentioned. In view of this, the safeguard rules enabling the external control of such procedures within a specific framework have an outstanding role. However, public access is excluded with regard to the data of the specific procedures.

In connection with the application of the "Pegasus" spyware in Hungary, individuals may, among the options to enforce rights, initiate an inquiry by the Authority, or submit a petition for conducting an authority procedure for data protection based on Section 22 of the Privacy Act.

In 2021, no data subject submitted a complaint or petition to the Authority in relation to the application of the "Pegasus" spyware. The Authority conducted an

inquiry procedure ex officio, the parts of the findings that could be made accessible to the public were published by the Authority in January 2022.[8]

In 2022, several petitions were received for conducting authority procedures for data protection requesting investigation of the unlawfulness of the processing of personal data in relation to the surveillance of the petitioner by the Pegasus spyware and ensuring the petitioner's data subject rights under Section 14 of the Privacy Act in accordance with Section 71(1a) of the Privacy Act.

Section 71(1a) of the Privacy Act stipulates that if the controller lawfully restricts or is entitled to restrict, on the basis of an act or a binding legal act of the European Union, the rights to which the data subject is entitled according to the provisions under Articles 13 to 18 and 21 of the General Data Protection Regulation and under Section 14 of this act, the Authority shall, in the context of its procedures,
a) ensure the data subject's rights in a manner and at a time, and
b) perform the mandatory notifications of the data subject specified in this act as the obligation of the Authority in a manner and at a time,
guaranteeing that the interests that may serve as a basis for lawfully restricting the data subject's rights shall not be impaired.

Pursuant to Section 8(1)-(2) of Act CXXV of 1995 on National Security Services, the Specialised National Security Service provides services, within the limits of the relevant legal regulations, with its special means and methods of intelligence gathering and covert data acquisition, in support of the organisations authorised to gather intelligence and acquire data covertly under the Criminal Procedures Act. In this respect, information provided by the Specialized National Security Service concerning the use of means was indispensable for the Authority for the clarification of the facts of the case.

However, in order to prevent screening of the operational records of the national security services, establishing the existence or absence of the capacity of controller with respect to the data subject is in itself protected data. In view of Section 27(2) of Act CL of 2016 on General Administrative Procedures and the provisions of Section 71(1)(a) of the Privacy Act, information on the data in the records of the Specialized National Security Service and procedural acts carried out by the Authority cannot be provided to the petitioner because that would jeopardize the national security interest – the national security interest linked to

8 https://naih.hu/adatvedelmi-jelentesek/file/486-jelentes-a-nemzeti-adatvedelmi-es-informacioszabadsag-hatosag-hivatalbol-inditott-vizsgalatanak-megallapitasai-a-pegasus-kemszoftver-magyarorszagon-torteno-alkalmazasaval-osszefuggesben

preventing a screening of the archives and operational records processed by the national security services – which interest constitutes a sufficient basis for restricting the private interest in accessing the personal data of the petitioner.

The Hungarian legislator stipulates that the provisions of the Privacy Act are to be applied in addition to processing for law enforcement purposes also to processing for national security purposes. When interpreting Section 71(1)(a) of the Privacy Act, Directive (EU) 2016/680 concerning the protection of personal data processed for law enforcement purposes (Law Enforcement Directive) has to be taken into account as well, which was transposed into national law by the Privacy Act. The above is in line with the provisions of Article 17 of the Directive. Based on Article 17(1), in the cases referred to in Article 13(3), Article 15(3)[9] and Article 16(4)[10], Member States shall adopt measures providing that the rights of the data subject may also be exercised through the competent supervisory authority. Pursuant to Article 17(3) of the Law Enforcement Directive, where the right referred to in paragraph (1) is exercised, the supervisory authority shall inform the data subject at least that all necessary verifications or a review by the supervisory authority have taken place. The supervisory authority shall also inform the data subject of his or her right to seek a judicial remedy.

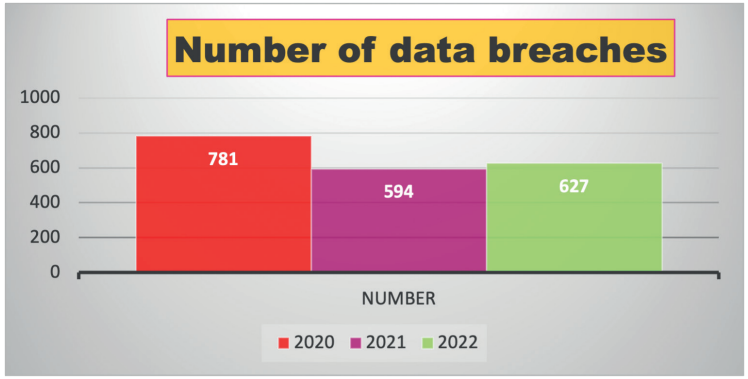
In the case referred to, the Authority conducted the procedure according to the petition, as a result of which it did not expose unlawfulness, hence it rejected the part of the petition concerning the establishment of unlawful processing and, upholding the part of the petition requesting the exercise of data subject rights with the Authority's assistance, informed the data subject in accordance with the above that it performed every necessary review concerning his petition. *(NAIH-6421/2022)*

9 (3) In the cases referred to in paragraphs (1) and (2), Member States shall provide for the controller to inform the data subject, without undue delay, in writing, of the refusal or restriction of access and of the reasons for the refusal or the restriction. Such information may be omitted, where the provision thereof would undermine the purpose under paragraph (1). Member States shall provide for the controller to inform the data subject of the possibility of lodging a complaint with a supervisory authority or seeking a judicial remedy.

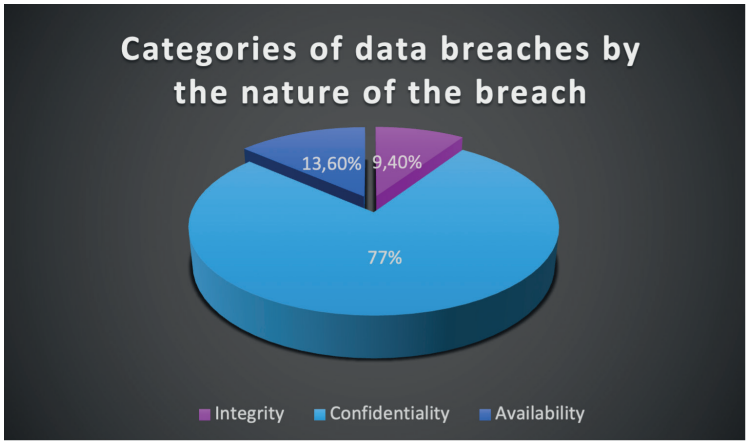
10 (4) Member States shall provide for the controller to inform the data subject in writing of any refusal of rectification or erasure of personal data or restriction of processing and of the reasons for the refusal. Member States may adopt legislative measures restricting, wholly or partly, the obligation to provide such information to the extent that such a restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interest of the natural person concerned in order to:
a) avoid obstructing official or legal inquiries, investigations or procedures;
b) avoid prejudicing the p9revention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
c) protect public security;
d) protect national security;
e) protect the rights and freedoms of others.
Member States shall provide for the controller to inform the data subject of the possibility of lodging a complaint with a supervisory authority or seeking a judicial remedy.

II.3. Reporting data breaches

In 2022, 627 data breaches were reported to the Authority constituting to a minor rise relative to 2021. Currently, several channels are available for a controller to report data breaches; of the 627 data breaches notified, 375 arrived through the data breach notification system, 50 were notified by e-mail, 196 via the official gateway, 5 by mail and 1 data breach was reported in person. The data verify that controllers prefer the dedicated electronic interface in contrast to the modes of notification preferred earlier.



Roughly 17% of the data breach notifications received took place because of the hacking of IT systems, while attacks by ransomware made up about 9.2% of all the notifications, and incidents due to phishing accounted for 9.3%. The above figures illustrate the trend that controllers are exposed to an increasing number of IT attacks calling attention to the importance of data security and the need for improving data protection awareness.



Examining the distribution of data breach reports among the various sectors reveals that the activities of the controllers concerned are highly varied, but in terms of numbers and shares, most of the data breaches were in healthcare, insurance and in the financial field as about 40% of all the data breach notifications came from these sectors. Naturally, this means on the one hand that controllers relate to the data breach with the highest level of awareness in these sectors, but on the other hand it also means that raising awareness towards data security and incorporating even more data security measures is needed the most in these sectors.

II.3.1. Major data breaches subject to the General Data Protection Regulation

1. In June 2021, a political party notified the Authority through the electronic route of a data breach affecting its processing. Altogether six Excel files, which had earlier been held by the party, became directly accessible to anyone through a link. Reference to the link was made also in an article published on an Internet news portal.

The tables contained a list of the names of the supporting members of the party, as well as operational data, and they also included access data (phone numbers, e-mail addresses, residential addresses, ID numbers). Based on the notification by the party, about 2,000 data were affected by the data breach, including the data of those volunteering to work in the 2018 election campaign, the exact data of the party's supporting members, the names of the party's internal coordinators and their assistants, and the list of the party's candidates for the 2022 elections.

As explained by the party, the tables were processed as Google Sheets tables online. Earlier, access to the tables was provided to the party's senior officials and its activists through a link. Once the tables were made public, access was restricted to the party's senior officials. Previously, access was also granted to the activists because the party's internal principles allowed them to communicate directly with one another.. By analysing the access log to the files, the party was unable to establish whether they were accessed by an unauthorized external hacker, or the disclosure of the files was the result of internal leakage.

In its decision dated 22 April 2022 on the case, the Authority established that the party infringed Article 32(1)(a)-(b) and (2) of the General Data Protection

Regulation as it failed to apply data security measures proportionate to the risks of storing the data of party's sympathisers and activists. According to the Authority, it was not proportionate to the risks of processing special category data, such as the party's sympathisers, that the data were stored on an online interface accessible to anyone, having merely a link. As files can be exported simply from Google Sheets and downloaded to the users' local computer, allowing access to such a large number of people without any other control of their authorisation (such as protection of the tables by password), the likelihood of accessing the data by unauthorized persons, or sending the files to others or disclosing them by a person previously authorised to access them, is great. Nor was encryption used to preserve the confidentiality of the files.

The Authority also established the infringement of Article 5(2) of the General Data Protection Regulation, as the party failed to respond to the orders of the Authority aimed at clarifying the facts of the case in spite of several calls to do so and a procedural fine of HUF 350,000.

With its decision in the case, the Authority imposed a data protection fine of HUF 3,000,000 on the party. The party did not challenge the Authority's decision in an administrative lawsuit before the court, hence it became final. (*NAIH-1855/2022*)

2. A private individual lodged a notification with the Authority because of a data breach taking place in the course of processing by a mayor's office as local elections office. According to the complainant, the decision of the mayor's office on the request to change polling districts in connection with the elections in April 2022 was not sent to the e-mail address provided but to an erroneous, but existing e-mail address. Furthermore, the mayor's office enclosed the decision with the e-mail as an unprotected file. Thus, the decision containing the personal data of the complainant was received by an unauthorized person, which constitutes a data breach. In relation to the complaint, the Authority initiated an inquiry procedure to clarify whether the processing by the mayor's office was in compliance with the provisions of the General Data Protection Regulation.

Based on the answers given by the mayor's office the Authority launched an authority audit – in parallel with its inquiry – under a separate case number to examine how the mayor's office handled the data breach. The Authority closed the authority audit with an internal memorandum, because no circumstance indicative of an infringement in relation to the management of the breach arose in this case.

In its inquiry procedure, the Authority examined the processing of requests for changing polling districts related to the electoral register by local election offices and the mode of communicating the decisions made as a result. To conduct the inquiry, it was necessary to involve the National Elections Office, in view of the fact that with its tasks specified in Act XXXVI of 2013 on Electoral Procedure (hereinafter: Electoral Procedures Act), its activities qualify as processing in accordance with Article 4(2) of the General Data Protection Regulation. Finally, the subject matter of the inquiry was whether the IT system the National Electoral System (hereinafter: NVR) installed and operated by the National Electoral Office complied with the provisions of the General Data Protection Regulation.

First, the Authority reviewed in what way requests can be submitted to the local elections office. Based on Section 91(1) of the Election Procedure Act, voters with address in Hungary may submit requests regarding the central electoral register – i.e. not only requests for changing polling district – in person, by mail, by electronic means after electronic identification through the client gateway or without electronic identification by electronic means through magyarorszag.hu or www.valasztas.hu with and election agent. Requests submitted in person or by mail, i.e. on paper, are recorded in NVR's request management module by the clerk of the local election office. In such a case, if the clerk misspells the e-mail address of the applicant while recording the request, the possibility of a data breach obtains if notification of the decision is sent by e-mail to an existing but different e-mail address. Requests submitted electronically land automatically in NVR's request management module and reach the local election office via NVR. In this case, there is no need for recording the request by the clerk, thus misspelling by the clerk is excluded. The processing of requests concerning the central and the local electoral register is handled uniformly via NVR, regardless of the form of submission. The clerk assesses the request in NVR and notifies the applicant on the decision.

According to the Authority's position, local election offices work with a large number of data and in view of the nature of the elections, many voters may submit requests during this period. Case numbers are increased by the fact that it is not only requests for changing polling districts, but all requests related to the central electoral register and the local electoral register coming to them, which further increases the potential number of cases. For requests submitted in person or by mail, there is always a possibility for the clerk to misspell the e-mail address provided in the request in NVR's request management module. The risks of a resulting data breach can be substantially reduced if .pdf file is encrypted when the decision is sent by e-mail by NVR.

In the course of its inquiry, the Authority found that currently NVR sends the decision by e-mail as a .pdf file without encryption. Thus, in the case of a .pdf file without encryption sent to an erroneously recorded e-mail address, which happens to be the real e-mail address of another person, the possibility of unauthorized access obtains. Based on all this, the requirement of secure processing according to Article 5(1)(f) and Article 32 of the General Data Protection Regulation was not complied with.

In relation to the need for the requirement of encryption, the Authority also examined exactly what document is notified by the local election office to the applicant, and what personal data it contains. Technically, the creation of a decision in NVR, when notified by e-mail, also means the automatic sending of the decision via NVR. Thus, communicating the decision means not only notification about the content of the decision, but also sending the decision in writing. Furthermore, the decision is valid without a signature and the print of a stamp based on Section 5(1)(b) of Decree 20/2019 (VII. 30) IM and Section 14 of Decree 17/2013 (VII. 17) KIM, thus, as an electronic document, there is virtually no attestation of the document. The decision contains the following personal data: name, address, the settlement where the voter wishes to re-register for polling and the e-mail address.

The Authority established that the local election office sends a decision aimed at giving rise to a legal effect to the e-mail address without electronic attestation and it contains data for the identification of a natural person as well as the expected place of stay of the data subject. In view of the risks involved in unlawful access, the Authority considers that encryption of the .pdf attachment is a practice that could be expected in NVR's operation. On the grounds of the above infringement, based on Section 56(1) of the Privacy Act, the Authority called upon the National Election Office to modify NVR it operates so that in the case of notification by e-mail, the IT system should send a decision to the applicant with the appropriate encryption, for instance as a password protected file. In its response, the National Election Office informed the Authority that the development of NVR took place and encryption through password protection has been implemented. (*NAIH-3823/2022*)

3.In relation to a petition pertaining to the establishment of unlawful processing because of an erroneous data query in the Electronic Healthcare Service Space (hereinafter: EESZT), the Authority established that there was a data breach in the case which, however, did not constitute unlawful processing.

Based on the facts of the case exposed by the Authority, the data breach occurred because the controller wanted to view specific findings of a patient of a name similar to that of the petitioner in EESZT. Because of exhaustion caused by the large number of patients and the increased administrative burden due to the Covid pandemic, the assistant clicked on the name of the petitioner through an oversight in the database opened in the patient registration program used in the surgery. Then, the assistant began downloading the patient data for the 6-month period automatically displayed by the system in EESZT opened in parallel with the patient registration program, and noted only after downloading several documents that in contrast to her intention, she had access to the data of a different patient, when she immediately closed the opened medical record. The patient's documents were not saved.

Once learning of the queries of his health-related data based on EESZT's event log, the petitioner wished to get information by phone in the surgery of the controller. It was only then that the assistant learned that the petitioner was the patient whose findings she erroneously opened. To clarify the situation, she then contacted the petitioner, acknowledged that the erroneous opening of the medical record was due to her error because of the increased workload and she apologized.

According to the position of the Authority, the occurrence of a security breach can only be linked to and result from an existing processing operation carried out on the basis of an existing decision by the controller. The occurrence of the data breach itself, however, does not result in another independent processing operation. The data breach is always an ancillary consequence related to the basic processing operation. It is no accident that the General Data Protection Regulation provides for separate legal consequences for such cases and this is separately manifested in the criteria for imposing fines [see: Article 83(4)(a) of the General Data Protection Regulation].

In this case when verifying the facts of the case, the Authority did not identify a processing purpose for which the controller would have deliberately inspected the petitioner's documents stored in EESZT. In view of this, the capacity of controller did not exist and in the absence of a deliberate decision on the purposes and means of processing. The data breach took place in the course of a fundamentally lawful, basic processing operation (processing of data generated in the course of occupational health care) through an oversight, because of the accidental mix-up of the names of two patients with similar names and it gave rise to a data breach from this security breach. The inadvertent query performed by

the controller is not linked to any legal basis or purpose determined in advance, which would have resulted in a separate processing. Accordingly, the Authority established the occurrence of the data breach, but rejected the petition for establishing unlawful processing. (*NAIH-107/2022*)

4.According to a notification received by the Authority from a data subject, the findings of his Covid-19 screening carried out by a private healthcare provider was transferred by the controller to an erroneous e-mail address. In the course of its procedure, the Authority found that the controller attached the findings of the screening without encryption, so as a result of using the erroneous address, a third party could have unauthorised access to the personal data, including the data subject's name, birth date, address, social security number and the findings of the microbiological test.

The controller learned of the case from the Authority's order aimed at the clarification of the case, thereafter it recorded the incident and called upon the erroneous addressee to erase the e-mail and its attachment, who confirmed it the same day indicating that he had earlier done so. After this, the controller notified the Authority of the data breach despite the fact that, according to its position, the risk of using these data in a manner injurious to the data subject was extremely low, due to the fact that the erroneous addressee confirmed that the e-mail and its attachment were previously erased.

The Authority established that the document containing health-related data was not encrypted in any way. The appropriate data security measures would have reduced the risk of unauthorised access to the health-related data by the erroneous addressee of the e-mail. In view of all this, the data breach was subject to the notification obligation as it entailed a risk for the rights and freedoms of data subjects. According to the Authority's position, the transfer of these data by e-mail without any access protection or use of encryption does not comply with a data security level appropriate to the extent of the risks posed by the processing.

Based on the facts of the case, the Authority established that the controller failed to comply with its obligations under Article 33(1) of the General Data Protection Regulation as it failed to notify the data breach without unjustified delay once it learned of it. Furthermore, by transferring the data without data security measures, it also infringed Article 32(1)(a) and (b) and Article 32(2) of the General Data Protection Regulation. (*NAIH-3217/2021*)

5.Based on the facts of the case established in an authority procedure launched upon request, a petitioner requested the petitionee to send his health documentation and clinical final reports from his childhood necessitated by a disability procedure in progress by phone, which request he did not confirm in writing. Because of the pandemic, the petitioner was notified that they can sent him the health-related documentation only by e-mail, so he gave his e-mail address by phone. In view of the fact that he received no answer to his e-mail address even days after, the petitioner again contacted the petitionee, who responded by stating that the requested documents were sent the previous day to the e-mail address given. The petitioner asked for the letter already sent, which revealed that the clerk sent the health documentation to a third person because of misspelling the petitioner's e-mail address.

Pursuant to Article 4(12) of the General Data Protection Regulation, "personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed". This case qualifies as a data breach because the breach of security and not the absence of appropriate measures led to unauthorized access to the personal data processed. In the case under investigation, the security breach as one of the conceptual elements of a personal data breach arose from the fact that the petitionee failed to apply the appropriate technical and organisational measures to safeguard the confidentiality of documents containing health-related data. Although the security breach stemmed from misspelling of the address through an oversight by the clerk, the error could also be traced back to the fact that there were no clear procedures on personal data that could be sent by e-mail, or how they could be sent. The data breach could have been avoided, had they not been sending personal data by e-mail at all, or if they had adopted appropriate measures to eliminate administrative errors (such as the four-eye principle, drafting an official memo on the data subject's request for sending the data by e-mail). Another necessary organisational duty is the regulation of the mode of requesting data by data subjects.

Having learned of the data breach, the petitionee implemented organisational measures to mitigate future risks and although the Authority took into consideration that the petitioner requested sending by e-mail, it stressed that such client-friendly solutions based on equity should be refrained from, if they significantly deviate from the protocol and compromise the security of personal data.

According to the provisions of Recital (75) of the General Data Protection Regulation, if the personal data processing may lead to identity theft or fraud, it

fundamentally qualifies as a risk. The name, birth data, mother's name and particularly the social security number of the data subject are data with which identity theft or fraud can be committed. Furthermore, data concerning health were also involved in the data breach, which belong to the special category of personal data according to Article 9(1) of the General Data Protection Regulation; such information concern the more sensitive aspects of the data subject's rights, therefore unauthorized access to them and their disclosure could be particularly injurious for the data subject. Accordingly, the above personal data breach qualifies as high risk, which must be notified to the Authority and of which the data subject must also be notified. The petitionee failed to meet these obligations.

In the context of data breaches, there is little technical possibility to remedy the data breach subsequently in the case of erroneously sent e-mails, so the prevention of risks of such data breaches and the proactive behaviour of the controller is particularly important. According to the Authority's position, the transfer of these data by e-mail without any access protection or encryption as in the present case does not comply with the data security level appropriate to the extent of the risks posed by the processing. Without appropriate protection, it is not possible to guarantee an adequate level of protection in the list of the state of the art that personal data processed are not disclosed or accessed by unauthorized persons in the event of an eventual data breach. Sending health-related data by e-mail without appropriate access protection is not regarded as good practice by the Authority.

Partially upholding the petition, the Authority established that the petitionee failed to meet its data breach notification obligation based on Article 33(1) of the General Data Protection Regulation in the context of the data breach that occurred when the previous health-related data of the petitioner were sent to an erroneous e-mail address. Furthermore, it established that the petitionee failed to comply with Article 32(1)(b) and (2) of the General Data Protection Regulation, when it failed to apply data security measures proportionate to the risks of forwarding documents containing health-related data. On the grounds of the infringements established, the petitionee was reprimanded.

6.The Authority received several complaints in which notifiers objected to the fact that by misusing the "breakglass" function of EESZT, the experts using it gained unauthorised access to their personal data in EESZT.

There are fundamental authorisation settings in EESZT to ensure access by the attending physician and the family physician in accordance with Act XLVII

of 1997 on the Processing and Protection of Health and Related Personal Data (hereinafter: Health Data Act); accordingly, every item of health-related data, which can be associated with the disease of the data subject can be transferred, which is of importance for treatment based on the decision of the attending physician or the family physician. In addition, data subjects may make digital self-determination statements in EESZT to set access restrictions.

These fundamental rules can be disregarded exclusively in the event of medical emergency specified in Section 10(4) of the Health Data Act. According to Section 3(i) of Act CLIV of 1997 on Health, medical emergency means "a sudden change in health, which would endanger the patient's life or result in severe or permanent health impairment in the absence of urgent medical care". The "breakglass" function referred to enables any physician to have access to the health data necessary for safeguarding the health and life of the patient in the event of a medical emergency.

The Authority stresses that this function may be used only in warranted cases expounded in the Health Data Act, it cannot be lawfully used in other cases, for instance, for the purpose of overriding the provisions of the Health Data Act, or the data subject's digital self-determination statement. It is contrary to the principle of purpose limitation, if this function is used for a purpose other than a medical emergency and personal data are processed that way. Incidentally, when using this function the physician has to appropriately mark the medical emergency situation according to Section 10(4) of the Health Data Act at the given time and the fact that he/she requests data from EESZT on that basis, which is considered as the physician's declaration with regard to the existence of a medical emergency. In addition to the responsibility of individual physicians as controllers and eventually their criminal liability in relation to such processing, the Authority deems it necessary that the National Hospital General Directorate operating EESZT also take the necessary steps to ensure the appropriate lawful use of the function.

7.Based on articles published on various Internet news portals, the Authority learned of a hacker attack against eKRÉTA Informatikai Zrt. and the resulting data breach on 7 November 2022; thereafter, because the circumstances that have come to its knowledge from press reporting and because prior to their publication it did not receive any personal data breach notification from eKRÉTA Informatikai Zrt., the Authority launched an authority audit focusing on compliance by eKRÉTA Informatikai Zrt. with the obligations according to Articles 32-34 of the General Data Protection Regulation on 8 November 2022.

Aware of additional news reports published in the days following the launch of the authority audit and the personal data breach notification sent to the Authority by eKRÉTA Informatikai Zrt. and individual school districts in the meantime, the Authority decided to launch an authority procedure ex officio for data protection on the grounds of the presumed infringement of Articles 32-34 of the General Data Protection Regulation based on Section 60(1) of the Privacy Act on 11 November 2022. The procedure is still in progress at the time of drafting this report.

II.3.2. Significant personal data breaches subject to the Privacy Act

1.*Data breach concerning documents erroneously issued upon release from a penitentiary institution*

In relation to a data breach notified by a penitentiary institution (hereinafter: Penitentiary), the Authority launched an authority audit ex officio and subsequently an authority procedure for data protection in order to assess whether the Client fully met its obligations set forth in Sections 25/J-25/K of the Privacy Act.

On the day of the release of a detainee, the Penitentiary handed over the document and valuables deposited by a detainee of the same name (but different registration number) (hereinafter: data subject) to the released person by mistake. The released person was documented to have received the document and valuables deposit of the data subject in error from the representative of the security department, for which he was unauthorised, and did not return them even though called upon to do so; he claimed to have thrown them away.

The personal data concerned in the breach clearly made identification of the data subject possible because the ID card, address card, tax card, driver's licence, school certificate and social security card were given to an unauthorized person. The Client did not identify any malevolent act or negligent act, which would qualify as malevolent within the organisation, or any external malevolent act or such act that would qualify as malevolent as the cause of the incident. According to the notification, identity fraud could occur and the confidential nature of the data was impaired by the fact that the risk of access to the personal data by an unauthorized person exists. According to the client's notification, the data could not be linked to other data of the data subject; furthermore, the unfair processing of the data for other purposes was not possible. Other circumstances of the data breach were not known. The Client considered the severity of the possible consequences of the data breach limited.

The conclusions of the Penitentiary related to determining the risks posed by the data breach were dubious and contradictory. This was substantiated by the fact that the Penitentiary officially called upon the former detainee to return the deposited objects, but as it was not successful, it lodged a criminal report with the competent police station.

Abiding by the chain of command, the depository reported the data breach to his service superior the next day. First, the head of the depository group, then the financial officer and finally the commander were informed. Measures were taken to have the documents and deposited items returned which were issued erroneously; this, however, was unsuccessful. This information was received by the disciplinary officer 22 days after the data breach, who then notified the data protection officer the next day, i.e. on the 23rd day following the data breach and 22 days after the first superior became aware of the data breach. This happened despite the fact that the person under whose charge the data breach took place reported the case to his superiors on the day following the data breach.

The Client conducted a disciplinary procedure in relation to the personal data breach. In the course of the audit and the authority procedure, the Authority established that, although minimally, but the data involved in the data breach could be linked to criminal personal data because the detainee's document and valuables were issued from the depository and in this way the fact of having committed some kind of criminal offence/ misdemeanour and being detained became known to another person in relation to the data subject. Several documents of the data subject containing identification data - including a document suitable for the verification of his identity - came into the possession of a person not authorised to access them (a person who had earlier committed a misdemeanour) who did not return them either voluntarily or upon being called upon to do so.

Having taken all the circumstances of the case into account, it was found that the data breach was of high risk. The Client notified the data subject after more than a month, which fails to comply with the requirement of action without undue delay. The Client should have notified the Authority of the data breach within 72 hours from learning of it, which the Client failed to do, and made the notification only with a substantial delay. The Authority took into consideration the fact that the data breach was due to a negligent action. Accordingly, in contrast to that stated in the Client's notification, it established that the reason for the data

breach was an act within the organisation that does not qualify as malevolent. Further, it established that the data could be linked with the criminal personal data of the data subject and that it was possible to process the data for other purposes in an unfair manner.

The data subject was also notified with a delay after more than a month and because of this, it was only thereafter that action could be taken to have the registering authority to invalidate the documents (reducing the possibility of fraud) and to have them replaced. The Authority also took into account that the data breach affected a single person, no information was obtained of fraud with the documents and this was a case of a single negligent breach of data security. However, the Authority in its decision established an infringement of the rules concerning the management of the data breach. *(NAIH-266/2022)*

2.Personal data breach in the course of the use of covert means

In the course of a data breach notified to the Authority, a staff member of a police organ(hereinafter: Controller) wished to send document samples containing personal data generated in a jointly investigated case by e-mail to a colleague working with another police organ. However, after forwarding the e-mail, it was discovered that the document samples were sent to a wrong e-mail address. Although the Controller tried to contact the wrong addressee to provide information on the error on two occasions by e-mail, there was no reply to these e-mails, so it was not possible to establish whether the person using the account concerned in the erroneous transfer had access to the data in the document samples. The clarification of the facts of the case revealed that the document samples concerned in the data breach did not contain classified data, but the personal data of 13 data subjects (such as name, place and date of birth, mother's name and address, and in the case of 11 persons also the mobile phone number), including memos containing criminal personal data of these persons ordering the use of covert means against them, together with the related deployment schedule.

Within the framework of an authority procedure for data protection, the Authority examined the instructions of the Controller concerning the transfer of the data and data security applied in the course of electronic correspondence, as well as whether the Controller lawfully waived providing information to the data subjects of the data breach.

With regard to not informing the data subjects on data breach, the procedure clarified that it was omitted based on Section 25K(6) of the Privacy Act, citing an interest in investigating criminal offences. The criminal procedure against the data subjects was in progress also at the time of the Authority's procedure, they have not been indicted yet, hence providing information to them about the fact of the data breach would have been concomitant with letting them learn that covert means were used against them. Providing information on the fact of deployment and the evidence obtained from it would have provided an opportunity for the data subjects to hide evidence and demonstrate behaviour, which could have influenced the outcome and successful conclusion of the criminal procedure. The Authority established that the reason for waiving the provision of information existed on the basis of Section 16(3)(a) and (b) of the Privacy Act and it was not unlawful.

The Controller categorised the data breach in its notification as of limited risk. In view of the factors to be considered when assessing risk in the WP250 guidelines of the data protection working party of the European Data Protection Board set up according to Article 29 of Directive (EC) 95/46 of the European Parliament and of the Council of 24 October 1995 such as possible damage to reputation and the criminal personal data, which are also special category data jeopardized by the data breach and the circumstances of the breach, the Authority established that the impact of the data breach on the rights of data subjects was high. When assessing the risk, the Authority also considered that the attempt to reach the erroneous addressee was unsuccessful and that the indictment of the persons affected by the breach has not yet taken place in the course of the procedure. In view of this, access to the data concerned in the breach by a third person could damage the data subjects' right to good reputation because according to the information made accessible covert means were used against them due to the alleged commitment of criminal offences.

Following the examination of the internal instructions concerning data security requirements and measures and electronic correspondence applied at the Controller prior to the data breach, the Authority established that all the Controller had provided for with regard to the general practice of transferring data and transferring personal data electronically was that when transferring data it must be assured that the addressee of the transfer is indeed authorised to process the requested data and if the authorisation of the addressee cannot be established, the request to forward the data must not be fulfilled. The Relative to the appropriate data security controls that could be expected to prevent data breaches, the Authority regarded this provision of the Controller as insufficient and in ad-

equate. The Authority did not accept the arguments of the Controller that the prohibition of private correspondence through the e-mail addresses provided by the Controller implied that, in addition to private correspondence, the exchange or sending correspondence using private e-mail addresses was also prohibited. According to the Authority's position, the designation "private correspondence" does not refer to whether the addressee's e-mail address is private or official, but concerns the content of the letter. In terms of omitting to take other data security measures, according to the Authority's positions, the nature of the documents concerned in the breach would have ab ovo required the use of more intensive data security measures for several reasons, e.g. special category sensitive data, the threat of deconspiration, though in the event of electronically transferring the documents concerned in the breach, the minimum expected requirement would have been to send them at least encrypted or without showing the personal data.

The Authority established an infringement of the provisions of Sections 25/A(1) and 25/I of the Privacy Act, which gave rise to a personal data breach due to the inadequate data security measures of the Controller. As to the legal consequences, the Authority considered all the circumstances of the case and established that in the case of the infringements explored during the procedure the mere establishment of the infringement as a legal consequence is not, in itself, a proportionate sanction, so based on Section 61(1)(b)(bg) of the Privacy Act, it decided to impose a data protection fine on the Controller. When imposing the fine, the Authority considered that the data breach concerned persons against whom a criminal procedure was in progress, in the context of which documents containing identification data and particularly sensitive criminal personal data required to order the use of covert means were sent to an unauthorized third person. The Authority exposed systemic data security deficiencies in the processing by the Controller and found further that contrary to its own instructions, the Controller did not adequately consider encryption even in individual cases. *(NAIH-9095/2022).*

II.4. Data protection licensing procedures

Pursuant to GDPR Article 41, without prejudice to the tasks and powers of the competent supervisory authority, the monitoring of compliance with a code of conduct may be carried out by a body, which has an appropriate level of expertise in relation to the subject matter of the code and is accredited for that purpose by the competent supervisory authority. In accordance with the consistency mechanism; the Authority invited the opinion of the body on the draft of its criteria related to the accreditation of such organisations; the version drafted after this was published on the Authority's website.

Pursuant to GDPR Article 43, without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, certification bodies, which have an appropriate level of expertise in relation to data protection, shall after informing the supervisory authority in order to allow it to exercise its powers pursuant to point (h) of Article 58(2) were necessary, issue and renew certification. It should be noted that of the options offered by the regulation in Article 43(1) the Hungarian solution implements that mentioned in point (b), i.e. the National Accreditation Authority (NAH) in accordance with Regulation (EC) No. 765/2008 of the European Parliament and of the Council in accordance with EN-ISO/IEC 17065/2012, and with the additional requirements established by the Authority will carry out accreditations. The document drafted by the Authority, containing the supplementary requirements mentioned, has been accessible on the Authority's website in English since early last year; in the meantime the Hungarian translation of the document was also completed and it is also accessible on the website.

In 2022, the Authority completed its procedure for the approval of the first Binding Corporate Rules (BCR) submitted submitted to the Authority since the GDPR became applicable. As a result, following the procedure set forth in Guidelines 263 of the Working Party and under the data protection licensing procedure regulated in Section 34/A of the Privacy Act, the Authority approved the binding corporate rules submitted by MOL Nyrt.

II.5. Cooperation with the data protection authorities of the European Union and international affairs

II.5.1. Review of the cooperation procedures conducted pursuant to GDPR

Since the application of GDPR beginning in 2018, the Authority has taken an active part in the cooperation procedures according to Article 60 conducted with the Member States of the EEA. The one-stop access[11] serves the investigation of cases launched on the basis of complaints related to cross-border processing or ex officio.

Communication among the authorities related to the cooperation procedures is conducted in an interface specifically transformed for these procedures in the Internal Market Information System (hereinafter: IMI system).

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

The initiating authority may presume the lead supervisory authority based on the centre of operations or a single establishment of the controller/processor[12], which authority may accept or reject this role with the appropriate justification.[13] In addition, the Member States in which the controller/processor does not have a main establishment or establishment 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 2022, the Authority received 616 cases from the authorities of other Member States through the IMI system in roughly a quarter of which, the Authority found itself concerned. The Authority acted as the lead supervisory authority in 12 procedures and launched 8 procedures according Article 56 of its own during the same period.

11 GDPR Article 60

12 Based on GDPR Article 27 in the case of controllers or processors not having an establishment in the European Union.

13 GDPR Article 56(3)

Lead supervisory authorities investigate the complaint based on their own procedural rules and draft a decision in the given case. All the authorities concerned have an opportunity to add comments or relevant and reasoned objections to the draft decision within four weeks. If there are no objections to a draft decision, the lead supervisory authority sends the last version to all the Member State authorities as the binding decision.

If an authority concerned submits a relevant and reasoned objection or amending motion against a draft decision, the lead supervisory authority may produce a revised draft decision based on the recommendations, which the authorities concerned may comment on similarly to the earlier version in another four-week period. The lead supervisory authority may modify its draft decision until 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 2022, the Authority received 226 draft decisions to be studied, 17 revised draft decisions and 328 binding decisions. In addition, the Authority received 50 informal consultations to assist cooperation according to Article 60. During the same period, the Authority sent two draft decisions and two binding decisions to the other authorities under cooperation procedures.

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

In 2022, four such procedures were launched against the draft decisions of the Irish authority and the French authority. The Board closed all of these procedures with a binding decision according to Article 65. No dispute settlement procedure has yet been launched against any draft decision of the Authority.

The cooperation procedures include the mutual aid procedures and voluntary mutual aid procedures according to Article 61. While the former is a procedure subject to stringent formal requirements to be performed within a given period of time generally conducted 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 supplying and obtaining information, inquiries in investigative procedures and general consultation.

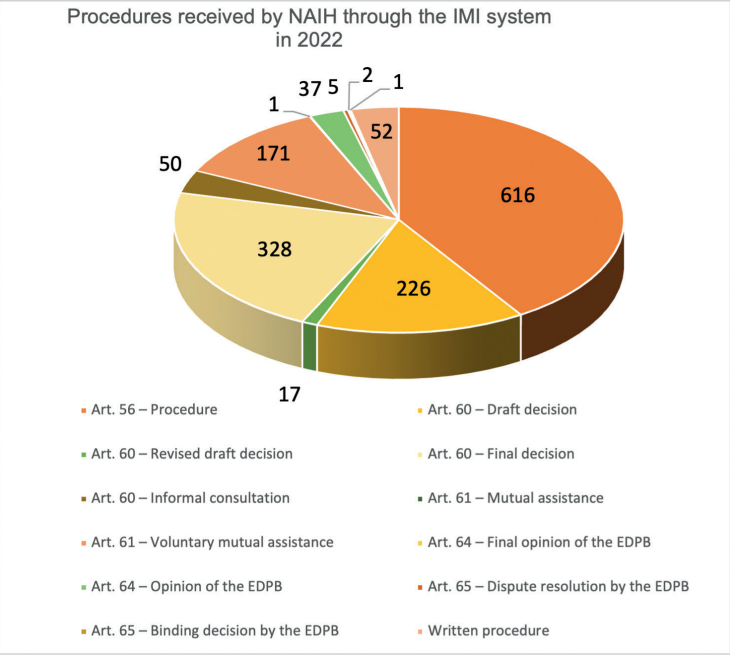
In 2022, the Authority received 171 requests for voluntary mutual aid and none for mutual (mandatory) aid. During the same period, the Authority initiated 5 mutual aid procedures and 9 voluntary mutual aid procedures.

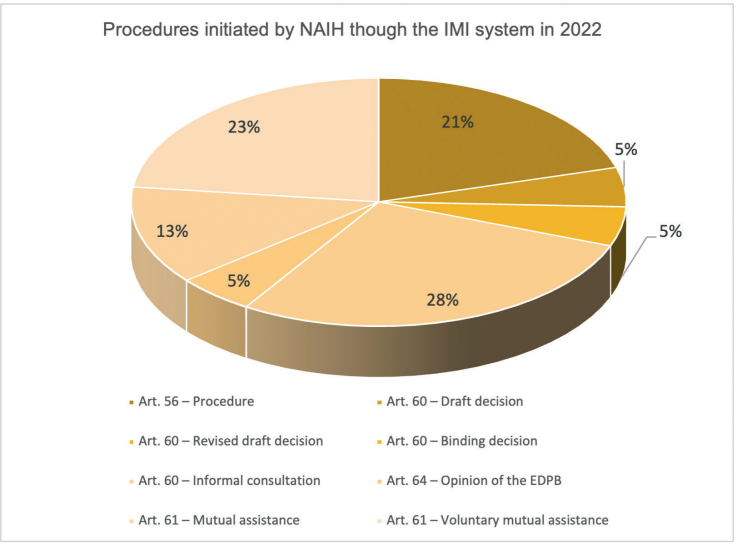
Although not closely related to the procedure according to Article 60, the opinions of the Board according to Article 64 should also be mentioned, of which 37 were received by the Authority in 2022, one of which was a Board decision according to Article 64.

In relation to cooperation among Member State authorities, 53 written procedures handled by the Authority in 2022 should be stressed; these are votes cast in the IMI system to streamline the agenda of the plenary sessions of the Board.

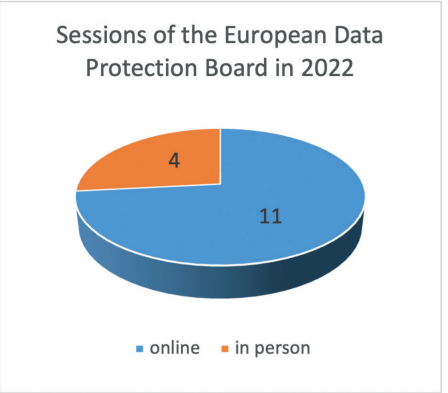
Based on the statistics kept since GDPR became applicable in May 2018, it can be stated that the trend, beginning in 2021, continues to prevail, according to which the main emphasis of the procedures among Member State authorities is shifting from the identification of the lead supervisory authority towards cooperation and communication.

Cases in 2022

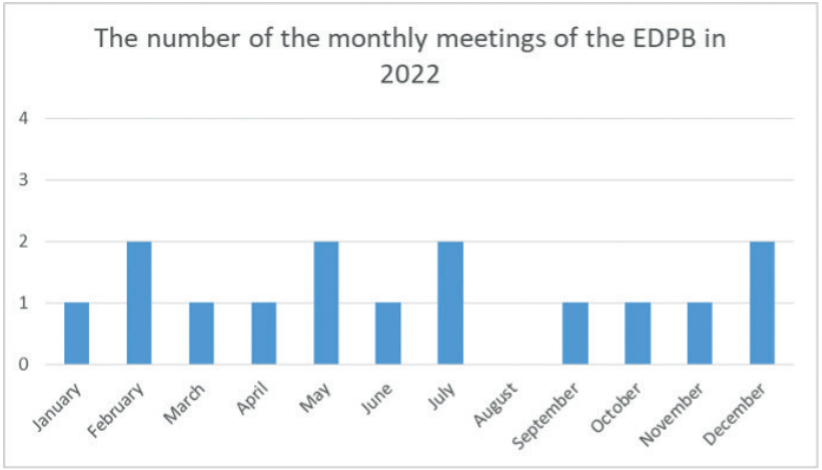


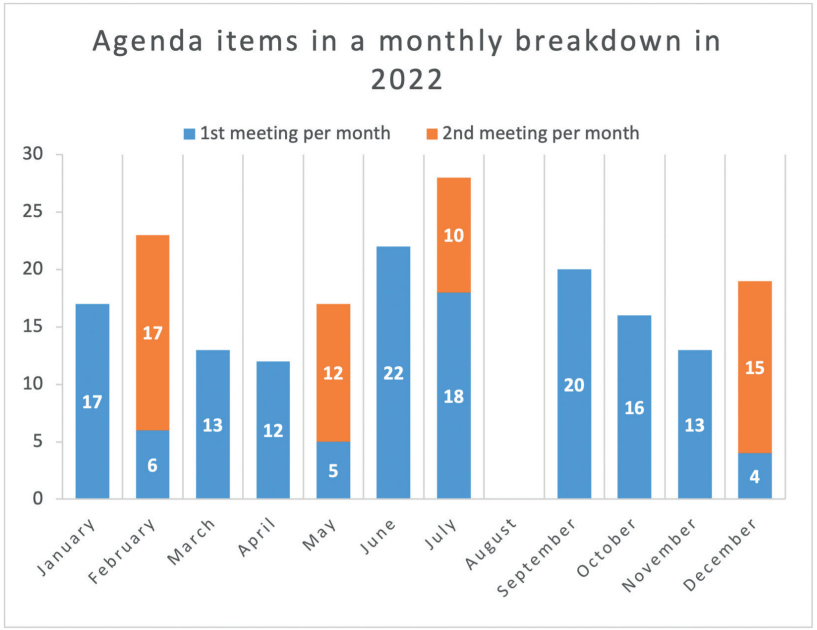


The Authority's participation in the activities of the European Data Protection Board – statistics



Altogether, 15 plenary sessions were held in 2022. Of the 15 sessions held, 4 were in person meetings in Brussels, while 11 were organised as video conferences. Although, online sessions were predominant in the first half of the year, half of the plenary sessions were organised in person from June; presumably, the other expert groups will also follow this trend in 2023. The European Data Protection Board discussed 200 agenda items in its 15 plenary sessions, which on average means the discussion of 13.3 agenda points/session, which is more than last year.





II.5.2. Dispute settlement procedures

1. *The ACCOR SA case*

The European Data Protection Board (hereinafter: EDPB) closed the dispute settlement procedure according to GDPR Article 65(1)(a) conducted in the case of the controller ACCOR SA with its binding decision under No. 01/2022 at its plenary session held on 14-15 June 2022. The Polish Data Protection Authority submitted a relevant and reasoned objection (hereinafter: objection) against the draft decision of the French Data Protection Authority as lead supervisory authority. In the basic case, the French Authority would have imposed an administrative fine on the grounds of the violation of the right to object to which data subjects are entitled with regard to personal data processed in the context of marketing activities and rendering the exercise of the data subject's right to access more difficult; however, the Polish Supervisory Authority deemed that the amount of the fine was too low and submitted an objection. According to the EDPB decision:

i. In determining the amount of the fine, the lead supervisory authority has to consider the turnover data of the controller for the year preceding the adoption of the authority decision and not the turnover data of the year preceding the infringement.

ii. The lead supervisory authority need not check the solvency of the controller, however, in order to ensure that the fine is proportionate; it has to take into account ACCOR's financial situation based on the relevant turnover data of this undertaking.

iii. As according to EDPB's position, the amount of the fine originally proposed to be imposed did not comply with GDPR Article 83(1) in terms of its dissuasive force, it ordered the French Authority to review the amount of the fine proposed to be imposed in the light of the above.

Based on EDPB's decision, the French Supervisory Authority imposed an administrative fine on ACCOR SA to a total amount of EUR 600,000.

2. *The Meta case*

EDPB closed the dispute resolution procedure according to GDPR Article 65(1)(a) launched in the Instragram case with its binding decision 02/2022 made

at its session of 28 July 2022. In the basic case launched ex officio, the Irish Supervisory Authority as lead supervisory authority investigated the compliance of processing by Meta IE operating the Instagram platform in the light of GDPR Article 5(1)(a) and (c), Article 6(1), Article 12(1) and Articles 13, 24, 25, and 35 with regard to processing when, under certain circumstances, the controller made certain personal data of under-age Instagram users (e-mail address and/or phone number) accessible to business Instagram accounts, moreover, this was included as a default setting. The German, French, Italian, Dutch and Norwegian supervisory authorities submitted objections to the draft decision of the Irish authority. EDPB established that:

i. Processing the e-mail addresses and/or phone numbers of children using a Instagram business accounts is not necessary for providing the Instagram service [legal basis according to GDPR Article 6(1)(b)], and with regard to legitimate interest cited as an alternative legal basis of processing, EDPB declared that processing based on the legitimate interest of the controller failed to comply with the requirements set forth in GDPR Article 6(1)(f). EDPB ordered the Irish Supervisory Authority to modify its draft decision and establish the infringement of GDPR Article 6(1).

ii. EDPB ordered the Irish Authority to revise the amount of the administrative fine originally proposed to be imposed to ensure that the final amounts of the administrative fines are effective, proportionate and dissuasive in accordance with GDPR Article 83(1).

Based on EDPB's decision, the Irish Supervisory Authority imposed an administrative fine on Meta IE totalling EUR 405 million.

3. *The Facebook and Instagram case*

EDPB closed the dispute resolution procedures according to GDPR Article 65(1)(a) with its binding decisions 03/2022 (Facebook) and 04/2022 (Instagram) made at its session of 5 December 2022. In very similar cases in terms of the legal issues under investigation, the Irish Authority acted as lead supervisory authority based on a complaint by persons represented by NOYB, a human rights organisation, as the personal data of the Facebook and Instagram users in the European Economic Area are processed by Meta Platforms Ireland Limited as it is currently known (hereinafter: Meta IE). The complaints were primarily focused on the fact that in 2018 the only choice offered to registered users was to accept the Terms and Conditions of Use and the related Privacy Statement amended with regard to GDPR or to delete their profile, i.e. "their consent" to processing was invalid. The Austrian, German, French, Italian, Dutch, Norwegian, Polish, Swedish, Spanish, Finnish and Hungarian supervisory authorities submitted objections to the draft decision of the Irish authority. Owing to the similarity of the facts of the cases, the essential points of EDPB's decision were the following in both cases:

i. Processing related to behaviour-based advertisements displayed for users is not necessary for performing the user contracts entered into between Meta IE and the users as it does not constitute an essential element of the content of the contracts, hence Meta IE unlawfully relied on GDPR Article 6(1)(b) when processing the users' personal data. Because of this, EDPB ordered the Irish Authority to impose an effective, proportionate and dissuasive administrative fine compliant with GDPR Article 83(1) and to order Meta IE to bring its processing in line with GDPR Article 6(1).
ii. EDPB ordered the Irish Authority to launch a new investigation to establish whether Meta IE processes data in the special categories of personal data and whether it meets its obligations relevant to this based on GDPR.
iii. EDPB ordered the Irish Authority to establish an infringement of the principle of fair processing and to apply appropriate sanctions.
iv. It ordered the Irish Authority to determine the amount of the administrative fine proposed to be imposed on account of the infringement of the principle of transparency in a higher amount so as to comply with GDPR Article 83(1) and (2).

Based on EDPB's decisions, the Irish Supervisory Authority imposed a fine of EUR 210 million on Meta IE for the infringements related to Facebook and of EUR 180 million for infringements related to Instagram.

4. *The WhatsApp case*

In his complaint, a person represented by NOYB, a human rights organisation, objected to the fact that in May 2018 the controller Whatsapp Ireland Limited IE (hereinafter: Whatsapp IE) operating the Whatsapp messaging application essentially forced the consent of already registered users to further processing as the only choice offered to them was to accept the Terms and Conditions of Use and the related Privacy Statement or to delete their profiles. The Irish Supervisory Authority took action based on the complaint as lead supervisory authority; the German, Finnish, French, Norwegian, Dutch and Italian supervisory authorities

submitted objections to its draft decision. As, according to the position of the Irish Supervisory Authority, these objections failed to meet the relevant requirements of form and content, a dispute resolution procedure was launched in the case in accordance with GDPR Article 65(1), which was closed by EDPB with its binding decision 05/2022 made on 5 December 2022. According to the EDPB's decision:

i. GDPR does not allow Whatsapp IE to cite a legal basis according to GDPR Article 6(1)(b) for the purpose of processing for service development and the improvement of security functions, because these are not essential elements of the contract between the users and Whatsapp IE; therefore EDPB ordered the Irish Authority to establish the infringement of GDPR Article 6(1) to impose an administrative fine and order Whatsapp IE to bring its processing operations carried out to develop the service and ensure its security in line with the provisions of GDPR Article 6(1).
ii. Whatsapp IE presented the legal basis of its processing in a misleading way to users; also, users did not receive adequate information with regard to the interrelations between the purpose of processing, the legal basis to be applied and the related processing operations; because of this, EDPB ordered the Irish Authority to determine the infringement of the principle of fair processing as set forth in GDPR Article 5(1)(a) in its decision.
iii. According to EDPB's position, the Irish Authority did not carry out a sufficiently thorough investigation relative to the content of the complaint because it failed to investigate the legal basis of several processing operations objected to, hence it ordered the Irish Authority to conduct additional investigations.

Based on EDPB's decision, the Irish Supervisory Authority imposed a fine of EUR 5.5 million on Whatsapp IE.

II.5.3. The activities of the European Data Protection Board and its most important guidelines adopted in 2022

1. *Guidelines 03/2022 on deceptive design patterns in social media platform interfaces*

The 2022 work schedule of the "Social media" expert subgroup of the European Data Protection Board included the drafting of guidelines on deceptive design patterns in social media platform interfaces, whose social consultation also took place that year. The final version of the guidelines will be submitted to the Board for adoption in 2023 after the consultation.

The guidelines offer practical recommendations to the designers and users of social media platforms about how to assess and avoid the deceptive patterns of social media platform interfaces, which violate the GDPR requirements.

In the context of the Guidelines, "deceptive design patterns" are considered as interfaces and user experiences implemented on social media platforms that lead users into making unintended, unwilling and potentially harmful decisions regarding the processing of their personal data. The purpose of deceptive designs is to influence user behaviour. Deceptive designs can hinder the users' ability to effectively protect their personal data and make conscious choices with regard to their processing. Data protection authorities are responsible for sanctioning the use of deceptive design patterns, if they breach GDPR requirements.

The guidelines state that the provisions of GDPR apply to all personal data processing carried out in the course of the operation of the social media platforms, i.e. to the entire life cycle of user accounts. The guidelines present the deceptive patterns through specific examples along the life cycles of user accounts.
In addition to examples of deceptive patterns, the guidelines also present proven practices. The guidelines also contain specific recommendations for designing user interfaces that facilitate the effective implementation of GDPR.

2. *Guidelines 06/2022 on the practical implementation of amicable settlements*

The European Data Protection Board accepted the guidelines on amicable settlements back in 2021, which was then an internal document. In 2022, the "Cooperation" expert subgroup of the European Data Protection Board recast the internal document into guidelines, addressing certain issues of the practical implementation of amicable settlements. The guidelines also specified the relevant steps arising in relation to amicable settlement in its Annex 1, providing guidance to Member State authorities where the institutions of amicable settlement are recognised. In addition, the guidelines contain a list of countries that do not recognise the institution of amicable settlement in its Annex 2.

3. Guidelines on the application of Article 60 GDPR - one-stop shop

The 2022 work schedule of the "Cooperation" expert subgroup of the European Data Protection Board also included the drafting of guidelines on the application of Article 60 GDPR.

With the introduction of the GDPR, the concept of the one-stop shop was established as one of the main innovations. In crossborder processing cases, the supervisory authority in the Member State of the controller's or processor's main establishment is the authority leading the enforcement of the GDPR for the respective crossborder processing activities in cooperation with all the authorities which may face the effects of the processing activities at stake, be it through the establishments of the controller or processor on their territory, or through complaints from their residents against these processing activities. Data subject should be able to easily pursue their data protection rights and should be able to complain to a supervisory authority at their place of habitual residence. This supervisory authority also remains the contact point for the complainant in the further course of the complaint handling process. In order to meet all these requirements, Article 60 GDPR regulates the cooperation procedure between the lead supervisory authority and the other supervisory authorities concerned.

These guidelines handled the interactions of the supervisory authorities with each other, with the European Data Protection Board and with third parties under Article 60 GDPR. The aim is to analyse the cooperation procedure and to give guidance on the concrete application of the provisions. The guidelines also contain an annex entitled "Quick reference guide" providing a quick review of the steps of the procedure.

4. Guidelines of the European Data Protection Board on certification as a tool for transfers to third countries

In 2022, the European Data Protection Board (EDPB) adopted the guidelines on certification as a tool for transfers.[14] Through the accreditation of the certification body and the approval of the certification mechanism, certification may also serve the purpose of providing adequate safeguards to controllers and processors when transferring data to third countries.

14 Currently, it is only accessible in English: https://edpb.europa.eu/system/files/2022-06/edpb_guidelines_202207_certificationfortransfers_en_1.pdf

The guidelines contain useful guidance for certification bodies, supervisory authorities, EDPB, as well as the Commission.
The guidelines address the following four main subjects:

i. Definition of the scope of the guidelines and their actors.
ii. Criteria to verify the requirements that the certification body has to comply with, in order to properly regulate the transfer of data under the appropriate safeguards under Article 46 of the GDPR, beyond those set out in EDPB Guideline 4/2018 and ISO 17065
ii. Special criteria concerning the certification requirement, whose purpose is to guarantee the appropriate safeguards needed for transfer.
iv. The rules of commitments to be undertaken by controllers and processors not subject to GDPR by way of contracts or other legally binding instruments about applying the appropriate safeguards, including those applicable to the rights of the data subjects based on GDPR Article 42(2).

The guidelines also contain examples of certification criteria, additional individual certification criteria and supplementary measures irrespective of whether they are applied by the transferor or the transferee.

5. European Data Protection Board Guidelines on codes of conduct as tools for transfers

In 2022, the European Data Protection Board (EDPB) adopted the guidelines on codes of conduct as tools for transfers.[15]
Once the competent lead supervisory authority approved the code of conduct and after approval by the Commission, it gained general validity in the EU based on GDPR Article 40(9), the code may also serve the purpose of providing appropriate safeguards to controllers and processors in the course of transfers to third countries (see the provisions of GDPR Article 46(2)(e)).

The guidelines contain useful guidance for the organisations wishing to develop a code of conduct, the supervisory authorities, EDPB, as well as the Commission. In addition to the general explanation, the finalised document endeavours to throw light on the content that should be included in the codes, the main actors and their roles and what guarantees a code should include through practical examples.

15 Accessible in Hungarian: https://edpb.europa.eu/system/files/2022-10/edpb_guidelines_codes_conduct_transfers_after_public_consultation_hu.pdf

The guidelines concern the following five main topics:

i. Specification of the scope of the guidelines.
ii. A checklist defining a minimum level of requirements on the basis of which it can be checked, what elements the code of conduct has to contain in order to regulate transfers based on appropriate safeguards according to GDPR Article 46.
iii. Specification of the minimum requirements related to guaranteeing data subjects' rights.
iv. The process of providing opinions on and adopting the code of conduct by the lead supervisory authority and EDPB, and the procedure of the Commission for making the code generally applicable in the EU.
v. Data subjects' right to complain and the procedure for doing so, if the infringement of rights arises in connection with transfers to a controller in a third country. In this context, the guidelines also take into account the Standard Contractual Clauses recently published by the Commission.

6. Guidelines on data subjects' rights - right of access

The Key Provisions expert group of the European Data Protection Board (hereinafter: KPESG) has an outstanding role in facilitating the uniform interpretation of GDPR. Its primary task is to develop general guidelines to facilitate the uniform interpretation and application of European Data Protection legal regulations in particular GDPR and the Law Enforcement Directive. KPESG involves those applying the law and other experts in its work in the form of social consultations. The 2022 work schedule of KPESG included the drafting of the guidelines on data subjects' rights - right of access (GDPR Article 15), whose social consultation took place in 2022. KPESG is currently evaluating its results and will adjust the final text accordingly. The general purpose of the right of access is that individuals receive sufficient, transparent and easy to access information on the processing of their personal data and to enable them to be aware of and check the lawfulness of processing and the accuracy of the data.

The data subject need not justify an access request and it is not up to the controller to analyse whether the request indeed assists the data subject in assessing the lawfulness of the relevant processing or in the exercise of other rights. The controller has to accept the request, unless it is clear that it was submitted on the basis of rules other than the data protection rules. The mode of providing access may change depending on the quantity and complexity of the data. Unless it expressly provides otherwise, the request applies to all the personal data of the data subject, however, in certain cases the controller may request the data subject to clarify his request. GDPR allows certain restriction of the right to access. The approval and adoption of the finalised text of the guidelines by the Board is expected in 2023.

7. Guidelines 04/2022 on the calculation of administrative fines under the General Data Protection Regulation

The European Data Protection Board (EDPB) endeavours to harmonise the methodology applied by supervisory authorities in calculating the amount of fines. For this purpose, it adopted and issued for public consultation guidelines 04/2022[16] These guidelines supplement the previous guidelines on the application and setting of administrative fines (WP253)[17], which focuses on the valuation criteria to be taken into account when imposing a fine.

The calculation of the amount of the fine is at the discretion of the supervisory authority subject to the rules provided for in the General Data Protection Regulation. Because of this, the calculation of the amount of fine is in each case based on individual assessment carried out on the basis of the parameters specified in the General Data Protection Regulation. Taking all this into account, the European Data Protection Board developed the following five-step methodology to calculate the amount of the administrative fines imposed in the event of breaching the General Data Protection Regulation.

i. First, in accordance with Article 83(3) of the General Data Protection Regulation, the processing operations to be assessed and the relationship between possible concurrent infringements have to be determined.

ii. The second step is the identification of the starting point for the calculation of the amount of the fine: the classification of the infringement in accordance with the General Data Protection Regulation, the severity of the infringement and the size of the undertaking.

iii. The third step is the assessment of the aggravating and mitigating circumstances related to the past or present behaviour of the controller/processor and increasing or decreasing the fine accordingly.

16 https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-042022-calculation-administrative_en

17 https://ec.europa.eu/newsroom/article29/items/611237

iv. The fourth step is identifying the relevant maximum penalties for the different infringements. Increases applied in the previous or subsequent steps may not exceed this maximum amount.
v. Finally, it needs to be analysed whether the calculated final amount meets the requirements of effectiveness, dissuasiveness and proportionality. The fine can still be adjusted accordingly, but without exceeding the relevant legal maximum.

8 The activities of the Board in relation to transfers to the United States of America

101 TF is an ad hoc working party of the European Data Protection Board (EDPB), which examines complaints submitted following the Schrems-II judgment[18]. Altogether 101 complaints of very similar content were submitted to the European data protection authorities against several controllers in EEA Member States because of the use of Google/Facebook services concomitant with the international transfer of personal data. In these, the complainant represented by NOYB – European Digital Rights (EDRi) – claim that Google/Facebook transfer personal data to the United States relying on the EU-USA data protection shield or the Standard Contractual Clauses, while according to the Schrems-II judgement, the controller is unable to guarantee the appropriate protection of the personal data of the complainants. The 101 TF analyses the cases and ensures close cooperation among the supervisory authorities concerned.

Some of the complaints mentioned concerned controllers within the jurisdiction of the Hungarian Data Protection Authority, hence NAIH is also a member of the 101 TF working party. As a result of NOYB's submission, NAIH investigated the use of Google Analytics on the website of the controller based on Section 38(3) (a) of Act CXII of 2011 on the Right of Informational Self-Determination and the Freedom of Information as part of an inquiry procedure. As a result of its inquiry, NAIH found that the given website unlawfully transfers data to the United States of American when using Google Analytics infringing Article 28(1) of the General Data Protection Regulation.

The adoption of a new adequacy decision may bring about a change in the legal assessment of transfers to the United States. On 13 December 2022, the European Commission launched a process for the adoption of an adequacy

18 Judgement of the Court of Justice of the European Union in case C-311/18. Additional information: https://edpb.europa.eu/sites/default/files/files/file1/20200724_edpb_faqoncjeuc31118_hu.pdf

decision, a new EU-USA Data Privacy Framework. The goal is to facilitate the transatlantic data flow while managing the concerns of the Court of Justice of the European Union in its Schrems-II judgement. The draft of the adequacy decision was forwarded to the European Data Protection Board, which is going to develop its opinion on the draft and the adequacy of the level of protection in accordance with Article 70(1)(s) of the General Data Protection Regulation. The adoption of the new adequacy decision is expected in mid-2023.

In the absence of an adequacy decision, the other instruments detailed in the General Data Protection Regulation are available to controllers and processors for international data transfers. These include the binding corporate rules (BCR), whose approval may be requested[19] from the Authority.

II.5.4. Participation in the joint supervisory activity of data protection authorities

1. Working group supervising data protection in the Schengen Information System (SIS II Supervision Coordination Group)

Originally it was envisaged that the SIS II working group would hold its last meeting in June 2022, whereafter its tasks would have been taken over by the Coordinated Supervision Committee (CSC) established in 2019; however, its due date was already twice modified, the latest due date for the entry into force of the new SIS regulation is 7 March 2023.

In 2022, data subjects turned to the Authority with regard to the processing of personal data stored in SIS II on 69 occasions. The majority of these requests was an issue related to the exercise of data subject's rights (request for information, data correction, erasure), in which cases the Authority provided general information to the data subjects concerning the right and the process of contacting the SIRENE Office and about the available legal remedies. The Authority launched inquiries based on data subjects' complaints in four cases and in two cases transferred the case to the competent organ.

19 https://www.naih.hu/nemzetkozi-adattovabbitas-bcr/mit-jelent-a-kotelezo-ereju-vallalati-szabalyozas-bcr

2. *Preparation for Hungary's evaluation for data protection under the Schengen Convention due in 2024*

The tasks specified in the action plan according to Article 16 of Regulation (EU) 1053/2013 for the implementation of the Commission's recommendations drafted on the basis of the onsite evaluation visit of 6-11 October 2019 concerning Hungary's tasks related to data protection were successfully carried out by the Authority by the agreed due date in December 2022. At the same time, the Authority began preparations for the next onsite evaluation visit to Hungary concerning data protection due in 2024.

3. *Participation of the Authority in the Schengen evaluation and monitoring mechanism*

The Authority took an active part in the expert activities according to Article 18(3) of Regulation (EU) 2022/922 on the establishment and operation of an evaluation and monitoring mechanism to verify the application of the Schengen acquis in 2022. Four Member States were subject to Schengen evaluations in 2022, and staff from the Authority were included among the members of the expert delegation designated for monitoring data protection in two of them (Norway and Iceland).

4. *Working group supervising data protection in the Visa Information System (VIS Supervision Coordination Group)*

In 2022, the working group supervising data protection in the Visa Information System (VIS Supervision Coordination Group) held two meetings. 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.

In 2022, the working group worked on the development of a joint audit plan, which would include a set of questions related to the data security of the Visa Information System, as well as questions related to the data protection supervision of external service providers, which could be used by each Member State similarly to the SIS II joint audit plan for their own supervisory activities. In addition, the working group is examining the possibility of enabling the authorities of the individual Member States to carry out coordinated joint onsite inspections in the future at both the consulates and the external service providers contracted by them.

In 2022, the Authority received 10 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, requests concerning specific cases were sent by the Authority to the competent body.

5. *Working group supervising data protection in the Eurodac System (Eurodac Supervision Coordination Group)*

The working group supervising the data protection of the Eurodac System (Eurodac Supervision Coordination Group) met twice in 2022. The work of the Eurodac SCG is greatly impacted by the fact that the review of the Eurodac regulation continues to be in suspense. As it is well-known, the improved Eurodac database will become fully interoperable with the border administration databases as part of an integrated migration and border administration system, assisting the management of illegal migration.

Although the review of the Eurodac regulation is yet to come, the working group developed a joint reporting mechanism, whose objective is not to double the work already began with the establishment of the joint audit plan but to provide an effective instrument enabling the comparison of the findings of supervisory activities carried out by the supervisory authorities at national level.

6. *Coordinated Supervision Committee – CSC*

In recent years, the large-scale EU information systems connecting the authorities of the EU Member States and the EU bodies have undergone a great deal of development. The EU bodies and the national authorities share personal data with one another electronically through these systems at an unprecedented speed and volume. In order to ensure that data processing operations are in line with the data protection framework system of the EU, there is a dual supervision in place: the European Data Protection Supervisor (EDPS) supervises the EU agencies processing personal data, while the national data protection supervisory authorities supervise the processing of personal data by the competent national authorities (e.g. public administration, police, border protection authorities). For this reason, the coordination of the supervisory authorities of the EDPS and the national supervisory authorities is indispensable. With the entry

into force of Regulation (EU) 2018/1725 in December 2019, the Secretariat of the committee looking after the cooperation between the EDPS and the national supervisory authorities, the Coordinated Supervision Committee (CSC) is provided by the European Data Protection Board (EDPB). CSC became the body coordinating supervision with regard to the Internal Market Information System (IMI), Eurojust, the European Public Prosecutors Office (EPPO) and Europol. The coordinating activities of CSC are expanding on an ongoing basis and in the future will extend to the supervision of additional systems, such as cooperation in border, asylum and migration affairs (SIS, EES, ETIAS and VIS), police and judicial cooperation (SIS, ECRIS-TCN) and the large-scale IT systems under the next generation Prüm Convention[20].

Within the framework of its activities to ensure the coordinated supervision of the large-scale IT systems and EU institutions, agencies and bodies, the members of CSC share information with one another, assist national supervisory authorities in carrying out audits and investigations and examine the eventually arising issues and problems related to the interpretation and application of the EU legal acts establishing the large-scale EU IT supervisory systems. CSC also investigates problems related to supervisory work or the exercise of data subjects' rights and develops coordinated recommendations for solving the problems and for facilitating awareness raising in the exercise of data subjects' rights.

7. Working group supervising data protection in the Customs Information System (Customs Information System - Supervision Coordination Group)

The task of the working group is the coordinated supervision of the Customs Information System (CIS) from the viewpoint of data protection with the participation of the data protection authorities of the Member States and the European Data Protection Supervisor. The purpose of the Customs Information System is to facilitate the prevention, detection and prosecution of the violation of the EU customs and agricultural rules. The heart of the system is a central database, to which Member State authorities can have access through a dedicated interface for uploading data and making queries.

20 Council Decision 2008/615/JHA OF 23 June 2008 on the stepping up of crossborder cooperation, particularly in combating terrorism and crossborder crime

8. Borders, Travel and Law Enforcement Expert Group (BTLE)

On 12 May 2022, the European Data Protection Board discussed the guidelines on the use of facial recognition technology in the area of law enforcement (hereinafter: Guidelines) and adopted unanimously.

The use of facial recognition technologies involves the processing of exceedingly large volumes of personal data, including special category data. A face and in general biometric data ultimately and irrevocably relate to the identity of a person. Because of this, the use of facial recognition has direct or indirect impact on the fundamental rights stipulated in the European Union Charter of Fundamental Rights (hereinafter: the Charter).

The European Data Protection Board is well aware that law enforcement authorities have to make use of the best possible means to rapidly identify the perpetrators of terrorist acts and other serious criminal offences. These means may, however, be used only in stringent compliance with the legal framework and only in cases when they comply with Article 52 of the Charter. Certain cases of use of facial recognition technologies constitute unacceptably high risk for both individuals and society. For these reasons, the European Data Protection Board (EDPB) and the EDPS had earlier called for a general prohibition[21].

In particular, the remote biometric identification of individuals in publicly accessible spaces poses a high risk of intrusion into the individuals' privacy and it has no place in a democratic society, because such cases are concomitant with massive surveillance by definition. According to EDPB's position, AI supported facial recognition systems, which use individuals' biometric data to sort them into clusters according to ethnicity, gender, as well as political or sexual orientation cannot be reconciled with the Charter. EDPB is convinced that the use of AI to guess the emotions of a natural person is highly undesirable and apart from sufficiently justified exceptions should be prohibited. EDPB also argued that the processing of personal data for law enforcement purposes relying on databases created by the massive and unselected collection of personal data, particularly if accessible through social networks, does not comply with the stringent requirements of EU law in terms of necessity and proportionality.

21 See EDOB-EDPS joint opinion 5/2021 on the proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).

9. Europol Cooperation Board (ECB)

Europol supports the work of the Member States' law enforcement authorities by collecting data, analyses, sharing data and coordination in combating international organised crime and terrorism. Until 2022, the task of ECB was to assist this work with consulting. However, in 2022 ECB was terminated, its last meeting took place on 31 May. Its tasks were taken over by the Coordinated Supervision Committee (CSC). From then on, the scope of CSC covers the entire area of police and judicial cooperation. It is hard to foretell whether this concentrated operation will promote effectiveness in the future, or to the contrary, less attention will be paid to exploring the data processing problems of the individual areas because of the complexity of the task.

At the last meeting of ECB, Europol's data protection officer reported on the general situation of data protection work, the cooperation with Member State authorities and the current situation of requests concerning the exercise of data subjects' rights to the working group. In addition, the working group was informed of a new project, the European Police Records Index System (EPRIS) which, when completed, will enable automatic data exchange also with regard to biometric and special category data with respect to all the actors of criminal procedures. ECB established that there are still many unclarified issues related to the project and its operation, for instance the infrastructure required for implementation is huge, it is not easily accessible because of its complexity and the proportionality of the planned processing is yet to be examined, requiring preliminary impact studies.

The Authority has participated in the work of ECB and will continue to play an active part in implementing the tasks affecting this area within the framework of CSC. In 2022, the Authority ex officio launched an inquiry concerning Europol in the context of the tasks of ECB to facilitate ECB's work.

10. International Intelligence Oversight Forum (IIOF)

The International Intelligence Oversight Forum (IIOF) held its annual event in Strasbourg in 2022, where in addition to independent bodies performing national security supervision and parliamentary committees, the staff members of national security agencies and national data protection authorities, academicians studying the field and the representatives of an NGO also participated. The fifth IIOF conference was held in the Palais de l'Europe. The forum is by invitation only, is private and the information presented at the Forum was confidential; therefore, no minutes of the plenary session or of the thematic meetings were drafted.

11. The European Entry/Exit System (EES) and the European Travel Information and Authorization System (ETIAS) working group

The Authority participated in the work of the working group run by the Ministry of the Interior coordinating the governmental measures for the development of the European Entry/Exit System (EES) and the European Travel Information and Authorization System (ETIAS). According to Government Decision 1538/2018. (X.30.), the working group was in charge of the following tasks:

1. Harmonization of governmental measures for the implementation of the national part of the European Entry/Exit System (EES) and the European Travel Information and Authorization System (ETIAS),
2. Harmonization of governmental measures for the implementation of the national part of the Schengen Information System (SIS),
3. Harmonization of governmental measures for the implementation of the national part of the centralized system for the identification of Member States having information on judgments against third country nationals and stateless persons (ECRIS-TCN),
4. Harmonization of governmental measures for the implementation of the national part of the requirements in the legal acts of the European Union on establishing an interoperability framework between Union information systems,
5. Monitoring and preparation for the application of EES, ETIAS, SIS and ECRIS-TCN, and for interoperability, and
6. Harmonization and preparation of governmental measures and decisions for the development of the national part of EES, ETIAS, SIS and ECRIS-TCN and interoperability.

Unfortunately, for the time being, it cannot be stated with any certainty when these projects requiring serious preparation and intensive cooperation between Member States and the state entities within the Member States will be implemented; they will, however, bring about substantial advances in the security of the European Union. All in all, it can be said that Hungary is proceeding according to plan with implementation, however the Justice and Home Affairs Council of the European Union has already been forced to adopt new schedules for implementation on several occasions leading to multiple modifications of the projects and dates. Typically, the reason for this was delay by EU level suppliers or

delay by the general contractors and difficulties in procuring certain indispensable IT devices.

II.5.5. Digital sovereignty and the digital strategy of the European Union

Currently, Europe attempts to achieve digital sovereignty through the merger of two main instruments: regulation and innovation. Through regulation, Europe aims to create a digital space where the rights of the various stakeholders are balanced and are respected.

Importantly, European level digital sovereignty requires action against data monopolies, whose main establishments are outside the EU, using the instruments of law on the one hand, and the development of the EU's own capacities and technology, so that there be genuine EU alternatives on the other hand. In the meantime, the appropriate protection of the fundamental rights must be ensured against risks outside the EU, as well as internal risks in accordance with the Charter of the European Union and the EU legal regulations in force.

Based on the above, the enhancement of digital sovereignty requires the parallel enforcement of two frequently competing interests as technical innovation and the protection of fundamental rights can lead to the enhancement of digital sovereignty only together.

To address this situation, the EU regulation as a source of law provides a directly applicable uniform basis across the EU that reduces existing differences between Member States.

To manage this situation, the EU is enacting a number of legislation at regulation level, and the number is growing. The EU regulation, which is directly applicable in the entire territory of the EU, provides for a uniform basis levelling out existing differences among the Member States.

The European Commission has set out to renew the entire EU digital sector through the announcement of its exceedingly ambitious digital package published on 19 February 2020.

A part of the digital package is the regulation of the digital market through the Digital Services Act (DSA)[22] and the Digital Markets Act (DMA)[23] already adopted. They introduce a single and transparent set of rules across the EU, which are more predictable for both market agents and EU citizens, through which the legislator intends to improve the competitiveness of smaller undertakings and better protect fundamental rights.

Another part of the digital package is the Artificial Intelligence Act (AI Act) still subject to debate, which aims to regulate AI technology, that frequently functions as a black box and is hardly transparent, or not at all, but is indispensable for development and digital sovereignty. Through this, it will be possible to develop a more transparent AI with safeguards, with more direct state involvement through the supervisory authorities. As with all the legal regulations in the digital package, the main objective is to make the results available to the widest possible audience, to prevent the emergence of monopolies, which are also important elements of digital sovereignty. EU Member States are much more vulnerable, if - as currently - a few very large actors have far too great and unavoidable influence over the digital world; and it is in the national security interest to stop this.

The issue of online identification is also important for the purposes of digital sovereignty. It is a classic public task to issue identity documents to citizens, providing them with authentic proof of their identity. To date, this has only worked offline, although there are a few isolated online identification services of limited use (e.g. in public administration) (such as the customer gateway or company gateway); however, these generally operate only within a given Member State. With the Internet and the EU single market, such online identifiers valid only in a given Member State are unsuitable for use in the private sphere; currently, only non-state actors offer such universal identification services with scant state control and dubious creditworthiness (e.g. identification with Facebook or Google accounts on websites). The amendment of the eIDAS regulation[24] is in progress

22 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a single market for digital services and amending Directive 2000/31/EC (Digital Services Act)

23 Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and the amendment of Directives (EU) 2019/1937 and (EU) 2020/1828

24 Regulation (EU) 910/2014/EU of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

to address this situation; its goal is to develop a single European digital identification system that can be universally used which, in contrast to the situation to date, would provide identification hitherto provided by the state typically offline subject to state control and in a creditworthy manner. This enhances independence from actors outside the EU, reduces vulnerability and filters out abuses on the part of both service providers and citizens, facilitating the operation of digital services. The regulation of digital means of payment is closely related to this, and drafting a separate regulation for this is currently in progress.

Assisting innovation within the EU with large databases enabling substantial and unprecedented development is part of digital sovereignty. Both the competitiveness of undertakings in the EU and the appropriate protection of fundamental rights depend on the proper regulation of access to these. The Data Governance Act[25] concerning state-owned databases was adopted and the Data Act concerning private and state access to private data is currently under discussion. An antecedent to this in Hungary is Act XCI of 2021 on the National Data Assets, which is currently in force and which introduced very similar rules to those of the Data Governance Act also with a view to giving a boost to innovation at Member State level. This is closely related to AI development as that requires the largest volume of data. Data must be provided in a way that does not violate fundamental rights, so in most cases anonymous data provision is the only option.. Exceptions to this may be granted only in limited cases, for instance when the processing of disease-related data is necessary for health-related development, where pseudonymisation is the only possibility. The purpose of the analysis cannot be attained by modifying health-related data, however, the symptoms of the disease and treatment data subsequently provide a good chance of identifying the patient, so genuine anonymisation is not possible.

Protection against malevolent third parties is indispensable for digital sovereignty. In this context, the Cybersecurity Act[26] is of importance, as well as the envisaged regulations of European cloud services.

Several related EU regulations are expected to be enacted in the future, for instance in the context of developing the digital knowledge of EU citizens. Without users being aware of their rights and the risks, and without continuous digital knowledge development, the digital eco-system will not be able to function properly. Continuous innovation means that learning about what's new, both inside and outside the EU, will be important to navigate safely in a changing digital world. In the absence of this, EU citizens as well as EU Member States will not have genuine control over what is taking place in the digital space, without which the implementation of digital sovereignty cannot be envisaged.

When developing opinions on the draft legal regulations discussed here, the Authority has taken an active part in the development of the Hungarian positions represented by specialised diplomats with regard to issues concerning data protection and the freedom of information. The large number of EU legislative acts reveals that, once they are gradually adopted, they will give rise to organisational and functional transformation both at the EU and the Hungarian scene, for which both the public and the private sector should be able to prepare in time. The effective preparation of Member States is supported by the European Data Protection Board through the opinions expounded in its positions and upon Hungarian initiative through the coordination of one of its expert subgroups.

25 Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724

26 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cyber Security) and on information and communications technologies cyber security certification and repealing Regulation (EU) 526/2013 (Cybersecurity Act)

III. Freedom of information

III.1. Introduction

In addition to dealing with inquiry and consultation cases related to the freedom of information, NAIH Department for Freedom of information also investigates so-called border area cases, i.e. those concerning data protection, freedom of information and other rights to information and communication whether under inquiry procedures or authority procedures for data protection (in 2022, there were 71 cases of the latter type of procedure), response to requests for data of public interest received by the Authority, and keeps the registry of reports on rejected requests for data. The Regulatory and Data Classification Supervisory Department carries out authority procedures for the supervision of data classification. The KÖFÖP (Public Service Development Operative Programme) freedom of information research project was closed on 31 December 2022.

III.2. Substantial changes in legal regulations affecting freedom of information from 2022

In each case, the origin of the amendments effected in October 2022 was the European Commission; they were formulated as claims in the so-called conditionality mechanism linked to the supervision of the use of EU budgetary funds.

First, major changes were made to the rules of fees for meeting requests for data of public interest with a view to easing access to data of public interest; the amendments to the Privacy Act and the Cost Decree entered into force on 13 October 2022[27]. The possibility of requesting fees because of the disproportionate use of labour resources regulated in Section 29 of the Privacy Act was deleted and with regard to the remaining cost elements (the cost of the data storage medium/making copies and the costs of delivery), the implementing decree established limits. Hereinafter, the costs of labour resources shall be borne in full by the organs performing public duties processing the data (data owners). In the case of costs not exceeding the minimum amount (HUF 10,000) set forth in Section 6 of the Cost Decree, no fee can be applied to cover the costs, while in the case of costs above this, the maximum amount that may be charged is HUF 190,000. There is no change in that only actually incurred - i.e. verifiable - costs may be covered by the fee and it should be underlined that charging a fee will not be mandatory in the future, it may only be done if the organ performing public duties processing the data decides responsibly to apply the rules concerning the establishment of the fee to cover the costs. In such a case, the request for data shall be fulfilled within 15 days from the payment of the fee by the requesting party.

On 8 November 2022, Parliament decided on another Privacy Act amendment which – incorporated in the law as *lex specialis* – determines the rules of litigation that may be launched in relation to a request to access data of public interest different from those of civil procedure (basically, similarly to press litigation, the amendment speeds up the process of the procedure and generally requires expedited hearing).

As a result of the amendment adopted on 22 November 2022, a Central Information Public Data Registry was set up, which enables access to the most important financial management data of budgetary organs in an integrated central database, in particular, the data of budgetary support amounting to at least five million forints granted by them from domestic or European Union funds, public procurements, contracts and payments which are updated every two months and will be accessible for 10 years. The Registry enables the classification and comparison of the data. Obligees are to disclose the data generated on or after 29 November 2022 for the first time by 28 February 2023 at the latest. The mode and accurate content of the disclosure are set forth in Section 37/C of the Privacy Act and Government Decree 499/2022 (XII. 8) on the detailed rules of the Central Information Public Data Registry. The reports are to be filed using a downloadable datasheet in accordance with the Guidance in the User Rules[28]. As the operator of the new registry, the Nemzeti Adatvagyon Ügynökség Kft. publishes the data on the workday following the receipt of the datasheet. If a budgetary organ fails to meet its obligation to disclose the data on this platform, or discloses inaccurate or deficient data based on request the Authority launches *an authority procedure for transparency or may launch an authority procedure for transparency ex officio*. The period open for conducting a new authority procedure is 45 days. In the event of an infringement, the Authority orders expedited

27 Act XXVIII of 2022 on amending certain acts related to the control of the use of European Union budgetary funds and Government Decree 382/2022 (X. 10) on the amendment of Government Decree 301/2016. (IX. 30.) on the extent of fees that may be set for fulfilling request for data of public interest (Cost Decree)

28 https://kif.gov.hu/#/regulation

meeting of the disclosure obligation, which shall not be later than within 15 days. If the budgetary organ still fails to comply within 15 days, the Authority may impose a fine whose amount may extend from a hundred thousand forints to fifty million forints. Requests for launching a transparency procedure may be submitted to the Authority from 28 February 2023.

Finally, it should be noted in relation to the period open for providing data in 45+45 days applicable in emergency situations in force for a, extended period of time that although the effect of Government Decree 521/2020. (XI. 25.) was extended in the context of the emergency of the war in Ukraine until 31 December 2022, thereafter a response period of 15+15 days specified in the Privacy Act was re-established, i.e. organs performing public duties have to respond according to the original procedure in 2023.

III.3. Important decisions of the Constitutional Court in 2022

Constitutional Court Decision 3438/2022. (X. 28.) AB concerning the rejection of the constitutional complaint against Curia Order Bfv.II.750/2021/6

According to the position of the mayor submitting the petition, the court decisions condemning him for defamation because of the disclosure of data of public interest related to the financial management of the municipality (in the context of a query by the National Tax and Customs Administration, he stated that the deputy mayor concluded a contract on behalf of the municipality without being authorized to do so), infringe his constitutional right to disclose data of public interest and his fundamental rights to the freedom of expression and fair court procedure. According to the facts of the case established by the courts, the petitioner made a statement of fact in the case under investigation, but he was unable to prove its truthfulness. Establishment of the truthfulness of a statement is the responsibility of courts with general jurisdiction and the Constitutional Court may not review its result. Even public figures may successfully invoke the protection of their personality rights against false statements or those made in front of the public that are not demonstrated to be truthful. In the course of their proportionality test, the courts took into account that the petitioner went substantially beyond responding to the request, accused the injured party of having committed a crime and the disclosure was objectively suitable for defaming the injured party.

Constitutional Court Decision 3258/2022. (VI. 3.) AB concerning the rejection of a constitutional complaint

The petitioner requested that the respondent business organisation be obligated to disclose data of public interest with regard to altogether ten investment projects financed from European Union funds or public money as the winner of public procurement tenders concerned in the data request or as a member of the winning consortia. He requested the disclosure of the exact types and total quantities of all the building materials and all the material assets used, their sources of procurement and prices, as well as documents verifying payment , procured and/or incorporated by the respondent. In its judgment 26.P.20.281/2020/9, the court of first instance rejected the petition in a repeated procedure because having jointly interpreted Article 39(2) and (3) of the Fundamental Law and Section 3(5)-(6) and Section 27(3) and (3a) of the Privacy Act, it concluded that the respondent was not managing public moneys, hence it was not subject to the obligation to publicly disclose its financial management. The court underlined that the amounts the respondent obtained through public procurement tenders financed by European Union funds could not be regarded as revenues, expenditures or claims of the state, hence they do not qualify as public moneys. The court of second instance taking action based on the petitioner's appeal altered the judgment of the court of first instance with its judgment Pf.III.20.050/2021/3 and ordered the respondent to issue the requested data; however, the Curia's judgment Pfv.IV.20.904/2021/5 annulled this and approved the judgment of the court of first instance. Instead of deciding on the acceptance of the complaint, the Constitutional Court adopted a draft decision containing the adjudgment of the complaint in merit and rejected the petition. According to the decision, the notion of public fund in the Fundamental Law overrides every other interpretation in earlier decisions of the Constitutional Court, and according to Article 39(3) of the Fundamental Law, it is not the source of the assets provided, i.e. its origin, that is the decisive factor in the notion of "public funds"; in addition, there is no rule, which would declare certain data in the contracts of business organizations concluded with one another as data of public interest or data accessible on public interest grounds.

Constitutional Court Decision 3177/2022. (IV. 22.) AB concerning the annulment of court decisions (judgment 8.Pf.20.188/2021/9 of the Fővárosi Ítélőtábla [Budapest Court of Appeal] and judgment 62.P.20.901/2020/11 of the Fővárosi Törvényszék [Budapest Municipal Court])

The petitioner NGO requested the Ministry of Human Resources in 2019 to send the findings of the investigation carried out by or on behalf of the ministry on the SROP - Bridge to the World of Work project. The Criminal General Directorate of the National Tax and Customs Administration is conducting an investigation against an unknown perpetrator in relation to the projects concerned in the litigation because of the well-grounded suspicion of having committed budgetary fraud. According to the court, the controller lawfully refused the fulfilment of the data request with reference to Section 27(2)(c) of the Privacy Act and Section 109(1)(e) of Act XC of 2017 on Criminal Procedures (hereinafter: Criminal Procedures Act). As pointed out by Constitutional Court Decision 4/2021. (I. 22.) AB, the framework for restricting freedom of information is set forth by the Privacy Act – also in view of Article I(3) of the Fundamental Law – which recognises three categories: a) classified data; b) data in support of a decision-making process [Privacy Act Section 27(5)]; and c) restriction by a separate act [Privacy Act Section 27(2)]. The Constitutional Court underlined that Hungarian constitutional dogmatics are driven by data and the application of the law, the restriction of data does not set in *ex lege* in any case, in actual fact "the decision to restrict freedom of information is carried out by the controller even with the most extreme reasons". This means that freedom of information is never automatically restricted by force of law, it always requires a decision by the controller. "This clause may be regarded as the essence and the primary safeguard of the freedom of information, which extends to all three types of restriction (classified data, data supporting decision-making and restriction by separate act). It is therefore constitutionally impossible to directly block data by law." {Constitutional Court Decision 4/2021. (I. 22.) AB, Justification [46]–[48]} [26].

In the case at hand, the court established that of the types of restriction of the freedom of information presented in Decision 4/2021. (I. 22.) AB, the third one applies. In such cases, the court weighs the matter in two phases: a) first, the court has to identify the legal regulations applicable to the case that restrict the right to access data of public interest and data accessible on public interest grounds, which enables the blockage of the data from the public (legal grounds), and b) on that basis it has to weigh the lawfulness of the controller's decision and the reasons for the restriction (necessity and proportionality). The challenged decision of the court formally meets this requirement, but in terms of content, it is not in line with constitutional requirements, if the court makes its decision concerning the restriction of the freedom of information without specifically examining the actual content of the documents requested. In its earlier decisions, the Constitutional Court acknowledged the prosecution and prevention of crimes as constitutional values which may in the given case warrant the restriction of fundamental rights {Constitutional Court Decision 3255/2012. (IX. 28.) AB, Justification [14]; Constitutional Court Decision 3269/2012. (X. 4.) AB, Justification [20]; Constitutional Court Decision 3038/2014. (III.13.) AB, Justification [32]}. [36] The justification of the challenged judgment, however, shows that the court referred only to the statement of the National Tax and Customs Administration in this regard and based its decision exclusively on it. It could not be established that the court itself examined the content of the requested documents and established as a result that they were subject to the restriction of access. Assuming that the refusal to issue the data rests on the appropriate legal basis, the statement of the investigative organ on the existence of interest in the prosecution of crime may be an important – even decisive – factor in demonstrating proof. However, knowledge of the content of the requested document and its actual examination by the court – similarly to the case of data supporting decision-making – cannot be dispensed with. Without this, the substantive review of the justification and reasonableness of the grounds for refusal put forward by the controller for restricting freedom of information – and so, the exclusion of an arbitrary decision by the controller – is not possible for the court as part of the protection of the freedom of information as a fundamental right, because it allows for its not strictly necessary – i.e. formal – restriction. In the absence of the consistent enforcement of the data principle, there is a risk that a general reference to the interest of criminal procedures would enable the denial of access to data that are otherwise undisputedly of public interest for an unlimited period of time.

Constitutional Court Decision 3179/2022. (IV. 22.) AB concerning the rejection of a constitutional complaint (related: Constitutional Court Decision 3401/2022. (X. 12.) AB)

The petitioner NGO made a request for data of public interest to a ministry in which it requested copies of reports on the Öveges-program project and the Bridge to the World of Work project investigated by the European Anti-fraud Office (OLAF) submitted to the Government and all other information or data concerning OLAF's and the Government's common position on these projects. The controller refused to issue the data stating that according to the Court of Justice of the European Union OLAF's investigative documents are entitled to a general protection, on the basis of which it was exempted from public access to the documents and only substantial public interests may allow for an exception. The court of first instance rejected the petition and established that an omission on the part of the respondent ministry with regard to the consultation to be conducted with the director general of OLAF may not automatically result in an obligation to issue the data. The reason for this is that in the absence of consul-

tation, the director general of OLAF is entitled to make a decision on the issue of the data. The court of second instance taking action as a result of the petitioner's appeal upheld the judgment of the court of first instance. In its judgment, it established that in relation to the investigative reports, the ministry only carries out coordinating activities, which is not the same as any of OLAF's activities, thus the requested data were generated not by the ministry and not in relation to the performance of its public duties, hence the ministry is not under an obligation to make them accessible. In its judgment, the Curia upheld the force of the final judgment and established that *"the respondent [...] had a legal position concerning the rejection of the issue of the data worthy of examination"*, which the Curia also regarded as being well-founded, when by reference to the indicated European Union regulations through their interpretation, it arrived at the conclusion that *"the director general of OLAF is entitled to make the decision on the issue of the data"* (Curia judgment Pfv.IV.20.948/2020/6, Justification [20]–[21]). According to the opinion of the Constitutional Court, the question whether the court correctly interpreted the EU legal requirements applied and whether, on that basis, it justifiably identified OLAF in the present case as the organ entitled to make the decision is an issue of the interpretation of specialised EU law, whose review would be outside the Constitutional Court's duty to protect fundamental rights, even if it would otherwise disagree with the legal interpretation of the court.

III.4. Important court judgments in 2022:

Pfv.IV.21.217/2021/5.: The petitioner Member of Parliament requested data of public interest concerning the transfer of an indirect holding in a power plant plc. from the respondent business organisation in public ownership ensuring the energy supply of the country. The court of second instance annulling the judgment of first instance correctly established that Section 7/I(1) of Act CXII of 2009 on the More Economical Operation of Business Organisations in Public Ownership contains requirements concerning non-accessibility without the need for carrying out any other investigation, hence the data of public interest specified in Annex 1 to the Act are not accessible for the period specified in its annex. It established that in the case under litigation, the blockage of the data from access was substantiated by the decision of the Ministry of Defence qualifying the power plant as a national critical system element, and the official statement of the Office for the Protection of the Constitution concerning the fact that national security interest obtained. In view of this, it was mandatory by force of the law for the respondent to refuse to issue the data without any additional consideration, hence the Curia found the petition for the review the final judgment submitted by the petitioner ungrounded.

Pfv.21.493/2021/5.: The petitioner asked for the documents of the impact assessment for Act C of 2020 on the Medical Service Legal Relationship in his request for data of public interest; however, the respondent refused to issue the data with reference to their nature of supporting decision-making. The court of first instance established that when refusing the request, the respondent failed to accurately indicate their future decision, as well as to weigh the public interests according to Privacy Act Section 30(5). The respondent in its counter-petition in the litigation indicated the three implementation decrees to the act, which had already been promulgated as "future decisions". The court of first instance had to take a position on whether the lawfulness of the issue of data of public interest supporting decision-making can be examined exclusively on the basis of the circumstances existing at the time of refusal under Section 27(6) of the Privacy Act, or if the decision indicated as the basis for refusal was made in the course of the procedure, whether the data could be issued without the submission of a new request for data. In its decision upheld by the court of second instance, the court of first instance ordered the respondent to issue the data. Under the decision, if the reason for refusal no longer obtains in the litigation and it is not disputed, the controller may be ordered to issue the requested data of public interest. The Curia upheld the final judgment.

Pf. 20.043/2022/8.: The petitioner submitted a request for data of public interest to the Ministry in charge of healthcare with regard to the study supporting the decisions concerning the transformation of healthcare made by the limited company and the technical description in the contract on the production of the study. The court of second instance arrived at the conclusion by examining the enclosed study and the documents submitted that the study also supports additional decisions as, according to the documents, the transformation of healthcare consists of three phases, of which the second has not yet been completed, and the third has not even started. The Constitutional Court in its decision 6/2016. (III.11.) AB pointed out that the entire document – in view of the fact that the data principle is enforced and not the document principle – cannot be blocked from access with reference to its decision supporting nature; in this case, however, the court established following the specific examination of the study that in view of the interrelations of the tasks, the entire document supported decision-making.

Pf.20.158/2022/5.: In contrast to the previous decision, in the case of a request for data of public interest concerning policy programmes approved by Government Decision 1722/2018. (XII.18.) – as the "*Healthy Hungary 2021-2027 Healthcare Sectoral Strategy*" was adopted based on the policy programmes and the respondent failed to prove that the programmes also laid the foundations for additional decisions other than the adopted strategy – the court ordered the respondent to issue the data in view of the fact that the decision was made and no evidence was provided that it laid the foundations for future decisions.

Pf.20.239/2022/6.: The petitioner requested that the respondent is ordered to issue the vaccination plan requested in his request for data of public interest. According to the respondent's defence, it was aware of the vaccination plan, but it was not its controller and as the petitioner himself disclosed on the Internet that he obtained the vaccination plan, the enforcement of his request does not comply with the social purpose of the Privacy Act. The court of first instance established that the respondent was not a controller with regard to the vaccination plan as the Operational Staff qualified as controller, thus the petitioner requested the issue of the vaccination plan from the inappropriate respondent. In addition, the petitioner was able to have access to the vaccination plan in another litigation in progress during the procedure of first instance, which was not disputed. The court of second instance established that the petitioner was able to have access to the vaccination plan from another controller and also because the respondent provided the link through which it could be accessed in the procedure of first instance. In view of this, the petitioner's request enforced in the litigation does not serve the transparency of public affairs and it is not reconcilable with the social purpose of a fundamental right. Even if the capacity of the respondent and controller obtained, the respondent could not be ordered to issue the vaccination plan because it had already given the public source containing the data to the petitioner. In view of the provisions of Curia Decision Pfv. IV.20419/2021/6, the petitioner's exercise of his rights was not regular, hence the court of second instance upheld the judgment of first instance.

Pf.20.117/2022/6.: The petitioner requested the issue of the vaccination plan against COVID-19 from the National Public Health Centre. The vaccination plan requested by the petitioner is included in the document entitled "*Schedule of tasks related to vaccination against COVID-19*" published by the Ministry of the Interior on its website. Following the launching of the litigation, the respondent referred to this and provided the electronic link to the document. The court pointed out that by reference to a public source, an organ performing public duties may fulfil a request for data, even if it was not that organ that had earlier made

the information accessible to the public. It is not contrary to the purpose of the Privacy Act, if the controller voluntarily meets its obligation to provide data in the course of litigation; voluntary performance is in place also in the case of litigation, but when fulfilling a request for the issue of data in the course of litigation, the enforcement of the request cannot be regarded as unnecessary, hence the respondent was ordered to reimburse the petitioner's litigation costs.

Pf.20.213/2022/8.: In his request for data of public interest, the petitioner requested data of public interest from the respondent related to the tender grants provided by the respondent to two limited companies. Within 15 days, the respondent informed the petitioner that based on Section 1(3) of Government Decree 521/2020. (XI. 25.), it will fulfil the request only within 45 days following the receipt of the request, but the petitioner did not wait for the expiry of this period, and submitted his petition. The court of first instance ordered the respondent to issue the data in accordance with the petitioner's petition and established that the petition was not premature because the respondent referred to its emergency tasks only in general and not in accordance with the requirements of Constitutional Court Decision 15/2021. (V.13.) AB and failed to specify the reasons, which would render it probable that fulfilling the data request would jeopardise the performance of these tasks. The court hearing the respondent's appeal found that the 45-day response period expired unsuccessfully even before the delivery of the letter of petition to the respondent and, in any case, being premature was not on the exhaustive list according to Section 176(1) of the Civil Procedures Act as a reason for rejecting the petition and subsequently for terminating the procedure. If, in the event of initiating a preventive procedure, in a litigation aimed at accessing data of public interest, the petitioner submits his petition prior to the due date for initiating a lawsuit as set forth in the legal regulation, and the due date expires even before the delivery of petition to the respondent without fulfilment of the data request, the petition shall not be rejected and the litigation shall not be terminated on account of the omission of the mandatory procedure preceding litigation. *The judgment of the court of first instance was upheld by the court of second instance.*

Pf.20.066/2022/5.: The petitioner requested data concerning an EU tender for agriculture, forestry and food processing. According to the respondent, some of the requested data are not public because according to Section 24(1) of Act XVII of 2007 on Certain Issues of the Procedure Related to Agri and Rural Development and Fishing Grants and Certain Measures (Agri Aid Act), the data generated or recorded in the procedure of the controller are not accessible as a main rule except for the data according to paragraph (2), for which the Agri Aid

Act requires a quarterly disclosure obligation in any case (www.palyazat.gov.hu and www.magyarallamkincstar.gov.hu). The court of first instance ordered the respondent to issue all the requested data because the provisions under Section 24(1) and (2) of the Agri Aid Act are not consistent with any of the reasons for refusal under Section 27(2) of the Privacy Act, hence the provisions of the sectoral legal regulation are irrelevant from the viewpoint of the fulfilment of the data request. The respondent appealed and presented that the two directly applicable EU regulations provide as follows: according to Article 111 of Regulation (EU)1306/2013 only the data specified therein need to be disclosed on the beneficiaries of a grant, while according to Recital (32) of Regulation (EU)908/2014 publication should not go beyond what is necessary in order to reach the transparency objectives pursued. According to the respondent's appeal, the part of the data request on "*who evaluated*" the tenders and "*who carries out control*" cannot be the subject matter of request for data of public interest as these are the personal data of civil servants. The Court of Appeal referred to the fact that in its Decision Pfv. IV.21.093/2020/5 the Curia clarified: Section 24(1) and (2) of the Agri Aid Act may not restrict the range of accessible data of public interest and data accessible on of public interest grounds. Hence, the Court of Appeal had to examine whether it would have been right to differ from the decision of the Curia in a legal issue based on the appeal. In relation to the EU regulations referred to, the Court of Appeal pointed out that they regulate the obligation to publish and do not contain any prohibition as to providing access to additional information related to tenders upon special request in addition to the data which are mandatorily published. The names, responsibilities and duties of the persons evaluating and controlling tenders are data accessible on of public interest grounds of civil servants according to Section 26(2) of the Privacy Act. In view of all this, the Court of Appeal upheld the decision of the court of first instance.

Pf.20.023/2022/10.: The court of first instance ordered the respondent to issue the calculations made in accordance with the requirements of Section 133(2) of Act CXLIII of 2015 on Public Procurement in a context of the announcement of the concession tender for motorway operating services and the related data substantiating compliance with the relevant legal requirements (all other data substantiating the 35-year period of the contract according to the invitation to tender) to the petitioner. The court pointed out that it does not follow from the fact that the Public Procurement Act does not require the accessibility of the data that they could not be accessible as data of public interest. Concerning the nature of the data supporting decision-making both paragraphs (5) and (6) of Section 27 of the Privacy Act are applicable in the legal dispute, because the announcement was published based on the calculation preceding the announcement, i.e.

a decision has already been made, but the calculation and the related data substantiating compliance with the relevant legal requirements also support future decisions as the concession tendering procedure continues even after sending the invitation to tender, and the preliminary calculation is finalised when the contract is concluded. When applying Section 27(5) of the Privacy Act, the controller should have carried out the public interest balancing test according to Section 30(5) of the Privacy Act. In this context, for the court's discretion it is necessary for the controller to enclose the data concerned by the data request as a sealed document in the lawsuit, with regard to which it is warranted to restrict access according to its own consideration; if respondent fails to do so, it is also unable to comply with its interest in providing evidence. Because of this, the court upheld the decision of first instance.

Pf.20.363/2022/7.: The petitioner submitted a request for data of public interest to the respondent with regard to copies of additional contracts, orders, performance certificates and invoices based on the two framework contracts for the fireworks and festivities of 20 August 2021. According to the decision of the court, the data request does not qualify as comprehensive, invoice level data request as it applied only to two framework contracts.

Pfv.20.040/2022/5.: The petitioner's data request was primarily aimed at having access to the loan contract between the Government of Hungary and the Export-Import Bank of China and secondarily, in the event of a dismissal of the data request, to the specific information the minister has considered and the foreign policy and foreign economic interests that would be jeopardised by the disclosure of the loan contract. The court pointed out that under Section 27(2)(f) of the Privacy Act, an act may restrict access to data of public interest in view of external relations. Section 2(3) of Act XXIX of 2020 promulgating the Convention on the investment for the reconstruction of the Budapest-Belgrade railway (hereinafter: BB Railway Act) specifies that the issue of data shall be refused for 10 years from the generation of the data, if access to the data would jeopardise Hungary's foreign policy and foreign economic interests free from undue external influence, and according to Section 2(4), the minister in charge of foreign economic affairs shall decide on whether or not a request to access the data can be fulfilled and on the disclosure of the data, having weighed Hungary's foreign policy and foreign economic interests and also obtaining the position of the Government of the People's Republic of China. In view of Article 3(8) of Act XXIV of 2016 promulgating the Convention, the minister is bound by the statement of the Chinese party: "[...] *Information provided by the parties to one another of this Convention or generated as a result of the Convention implementation shall not*

be disclosed and shall not be transferred to any third party without the prior written consent of the two parties." According to the court's decision, the minister has no obligation to justify his considerations as the BB Railway Act does not specify the criteria of consideration as it is within the discretionary powers of the minister; the court may not review the minister's consideration as that has no legal basis. The court annulled the final judgment ordering the respondent to fulfil the request for data of public interest and upheld the judgment of first instance rejecting the petitioner's petition.

Pfv.20.258/2022/11.: The petitioner requested data of public interest from the respondent prize-awarding body; however, according to the respondent's position it was not an independent subject of law: it does not manage funds, it has no independent account, it does not spend public funds, it does not perform public tasks, it merely awards the prize and organises the award ceremony, i.e. it is but a group of persons consisting of the managers of the founders, it is not an NGO or any other organisation, it is merely a framework for cooperation among the organs enacting the deed of foundation and its legal relationship according to civil law. The court of first instance terminated the litigation by order in view of the fact that prior to the litigation, the petitioner submitted his request for data of public interest to a non-existent entity in the absence of an operating organisation, the respondent does not process data of public interest, the data and documents are processed by the founders and the secretary of the body. The Curia adjudged the petitioner's request for review as unfounded. In a litigation for the issue of the data of public interest when assessing whether the subject indicated as respondent has legal capacity in the litigation based on Section 31(4) of the Privacy Act, it is necessary to take into account the actual activities of the subject indicated, whether it is capable of processing data of public interest, or data accessible on public interest grounds, whether it had the organisation needed for this. In the absence of such capability and organisation, the petition for the issue of data of public interest shall be rejected and in the absence of this, the procedure shall be terminated.

2.Pf.20.567/2022/3.: The defence put forward by the respondent in the litigation was that it was not a controller based on Section 3(9) of the Privacy Act. The court pointed out that based on Sections [31]-[33] of Constitutional Court Decision 6/2016 (III. 11.) AB what needs to be examined in litigations of this kind is not whether the respondent is defined for the processing of personal data by the legislator, whether it is a controller according to the definition specifying the purpose of processing the data, but whether the condition set forth in Section 26(1) of the Privacy Act is met with regard to it, i.e. whether the data desired to be accessed are actually processed by it.

Pf.20.893/2021/5.: The respondent is a business organisation fully owned by the Hungarian State, carrying out public task specified in a legal regulation concerning tourism. The respondent's data request was for the respondent to disclose by name, who decide on individual support and who are on the professional panel referred to by the respondent in an interview. The court of first instance found that what has significance is not that the professional panel does not act as a body according to the defence put forward by the respondent, but who the persons are that are involved in the evaluation of requests for support. Pursuant to Section 2(1)(c) of Act CLXXXI of 2007 on the Transparency of State Aid from Public Funds (State Aid Transparency Act), these persons qualify as decision-makers and pursuant to Section 26(2) of the Privacy Act, they are persons acting within the functions and powers of the organ performing public duties. The court of first instance ordered the respondent to issue the names of the decision-makers as data accessible on public interest grounds and the decision was upheld by the court of second instance.

Pfv.21.441/2021/5.: The respondent is a business organisation held exclusively by the state, which was designated by the Government to supply textbooks, produce textbooks for schools and carry out the tasks related to ordering textbooks. The petitioner requested access to the contract and its annexes with which the respondent purchased 97.71% of the shares in the LLC from a natural person. According to the defence put forward by the respondent, the amount that it spent on purchasing the shares in the LLC does not qualify as public funds because the procurement was financed in 2020 by receipts that it had obtained prior to 2020. With reference to the case law of the Constitutional Court, the court of first instance established that the management of funds used in the course of performing public duties does not lose its public fund nature only because it is carried out by a non-profit business organisation; the respondent performs public duties, its assets are the assets of the state, i.e. national assets. The court of first instance ordered the respondent to fulfil the data request and the judgment was upheld by the court of second instance. In the review procedure, the Curia upheld the force of the final judgment.

III.5. On the fee covering costs that may be imposed in relation to the fulfilment of data request

As explained above, the rules concerning the fee to cover costs that may be imposed in relation to the fulfilment of data requests have changed significantly in a favourable direction for the enforcement of the freedom of information from October 2022, but over the past years, this was a topic that generated a great deal of legal disputes, particularly because of the fees imposed with reference to labour resources. In 2022, NAIH reviewed altogether 35 fees for costs, of which 11 enquiries were launched in 2021: controllers were municipalities, government offices, business organisations in public ownership and foundations, and in the majority of cases the infringement could be remedied by having the data issued free of charge or with a substantially reduced fee. In 2022, the highest fee covering costs into which an inquiry was made was HUF 558,093; the petitioner requested the contracts and permit applications by an organ performing public duties for a period over two years. *(NAIH-2812/2022)*

In another case, the petitioner requested copies of the statement of assets of the mayor, deputy mayors and representatives of the municipality, in addition to copies of the invoices of cash desk payments, cash desk logs and bank account statements of the mayor's office for 2019-2021. The Authority regarded the moderate amount of the fee (HUF 81,987) imposed by the municipality as acceptable with regard to the invoices, in view of the small staff working for the municipality and the large quantity of the requested data - the documents requested made up altogether 909 pages. At the same time, the Authority called upon the municipality to fulfil the request for the statements of assets without imposing a fee to cover the costs. *(NAIH-2894/2022)*

HUF 79,200 were incurred as cost in a case where the petitioner wished to know the total number of nights spent by children and their escorts in two Erzsébet camps in the preceding year, what was the per capita cost of accommodation and the daily board and what was exactly included in the board. In the course of its inquiry, the Authority established an infringement as the petitioner was notified of the amount of the cost to be charged after the expiration of the relevant period, and it was not informed in sufficient detail of the reasons on the basis of which the labour resources needed qualified as disproportionate in the operation of the Foundation, and the Foundation in its answer failed to call attention to the possibilities of legal remedy. In view of the above, the Authority called upon the Foundation to send the requested data free of charge. *(NAIH-2718/2022, NAIH-1857/2022)*

III.6. NAIH recommendation concerning the obligation to provide information for the entity actually processing the requested data of public interest

With reference to the Tromsø Convention and specific investigative experiences, NAIH issued a general recommendation in 2022 stating that the requested entity should – simultaneously with the rejection of the data request and the information on legal remedy to which the data subject is entitled pursuant to the Privacy Act – provide additional information on the identity of the actual controller provided that it has the relevant information (particularly if the actual controller is now or has earlier been subordinated to it, or based on relevant legislation, the identity of the controller can clearly be identified by the entity). The full text of the recommendation is accessible here: https://naih.hu/informacioszabadsag-ajanlasok.

III.7. Personal data accessible on public interest grounds

Ever since the establishment of the Authority, or perhaps since the introduction of the legal institution in 2005, it has been an evergreen issue to which personal data are guaranteed access by the Privacy Act or the provisions of other laws on grounds of public interest and which are not accessible to petitioners. A common feature of data accessible on public interest grounds is that an Act of Parliament provides for their accessibility. The assessment of accessibility is, however, not always self-evident because beyond the fact that Section 26(2) of the Privacy Act – as a main rule – places other personal data related to the discharge of public duties into the accessible sphere, Annex 1 to the Privacy Act (in the General Publication Scheme) and the special publication provisions of other acts require also additional types of data to be published, which otherwise qualify as personal data. It is also important to note that the so-called legal status acts applicable to persons discharging public duties may not restrict the provisions of the Privacy Act ensuring general assess, except if this is allowed by the Privacy Act, for instance in the case of Section 26(3). The evaluation of the accessibility of personal data on public interest grounds is basically possible through a three-step process of analysis:

1.Whether the data subject (or a specific range of persons), is a person acting within the functions and powers of the organ performing public duties, i.e. does the entity "employing" the data subject perform public duties.

2. If the answer is yes, then a well-grounded decision has to be made on whether the activity, actions, work of the data subject concerned in the request for data fall within the responsibilities of the organ (discharging public duties), whether he or she participates in that in merit.

3. The third step is to assess on a case-by-case basis, whether there is a link between the type(s) of data requested (data sets) and the performance of the tasks concerned, such that the specific data to be accessed are in the public interest and therefore can be disclosed.

Otherwise, the refusal to disclose the data has to be justified, i.e. the petitioner has to be informed why the data is not accessible on public interest grounds, or why it is not related to the discharge of public duties by a person performing public duties, or why the data clearly belong to the protected private sphere of the data subject. In addition, the established case law of the courts and NAIH has also to be taken into account. The provisions concerning access to data of public interest have to be applied to accessing data accessible on public interest grounds; in the absence of a provision for publication, these data can be accessed through data requests.

In addition, it is an important requirement to which the attention of controllers must be called in every case that personal data accessible on public interest grounds may be promulgated respecting the principle of purpose limitation. The provisions of Annex 1 of the Privacy Act and separate acts concerning the legal status of persons discharging public duties govern the publication of personal data accessible on public interest grounds on websites. According to the justification of the amendment of 2013: "*Although the rules on accessing data of public interest are to be applied to access such data, the nature of these data as personal data remains in spite of their accessibility, as the most important safeguard of data protection, the data requirement of the principle of purpose limitation must still be upheld and enforced in full in the course of the subsequent use of the personal data already published. At the same time, purpose limitation cannot be an impediment to the freedom of the press. The act intended to constrain the use of publication obviously contrary to the original intent of the legislator, such as the publication of databases containing personal data within the framework of the law."*

To the extent that the processing and accessibility of data accessible on public interest grounds is needed for the transparency of public affairs and for the democratic discussion of public matters, processing (necessary and sufficient) in line with this also qualify as lawful under the GDPR [Recital (153), Article 17(3)(a),

Article 85 and Article 86] provided that it is done with the appropriate legal basis and purpose. Establishing to what extent the data processed relate to the performance of public duties or to what extent they are part of privacy to be protected requires separate consideration in each case. In the justification of its Decision 443/D/2006. AB, the Constitutional Court expounded that "*it is not in itself sufficient for a restriction of a fundamental right to be the constitutional (...)that it is done to protect another fundamental right or freedom, or with a view to some other constitutional purpose, it is also necessary that it complies with the requirements of proportionality: the importance of the purpose to be achieved and the seriousness of the infringement of the fundamental right caused for that purpose must be in proportion to one another.*"

A citizen complained that a county self-government, disclosing contracts for grant over the Internet, published his personal data when it published the contracts for development projects implemented with European Union funding in accordance with Privacy Act, Annex 1, General Publication Scheme, III. Financial Management Data, point 7,. As the head of a non-profit business organisation fully held by the state performing public duties, the complainant performed public tasks at the time of signing the contract, hence his name, position, signature and initials qualify as personal data accessible on public interest grounds. The publication of the contract on the Internet containing personal data accessible on public interest grounds took place in accordance with the requirements of the Privacy Act, consequently rendering these data unrecognisable cannot be requested lawfully. *(NAIH-3115/2022)*

Another private individual contacted NAIH asking whether he may request data concerning the secondary school certificate of the settlement's mayor of his former school. Legal regulations do not prescribe any specific school qualification as a condition of filling the post of mayor, hence the secondary school certificate of the mayor does not qualify as data accessible on public interest grounds, hence according to the rules of the Privacy Act, a controller must reject such request for data. In the case when a mayor voluntarily published the data related to his school qualifications, or it was done based on his recorded consent, is separate from the above case; according to the Authority's position these data are accessible in such a case. *(NAIH-3340/2022)*

The Hungarian Medical Chamber (MOK) requested the Authority's position on MOK's recommendation for the transparency of medical ethics procedures, the constraints of implementation in the current legal environment and the law

amendments needed for implementation[29]. GDPR Article 86 provides that: *"Personal data in official documents held by a public authority or a public body or a private body for the performance of a task carried out in the public interest may be disclosed by the authority or body in accordance with Union or Member State law to which the public authority or body is subject in order to reconcile public access to official documents with the right to the protection of personal data pursuant to this Regulation."*

In its earlier statement,[30] the Authority expounded that it follows from the joint interpretation of Section 26(2) of the Privacy Act and Section 112 of Act CLIV of 1997 on Healthcare (Healthcare Act) that if an ethics procedure initiated in the context of a physician performing his public duties (for instance, fraud in the context of medical activity) was closed, then the right to informational self-determination of the person performing public duties may be restricted. With a view to the fulfilment of a request for data of public interest, it is necessary to distinguish whether the ethics procedure conducted by MOK concerns and if so, to what extent, the performance of public duties by the physician. When a decision bought as a result of the ethics procedure is made accessible to fulfil a data request, the disclosure has to be restricted to the content relevant to the performance of public duties by the physician. According to the regulations in force, the fact of a final penalty imposed under an ethics procedure, the date when the decision imposing the penalty becomes final and an indication of the date of its statutory limitation as other personal data related to the performance of the public duties of physicians qualify as data accessible on public interest grounds. The legal situation would be clearer, if the Act (such as an amendment to Section 112 of the Healthcare Act) were to determine which data of the ethics procedure can be accessible through data request. For the time being, the publication of these data on websites is not required by any legal regulation, i.e. they do not qualify as personal data accessible on public interest grounds. *(NAIH-1715/2022)*

Also in the field of health care, a pharmacist complained about the obligation imposed by the authorities on pharmacy employees to wear a badge with their full name and position. In its decision, the Authority concluded that the data in question are the data accessible on public interest grounds under both the sectoral law and the Privacy Act, thus wearing a name badge in the pharmacy as processing is lawful, it does not infringe the data subject's right to informational self-determination, but it is a restriction proportionate to the purpose of data processing. In a remedial procedure, the court also upheld NAIH's decision. *(NAIH 962/2022*).

A legal adviser asked for information on the interpretation of the aggregated data on personal allowances paid to persons employed by public bodies (Privacy Act, Part III (Management Data), Annex 1, disclosure unit in point 2).

According to judicial practice, if by virtue of the nature of the work, the activity can be carried out not only on the basis of an employment relationship but also under some other legal relationship aimed at the performance of work, in view of the principle of the freedom to contract, the parties can freely decide on the type of contract (civil law contract or employment contract) for the work to be carried out. Because of this, the range of persons employed and the full publication of the data related to the use of public funds in relation to them should be interpreted broadly with a view to proactive freedom of information. In view of the above, all the circumstances of the case should be considered to establish whether the public funds paid in lieu of the legal relationship and the performance of tasks by a given person were used for the purposes of his/her employment. Under the law, in the case of employees, the number of persons (headcount) receiving payment from the given organ has to be disclosed quarterly (every three months) together with the total amount in forint terms. In the case of managers, it is also quarterly (every three months) that the number of persons in managerial positions or senior officials is to be stated at the given organ, and what is the amount paid to them in total (as wages or dues). Furthermore, if they received regular benefits, then what the total amount paid by the organ for these benefits was, and over and above these, what cost reimbursement they received and what the total amount paid for this during the given period was. Point 3 of the publication unit covers every employee not in a managerial position. It is also quarterly that their benefits received from the given organ (personal and other benefits) and their total amount during that period is to be stated. The text of the statement is available in full in the website[31] *(NAIH-933/2022)*

The request for data concerning the disclosure of wage data of employees making use of the work time allowance due on trade union work at a public transportation company was lawfully rejected. Employees carrying out trade union work at the company are not in the category of persons performing public duties, in view of the fact that these activities are not included in the functions and pow-

29 https://naih.hu/dontesek-infoszab-allasfoglalasok?download=504:allasfoglalas-az-orvosetikai-eljarasok-transzparenciajara-vonatkozo-javaslatrol

30 Statements NAIH/2017/1936/5/V and NAIH/2017/1936/10/V

31 https://naih.hu/dontesek-infoszab-allasfoglalasok?download=494:allasfoglalas-konzultacio-a-kozfeladatot-ellato-szerv-altal-foglalkoztatottakra-vonatkozo-adatok-kore-es-kozzetetel-targyaban-infotv-1-melleklet-iii-resz-gazdalkodasi-adatok-2-pont

ers of the company providing public services. In addition to this, there is no legal provision currently in force that would ensure the accessibility (accessibility or publication) of the personal data of persons carrying out trade union activities. Although Section 2(1) of Act CXXII of 2009 on the Economical Operation of Business Organisations in Public Ownership (Public Company Operations Act) classifies the data listed therein as accessible on public interest grounds and also provides for their publication, this, however, does not automatically render other personal data processed by organisations or companies discharging public duties accessible on public interest grounds. The requested data may be made accessible in a cumulative form or in a manner unsuitable for the identification of persons. *(NAIH-3353/2022)*

III.8. "Post-Covid"

The Authority continued to receive notifications related to epidemic (vaccination) data in 2022; also, several inquiries launched in 2021 were concluded in this year. Below, we provide information on these.

III.8.1. Consultation with the National Public Health Centre (NNK)

In October 2022, the leaders of NNK presented the systems, processes and related problems in connection with the registration of infection data in the course of a personal consultation.

Section 15 of Act XLVII of 1997 on the Processing and Protection of Healthcare Data and Related Personal Data and the provisions of Decree 1/2014 (I. 16) EMMI on the order of reporting infectious diseases provide a clear legal framework for the collection of epidemiological data on infectious patients. However, any conclusion to be drawn from the raw set of data or answering any professional questions arising and/or data requests is only possible after the appropriate validation and analysis of the data, which includes the correction of accidental errors and the comparison of individual data fields with the help of computer programs in order to identify conflicting information. Calling upon a healthcare provider to correct or supplement data after their recording is not warranted either medically or epidemiologically because their primary task is to provide patient care. The infectious patient reporting subsystem of the National Professional Information System for Epidemiology (hereinafter: OSZIR) was developed for

a low number of cases. The more than sevenfold increase in the volume of data entering the epidemiological system could not be handled by the methods used previously. There was no time to prepare the system in 2020 for the mass processing of the data of the Covid-19 epidemic, thus IT problems arose from September 2020. The fact that the same staff member had to carry out validation as well as contact research and issue obligations constituted additional difficulties. The use of OSZIR requires special knowledge and the recruitment and training of additional staff members was not successful during such a short period of time. The path of infection data is complicated. The infectious patient notifier (family) doctor or the staff member authorised to notify infectious patients from hospitals may report to the infectious patient reporting subsystem of OSZIR. The district epidemiologists competent according to the place of contracting the disease create disease cases from the reports (a form containing the data of the given disease). Patients are identified using a unique identification code generated on the basis of the name and the TAJ (Social Security) number. If laboratory testing substantiates Covid-19 infection, the epidemiologists of the district public health office classify the suspicious case as verified after receipt of the laboratory finding and collate the clinical data with the microbiological data. NNK staff check the reports and the entries concerning epidemics. If they raise a question or note an error or deficiency, it is then indicated to the notifier who is able to correct the error or supplement the missing data on the message board. Logical validation (for instance, if a case of the same patient was notified in several places) and annual validation (for instance, if a case was incorrectly closed, or the removal of a patient warranted because of recovery was omitted) are carried out on the data. Annual closure takes place on 1 March of each year, when all the cases of the previous year are closed. The data in the NNK system are also compared with the post mortem certificates received by the Central Statistics Office; the final data which may be regarded as valid from the reports of the preceding year are made available in May.

Data concerning vaccinations are recorded in a separate interface in the Electronic Healthcare Service Area (hereinafter: EESZT). This means that data on infected persons and data on vaccination are located in two different databases. (In the meantime, a so-called Master Table was generated from the two databases.) The system includes only the location of the vaccination, not the place of residence. There was no time to enter additional data, the primary objective was a rapid recording of the data. One of the fundamental problems and source of errors of data entry was that the system did not provide an opportunity for the automatic entry of the patient's personal data - i.e. entering these data from the accurate and creditworthy healthcare database already available through an in-

terface. Thus, the physicians and healthcare providers admitting the patients had to key in the data manually, increasing the errors arising from erroneous data entry. The ratio of erroneous data concerning the cause of death exceeded 30 percent, and only the data on the dead are validated, hospital care data are not. Another important aspect is that it is not possible to isolate, if a hospital patient is also Covid-19 infected, but the reason for his/her hospital care is not this, as the Covid-19 infection would not otherwise require hospital treatment. In individual cases, the physician providing care could sort these out, but at other times this is not professionally possible, and this may change also from hour to hour for any patient.

Information notified concerning the location of care is available in the OSZIR Infectious patient reporting subsystem; however, NNK is unable to generate the data concerning how many of the Covid patients requiring hospital care were vaccinated and what vaccine was given to these patients. Such a question can only be answered if all the healthcare providers having reported infectious patients in the period under study are called upon to check every single case and correct the information concerning the location of care. A typical example is when the family physician reports a confirmed Covid-19 infected patient notifying him, who is quarantined at home, and selects the information to be entered in the OSZIR data field accordingly. At the same time, it may happen that the patient is taken to hospital in a few days' time, and the family physician is unaware of it. Similarly, patients admitted to the emergency wards of hospitals diagnosed with Covid-19 infection is reported by the hospital characteristically as under hospital care, although the patient may be allowed to go home after a few hours of observation. In such cases the healthcare provider is able to provide valid information after consulting the patient and his/her family, and studying the .pdf documents one-by-one accessible in EESZT.

The IT refurbishment of OSZIR is in progress, more automatic debugging opportunities will be available and it will be easier to process the data, nevertheless the need for human factor validation will remain. NNK emphasized that no organ has accumulated data based on the relevant personal data as to how many Covid-19 infected patients were treated in hospitals, how many patients' breathing was assisted and how many Covid-19 patients were treated in intensive care units.

III.8.2. NAIH's inquiries

In the inquiries related to Covid-19 data, most of the time, the Authority had to check whether the issue of the requested data indeed required the generation of new data and whether the new data could in fact be generated simply and quickly.

A person requested data from the National General Directorate of Hospitals (OKFŐ) with regard to those newly infected, those treated in hospital with coronavirus infection and those dying of coronavirus infection, asking what percentage of them was vaccinated with one and what percentage with two vaccines, however, OKFŐ rejected the data request. The Authority examined whether OKFŐ had data in its possession, of which the requested data could be generated using simple mathematical or other operations not constituting substantial difficulty (such as aggregation). OKFŐ explained that there were no legal requirements, which would place an obligation in it to generate the data in the structure according to the criteria given by the person requesting the data. According to the information they provided the requested data were available in EESZT as follows:

– newly infected: available (Annex 1 to EESZT)
– persons treated with coronavirus infection in hospital: partially available. From the availability of positive Covid-19 test results and the commencement of inpatient care, it can be deducted only conditionally that any given citizen was admitted to hospital with coronavirus disease. This can be stated for certain only if the governing attribute "main diagnosis warranting care" was completed by the healthcare provider entering the data when sending in the inpatient care event. Citizens having positive coronavirus test results 30 days prior to or within 15 days after the commencement of inpatient care are regarded as hospitalised with Covid-19 infection. Screening is complicated by the fact that while EESZT stores data at the level of organisational units, hospital admissions can only be interpreted at the level of institutions. Because of this and because of the frequent relocations within a hospital occurring in more severe cases of infection, a formula has to be applied to determine the commencing and closing dates based on the given institutional care.
– deaths related to coronavirus infection: partly available to the extent it can be unambiguously established that the person was admitted because of Covid-19 infection.

OKFŐ also emphasized that the various data types concerned in the data request could be generated in the EESZT system using database operations only,

specified by an expert, whose full lead time is 56 work hours. OKFŐ provided detailed information on the database operation specified by an expert and their time requirement. The Authority established that the generation of the new data exceeds the level of simple IT mathematical or other operations not constituting substantial difficulties, hence the rejection of the data request was lawful. *(NAIH-193/2022)*

A Member of Parliament requested the vaccination data of Covid patients in hospital care, those requiring treatment by ventilator, and deceased Covid patients from EMMI, NNK and the Prime Minister's Office. NNK has an obligation to collect data only with regard to those deceased; NNK has vaccination data (not in the OSZIR database), which may be linked to this, but compiling the answer by comparing these databases would have been possible only by generating a new database. NNK does not collect data on those requiring hospitalisation or treatment by ventilator.

In addition, the Authority examined what data NNK was required to transfer every week to the pandemic- evaluation register based on Section 2(3)(a) of Government Decree 333/2021. (VI.10.) in force at the time of making the request. The obligation to forward data applied only to the data of the PCR findings and not to the place of treatment or those requiring hospitalization. With respect to hospitalized Covid patients and those requiring treatment by ventilator, the Authority accepted NNK's justification and established that in view of the fact that NNK did not have the requested data, there was no infringement when it rejected the request for these data. The Authority also requested information from EMMI about the statistical analyses it received from the National Health Insurance Fund Manager (NEAK) pursuant to Section 2(2) of the decree. According to the provision referred to, NEAK in collaboration with NNK, OMSZ and OKFŐ produces statistical analyses supporting vaccination strategy, which it sends inter alia to the minister for human resources on a weekly basis. The Authority has found that the questions in the data request cannot be answered from these analyses, because they concerned the vaccination data of those infected by Covid in general, and did not contain data concerning the hospitalization, mechanical breathing support and death of the infected patients. Because of this, the Authority accepted EMMI's justification and established that in view of the fact that EMMI did not have the requested data, there was no infringement. The Authority found the same with regard to the Prime Minister's Office for the same reason. Although the data request did not concern NEAK, the Authority also requested information from NEAK, which explained that it only had data on deaths in publicly funded hospitals in Hungary , but it failed to confirm, despite

repeated requests, whether the requested data are available to NEAK concerning those treated and deceased in publicly funded hospitals in Hungary. *(NAIH-2597/2022)*

In another comprehensive inquiry, a person asked NNK, OKFŐ, the Prime Minister's Office and the Semmelweis Medical University (hereinafter: University) what percentage of those newly infected by coronavirus, those hospitalised with coronavirus infection, those on ventilators and those dying in relation to coronavirus disease were vaccinated and unvaccinated (in a chronological breakdown, processed by the organs contacted). The Prime Minister's Office declared that it did not have the requested data, NNK explained that only Covid-19 infected persons associated with nosocomial epidemics (i.e. those infected in hospital) are included in the judgment referred to by the Authority (Budapest Municipal Court 2.Pf.20.641/2021/4/II.) and in the Excel table also mentioned by the Authority, whereas the data request concerned those hospitalised with Covid-19 infection and whether they were vaccinated.

Concerning the vaccination of those newly infected with coronavirus and those dying in relation to coronavirus disease, NNK informed the Authority that it validated the data received in the meantime and using mathematical operations and by sorting and comparing the data, it generated the requested data and sent the answer to the notifier. This was possible because after the validation of the data received in the OSZIR system, NNK created another register, which contained the requested data. The University informed the Authority that the Clinical Epidemiological Working Group did not have the requested data in an aggregated format with regard to the four university clinics and data were not collected for such a purpose. The requested data exist in the MedSolution system as meta data, but their aggregation according to the data request is not done with respect to the University as neither legal regulation, nor any other obligation to provide such data exists. The University explained that the aggregation of the data in the system amounting to millions of records according to the parameters requested would require the custom development of the MedSolution system, certainly demanding substantial expenditure, in addition the University - even after the development - could provide the requested data only in part with regard to its own institution. In the absence of such development, searching the data of several million records and their requested compilation manually is unimaginable as the University does not have the human capacity to do it. According to the University's statement, the Working Group did not possess the data, of which the requested data could be generated. The Authority established that the University did not commit an infringement. *(NAIH-2597/2022)*

In another data request submitted to NNK, the number of coronavirus infected persons was requested between 1 January 2021 and the day of providing the data, and of this, the number of those having one, two or three vaccinations in a daily breakdown. NNK stated that the requested data were accessible to the public on the website koronavirus.gov.hu and also informed the notifier that the controller is not under an obligation to collect data, or to produce qualitatively new, other data or series of data by comparing the data it processes. The Authority found that NNK violated the notifier's right to having access to data of public interest when it failed to provide the exact accessibility of the requested data, and directed the notifier to a central website instead. Furthermore, it is not clear from the answer given to the data request which of the data were published in the public website mentioned and which are the data which would have to be generated. NNK issued the requested data, but also noted that the requested data were generated exclusively after the NAIH's call using mathematical and IT operations through the comparison of databases generated as a result of the validation of the data. In addition, NNK informed the notifier that the issued data alone, by simple comparison, were not suitable for drawing conclusions concerning the dynamics of the epidemic or the efficiency of the vaccines. *(NAIH-5254/2022)*

III.9. The transparency of municipalities

In general, citizens come into direct contact with organs performing public duties and managing public funds at the level of the municipality of their own settlement, so accessibility to the operation, performance of tasks and financial management data of these organs is of outstanding importance.

III.9.1. The accessibility of criminal data

The accessibility of criminal personal data is a recurrent problem [see Constitutional Court Decision 3177/2022. (IV. 22.) AB presented], and this was also discussed in last year's report: the fact in itself that a criminal procedure is in progress in relation to a case does not exclude the accessibility of all of the documents. Based on judicial practice, the body of representatives of a municipality may put cases on its agenda, in relation to which a criminal procedure is in progress; however, in view of the provisions of Section 27(2)(c) and (g) of the

Privacy Act, the preliminary opinion of the investigative authority, the prosecution or the court taking action in a criminal case (depending on the phase in which the criminal case is) has to be obtained before the session with regard to the pending criminal procedure, which data of the case are subject to the conditions excluding accessibility ; also appropriate organisational and technical (data security) measures have to be taken during the preparation and holding of the meeting to ensure that the data indicated by the organs taking actions in the criminal case are not made accessible to the public. Following anonymisation depending on the answer of the organs contacted, the data may be promulgated while respecting the requirement of purpose limitation in processing. *(NAIH-4668/2022)*

The complainant - the managing director of a business organisation performing municipal public duties at the time of the processing objected to - initiated the Authority's investigation because he objected to several Facebook entries reporting a scandal in which the discovery of the unlawful acquisition of his secondary school certificate and a criminal case launched in relation to this was in the focus. The Authority established that the controllers complained against lawfully processed the disclosed criminal personal data, while discussing a public affair in public, exercising their freedom of expression with a view to informing voters. At the same time, however, the Authority classified the disclosure of the place of birth and the photo of the complainant depicting private activities as an infringement because the former does not qualify as personal data accessible on public interest grounds, while the latter depicted the complainant while acting as part of his private life. *(NAIH-6968/2021)*

According to another complaint, a business organisation fully held by the municipality of a city with county rights, which manages public funds and performs public duties, failed to fulfil the request for data of public interest concerning the organisation's transparency report because a criminal procedure was in progress in relation to that report. When contacted by the Authority, the police station taking action in the criminal case stated that the criminal procedure was no longer in progress when the data request was submitted, thus access to the document could no longer violate the public interest in conducting the criminal procedure. *(NAIH-1099/2021)*

III.9.2. Self-governments of ethnic minorities

Also as part of the KÖFOP research project, the Authority studied and analysed the enforcement of freedom of information in relation to the self-governments of ethnic minorities; the positions of the professional managing organs as well as of the government offices were solicited and the Deputy Commissioner for Ethnic Minorities was also involved in the comprehensive inquiry. Summarising the investigations of specific individual cases, the signatories of the joint report[32] consider it appropriate that the municipal executive and the staff of the mayor's office should actively cooperate in the mandatory electronic publication - i.e. the publication of the relevant documents in the appropriate publication units - and in the fulfilment of requests for data of public interest. The performance of these tasks presupposes mutual, efficient and ongoing cooperation regulated by an agreement based on consensus as well as by internal rules. It is also necessary that the legislator expressly provide, among the mandatory content elements of the administrative contract, for the tasks promoting the transparency of self-governments of ethnic minorities and their distribution in Section 80(3) of Act CLXXIX of 2011 on the Rights of Ethnic Minorities (hereinafter: Ethnic Minorities Act). In the future, informative and case management processes supporting the fundamental work of the self-governments of ethnic minorities, including the development of information and training materials and, in this context, the organisation of personal and online training courses which similarly to the representatives of municipalities provide adequate knowledge and information to the representatives of the self-governments of ethnic minorities with a view to the transparent operation of the self-governments, will have major importance. *(NAIH-8317/2022)*

The municipal executive of a municipality, which also has an ethnic minority self-government, invited the position of the Authority concerning the person of the controller in relation to a request for data of public interest (aimed at accessing data on the emoluments of representatives, employment on public works, contracts of assignment and other wage-type payments). Taking the definitions of the Privacy Act as the point of departure, in this case the ethnic minority self-government is the organ which, in the course of its operation, generates data of public interest and data accessible on public interest grounds and it follows that the ethnic minority self-government is responsible for the data. The Authority established that the data to be accessed through the request for data of public interest were processed by the various organisational units (organisation and

32 https://naih.hu/dontesek-infoszab-allasfoglalasok?download=575:a-nemzeti-adatvedelmi-es-informacioszabadsag-hatosag-elnoke-es-a-magyarorszagon-elo-nemzetisegek-jogainak-vedelmet-ellato-biztoshelyettes-kozos-jelentese-a-nemzetisegi-onkormanyzatok-mukodesi-transzparenciajanak-vizsgalata-targyaban

administration, compliance, finance, audit and internal supply) of the mayor's office, even though they relate to the operation of the ethnic minority self-government. As the performance of public tasks by an ethnic minority self-government is affected under the professional supervision of the municipal executive through the various organisational units of the mayor's office, according to the position of the Authority, the fulfilment of the requests for data of public interest is also the task of the mayor's office managed by the municipal executive. *(NAIH-166/2022)*

Section 103 of the Ethnic Minorities Act states that representatives of the ethnic minority self-governments have to make statements of assets in accordance with Annex 2, to which they have to attach the statements of assets of their spouses/life companions and children living in the same household in accordance with the Ethnic Minorities Act. Pursuant to the second sentence of Section 103(3) of the Ethnic Minorities Act, the statement of assets of representatives of ethnic minority self-governments is accessible with the exception of identification data provided for audits, whereas the statements of their relatives are not. In view of all this, the statement of assets of representatives of ethnic minority self-governments qualify as accessible on public interest grounds, they are accessible to anyone by way of request for data of public interest and can be published in organ-specific publication schemes provided that the identification data needed for checking the statement of assets and the protected data are locked. *(NAIH-1939/2022)*

III.9.3. The transparency of statements of assets

Interest for the statements of assets of mayors and representatives of municipalities, as well as self-governing bodies of ethnic minorities continue to be keen[33]. The statements of assets of mayors and municipal representatives are data accessible on public interest grounds, which must be made accessible to anyone by way of data request. *(NAIH-6476-2/2022)*

Because of the high number of data accesses based on individual requests, several municipalities wished to make decisions on the publication of these data in organ-specific publication schemes and therefore, in compliance with the legal requirement, solicited the opinion of the Authority. The Authority recommends the enactment of municipal decrees concerning the transparent operation and the publication of organ-specific publication schemes because this is a case of

33 https://naih.hu/dontesek-informacioszabadsag-tajekoztatok-kozlemenyek?download=560:tajekoztato-a-vagyonnyilatkozati-rendszer-valtozasairol

so-called mandatory data processing ordered by the controller (in this case the body of representatives). Pursuant to Section 5(3) of the Privacy Act, the type of data, the purpose and conditions of processing, the access to such data, the controller and the duration of the processing or the regular examination of its necessity shall be specified by the act or local government decree ordering mandatory processing, the consent of the data subject is not and cannot be necessary. The data types, which constitute the publication units of the general publication scheme mandatorily published, need not be included in the organ-specific publication scheme. The data in the statement of assets qualify as personal data accessible on public interest grounds, thus the processing of these data, including their publication, is possible only for the period specified in the act ordering the processing, i.e. for one year after the statement of assets was made. The personal data of relatives have to be deleted from the published statements of assets, because they cannot be accessed by people requesting to inspect them. Legal regulation still does not provide an opportunity for the controller to specify a retention or archiving period for the published statements of assets, the term applicable with regard to retention is: "*the previous status is to be deleted*". *(NAIH-4929/2022., NAIH-6903/2022)*

In an inquiry, the mayor's office concerned only partially fulfilled the request for data of public interest for accessing the statements of assets for 2020 of the municipal representatives and the deputy mayor functioning under a community mandate because – apart from the statement of assets of the deputy mayor functioning under a community mandate – the data desired to be accessed were published on the official website of the municipality. The Authority found that three of the published statements of assets revealed the protected personal data of close relatives. The municipal executive in charge of the office rejected the possibility of creating an organ-specific publication scheme "*short of human resources*". *(NAIH-2805/2021)*

III.9.4. Additional data to be published in the organ-specific publication scheme

Following the entry into force of the local decree on the creation of an organ-specific publication scheme, in the case of the subsequent publication of contracts included to the publication unit and in the course of the preparation of future contracts, the Authority recommends that the municipality inform the contracting parties of its intent to electronically publish such contracts in full detail, including

the range of data, the mode, place and duration of publication, , and that the data subjects are duly informed.

To publish invoices accepted by the municipality and its institutions, it is also necessary to create an organ-specific publication scheme. In the course of publication, it is necessary to review the data content of the invoices and the data, which are not of public interest or accessible on public interest grounds, have to be anonymised; the review has to extend to the examination of purpose limited processing with regard to the data content of the invoices received. The Authority disagrees with the publication of municipality decrees, decisions of the body of the representatives, public procurement procedures launched and the audit reports carried out at the municipality in organ-specific publication schemes because these sets of data belong to the publication units of the general publication scheme, whose publication is mandatory. (*NAIH-6903/2022*)

III.9.5. Financial management data

The complainant initiated the investigation of the Authority with regard to rejected data requests, in the case of which business organisations held by the municipality failed to provide data of public interest on contracts, which they concluded with a business organisation held by the incumbent mayor and his wife. Under the data principle, according to the consistent practice of the Authority and the courts, the data of the requested contracts regarded as business secrets must be examined one by one and established exactly which are data qualifying as business secret, whose disclosure would give rise to disproportionate violation of interest. As a main rule, public interest in the accessibility of the financial management of public funds and state or municipal assets precedes the protection of business secrets. The automatic declaration of the entire document as a business secret is not acceptable. It is necessary to substantiate with reference to specific facts which data of the requested documentation and why are subject to the Act on Business Secrets. Within this, the facts, data and compilation related to the business activity concerned, which are to be protected, must be accurately indicated together with the technical, commercial and organisational knowledge, experience or their compilation of value are contained in the documentation requested to be issued. Furthermore, the specific financial, commercial or market interests, which would be violated by access to the data, would have to be named. In addition, it is also necessary to consider which of these data regarded as business secret are the ones whose disclosure would cause disproportionate injury to the holder of the data. *(NAIH-4236/2022)*

The complainant wished to access data related to the use of a property held by the municipality subject to local protection. Following the calls of the Authority, the controller municipality made the contracts available to the complainant, but the information related to the financial conditions and the names of persons administering the transaction - representatives of business organisations, law offices - were blocked. The Authority called the attention of the municipality to the fact that the data of business organisations and undertakings entering into business relationship with the municipality and the data of the law office, as well as of the person representing it. are data of public interest or data accessible on public interest grounds. As the municipality failed to respond to the calls of the Authority, a public report was issued on the case. *(NAIH-221/2022)*

In its response to a consultation request on sending the draft budget supporting decision-making prepared as an internal work document to a third person by a municipal representative, the Authority explained that based on the Privacy Act, information which genuinely constitutes part of the decision-making process, whose disclosure could jeopardise the success of implementation or would allow individual market agents to gain unjustified advantage can be excluded justifiably from accessibility as decision supporting data. At the same time, restriction of accessibility of decision support data cannot aim at rendering preparation for decision-making untransparent, to the contrary, its purpose is to allow the organ performing public tasks to carry out its internal decision-support activities free of unauthorized influence. The head of the organ processing the data, i.e. the municipal executive, may allow access to the draft budget prepared as an internal work material as decision-support data by a third person; the municipal representative may not have lawfully forwarded it to a third person without the permission of the municipal executive. *(NAIH-2945/2022)*

Pursuant to Section 27(3)-(3a) of the Privacy Act, in the case of a financial or a business relationship with a municipality, the name of the contracting party is definitely data accessible on public interest grounds. Natural persons who rent property held by a municipality in view of their welfare situation or enter into some other type of contract related to the utilisation of assets or the use of municipal funds taking their welfare situation into account cannot be regarded as persons in a business relationship with the municipality. In view of the fact that they use public property or public funds, their personal data other than their names and the fact of the legal relationship included in the contract do not qualify as data accessible on public interest grounds.

III.9.6. Data accessible on public interest grounds, personal data

The fact of unworthiness established about a municipal representative or mayor is data accessible on public interest grounds because it is directly related to the performance of their public duties. The municipality's body of representatives has to make a decision on this at a mandatorily closed session, and as under Section 52(3) of the Municipalities Act, the decision of the body of representatives made in a closed session is accessible to the public, hence by the publication of the decision on unworthiness in the general publication scheme, the municipality meets its obligation to provide information. At the same time, if the cause resulting in the fact of unworthiness is established not in relation to the performance of public duties related to the position of a representative, such data continued to be personal data to be protected and neither the details of the procedure, nor the specific cause qualify as data accessible on public interest grounds. *(NAIH-7194/2022)*

The municipal executive of a mayor's office asked whether the minutes of a public meeting of the body of representatives could record the representative's remarks, in which - in relation to the subject matter - he named the business organisation with which the municipality concluded a contract and the fact that it was subject to distraint by the National Tax and Customs Administration. Authorised by an act, the National Tax and Customs Administration publishes numerous data within the notion of tax secret on its official website. According to Section 125 of the Taxation Act, the tax authority keeps public records on its website with regard to data specified in Section 266(d) and publishes inter alia the names and tax numbers of taxpayers with reference to erasure against whom the National Tax and Customs Administration conducts a distraint procedure, from the commencement of the distraint procedure until its completion. The full transparency of the public trade register data of companies, including business organisations, ensures accessibility to data significant for the protection of creditors, thus the answer to the question asked by the municipal executive is clearly: yes. *(NAIH-419/2022*)

Municipal representatives obtain their mandates enjoying the confidence of the majority of voters, this underlies their responsibility for the entire municipality, including the representatives' rights and obligations. The quality and effectiveness of the work of the municipality depends fundamentally on the work of the municipal representatives, so exercising the rights of representatives is also an obligation: to appear, to prepare, to ask questions, to make comments, to vote responsibly, to comply with the confidentiality obligation, to maintain contact with

voters and to behave in a manner worthy of public activities. Thus, the representatives' votes cast on the individual items of the agenda at a public session of the body of representatives are data generated in relation to their discharge of public duties and are data accessible on public interest grounds, the votes cast by roll call can be displayed on the display showing the results of the vote. *(NAIH-6902/2022)* The accessibility of the votes of representatives cast in private sessions is restricted by secret ballot according to Section 18(4) of the Municipalities Act. *(NAIH-5501/2022)*

A representative made a video and sound recording using his mobile phone prior to the opening of the session of the body of representatives and shared the recording in a public Facebook group. The complainant explained that persons not qualifying as public actors (municipal executive, deputy municipal executive, heads of the departments of the mayor's office) also participated in the session of the body of representatives, and the purpose of the controller was to discredit the session of the body of representatives and of the municipal representatives and make them look ridiculous. As the session could not be opened on account of obstruction by representatives, no information was given that could qualify as data of public interest at the event. According to the position of the Authority, the behaviour of the members of the body of representatives, which prevented the body of representatives to work, is information of public interest for a wide range of voters. The transparency of municipal operation means not only accessibility of the decisions made, but also the transparency of the decision-making processes. Participation in a public session of the body of representatives in an official capacity qualifies as action in public life according to Section 2:48(2) of the Civil Code and there is no need for the consent of the data subject for recording it, using the recording or streaming it. In addition to the municipal representatives and the mayor, the civil servants performing their public duties at the public session of the body of representatives participating in an official capacity are also to be regarded as public actors, who are obliged to tolerate wide-ranging publicity concerning their activities related to the performance of their public duties. *(NAIH-7570/2022, NAIH-6892/2022)*

In a case related to the amendment of the local building code of a municipality, the Authority found unauthorized processing because of the publication of the decision of the body of representatives on residents' request submitted for the review of the settlement development concept and the settlement planning instruments, and called upon the municipality to remedy the infringement found. With respect to proposals made within the framework of partnership reconciliation with names and other personal data, it is not the citizen who submitted the

proposal that is relevant, but the content of the proposal is important for the municipality's decision-making. Because of this, the publication of the identity and personal data (name, address, other identification data) of the person making the proposal cannot be regarded as necessary either when considering the proposals, or when developing the final decision or when publishing the decision. *(NAIH-5736/2022)*

In his complaint, the complainant objected to the data processing practice of the evaluation procedure of applications to the post of head of institution invited by one of the national self-governments of ethnic minority. In contrast to the complaint, the Authority established that the expert committee lawfully involved in the evaluation procedure of applications for the post of head of institution carried out its work in a private session excluding the public. Applicants were heard in an alphabetic order one by one, which was substantiated by the minutes of the committee's meeting. According to the Authority's position, the professional opinion provided by the expert committee was based on legal authorisation and Article 6(1)(e) of the General Data Protection Regulation can clearly be indicated as the legal basis of processing. *(NAIH-3429/2022)*

III.10. Freedom of expression - on-line transparency

A complainant objected to being included in a publication of an NGO dealing with events suspicious of corruption. In his view, the publication was on the one hand based on untrue articles and on the other hand it placed the collected information into a new context and drew untrue conclusions from them. The controller informed all the data subjects of the processing prior to its commencement. The information provided said that the primary legal basis of processing was Article 6(1)(e) of the General Data Protection Regulation because the petitionee functions as a foundation for public benefit, its goal is inter alia to map out problems of corruption, informing the public, checking whether expectations concerning transparency were met and facilitating transparency, particularly in view of the use of public funds. Publishing the publication serves this purpose and therefore constitutes an activity of public interest. Secondarily, in view of the practice of the Authority, the petitionee also indicated Article 6(1)(f) of the General Data Protection Regulation and also carried out a balancing test in this context. First and foremost, the Authority stated that data protection supervisory authorities will not and may not take action in cases subject to the competence of civil courts and the right to the protection of personal data cannot become an instrument of

restricting opinions hurtful to the data subjects and (perceived to be) unlawful from the viewpoint of civil law. Accordingly, the Authority did not and could not examine the petitioner's allegations concerning untruthfulness and defamation. At the same time, by indicating two legal bases for the same processing operation, the controller violated the principle of transparency. The Authority accepted the legitimate interest of the controller as the legal basis of processing with the provision that although the petitionee acted superficially in assessing the circumstances of the petitioner and in the balancing of interests and did not do everything in order to examine the consequences of processing, particularly those concomitant with accessibility, with regard to the individual life situation of the petitioner, the deficiencies exposed in relation to the balancing test did not reach the level enabling the establishment of an infringement in view of all the circumstance of the case and the purpose of processing. In this regard, the Authority took into account in particular that the petitionee carries out activities of public benefit as an NGO. Furthermore, the Authority established an infringement of Article 21(4) of the General Data Protection Regulation, because, in its information, the petitionee listed the right to object in the same sentence as the other rights of data subjects, mentioning only that a data subject has a right to object, although pursuant to the General Data Protection Regulation, the controller has to display the information related to the right to object clearly and separately from all other information. *(NAIH-1047/2022)*

In another case, the complainant objected to the fact that the information displayed on the datasheet of the one-man law office bearing his name included data referring to negative credit events on a company information website. In the course of the procedure, the Authority had to decide whether the data of the one-man law office qualify as the personal data of the lawyer. The Authority based its decision on the fact that in the event of a legal person, such as the law office, the legal person and the natural persons behind it can be clearly delineated and although a natural person takes action by necessity on behalf of and in the interest of the legal person, this does not warrant classifying legal facts related to the legal person as part of the private sphere. Doubtless, the relationship between the natural and the legal person in the case of a one-man law office is much closer, yet even in this case the subjects of the law are clearly separate, the rights and obligations of the law office can be clearly separated from those of the member of the law office as a natural person. The Authority also referred to Recital (14) of the General Data Protection Regulation, which clearly states that the Regulation does not cover the processing of personal data, which concerns legal persons. In view of this, the Authority rejected the petitioner's petition. *(NAIH-740/2022.)*

III.11. The transparency of environmental data

The accessibility of environmental information is frequently restricted with reference to the fact that the *person requesting the data is not a client in the procedure*, hence he cannot have access to the data of public interest he wishes to know. The Authority consistently established the primacy of the Privacy Act as a source of law in these cases, and warned that it is improper practice to qualify requests for data of public interest as requests to inspect them and thereby restrict the transparency of environmental information.

A complainant requested a permit to cut down a tree and the application for the permit from a municipality, which justified the rejection of the request stating that "*the decision is an individual case of administration containing personal data*" and the complainant did not meet the legal conditions of inspection as a third person. The Authority referred to judgment P. 20.997/2019/8 of the Budapest Municipal Court, according to which "*Section 33(1)-(4) and (6) of the General Administrative Procedures Act referred to inspection of documents, but the decision according to paragraph (5) is accessible to anyone without restriction"*. The decision containing the permit to cut down a tree qualifies as environmental information according to Section 2(c) of Government Decree 311/2005. (XII. 25.) on the order of public access to environmental information (hereinafter: Decree) as a measure related to the environment taken to protect the environment and its elements. Upon the Authority call, the municipality sent the requested decision and application to the petitioner while blocking the personal data. *(NAIH-1948/2022)*

Also in the area of access to environmental information, one of the most frequent reasons of rejection is reference to supporting decisions pursuant to Section 27(5)-(6) of the Privacy Act. It is a general problem that the holders of the data maintain automatically the restriction of access to data supporting decision-making even after the decision has been made, although by then the main rule is the accessibility of the data. In the public procurement procedures concerning the development of Lake Fertő Aquatic Centre I (Procedure 1) and the development of the Lake Fertő Aquatic Centre II (Procedure 2), the draft contracts demanded the use of an Llc specified by name to perform the monitoring tasks. The notifier requested the tourism development non-profit company (hereinafter: Zrt.) to provide the details of the procedure concerning the selection and use of the Llc. According to the Zrt., the data of the procedures in progress are data supporting decision-making and thus they are not accessible until the selection of the winning bidder. At the time of the data request, Procedure 1 was already closed,

hence the Zrt. incorrectly referred to Section 27(5) of the Privacy Act. Procedure 2 was still in progress at the time of the data request. Despite this, the Authority did not accept the Zrt.'s reference to Section 27(5) of the Privacy Act, because the specification of the content of the public procurement documentation also qualifies as "decision", including that the draft contract constituting a part of the documentation named the Llc. as performing monitoring. The data supporting the decision to select it and the public procurement document - as the decision on launching the public procurement decision was already made and the announcement of the procedure was already published - are accessible to the public as a main rule. The Zrt. failed to accurately specify the legal regulation that prohibits the issue of public procurement documentation in the event of a request for data of public interest and in what way the accessibility of data concerning the selection of the company for monitoring and of the public procurement documentation would jeopardize the closure of the procedure - i.e. its justification did not exceed the level of generalities. When carrying out the balancing test based on Section 30(5) of the Privacy Act, according to the Authority's position, the fact that the data concerning the selection of the company for monitoring qualifies as environmental information based on Section 2(c) of Government Decree 311/2005. (XII.25) is of particular importance. The requirement of monitoring serves the protection of an area, which is part of world heritage, it is a protected nature conservation area, it is part of the Natura 2000 network, it is a special bird protection area and a natural conservation area of outstanding importance, there is therefore an overriding public interest in the accessibility of the data concerning the selection of a company doing it. *(NAIH-4719/2022)*

An NGO submitted a data request to the National General Directorate of Water Management (hereinafter: OVF) in relation to the Lake Fertő Aquatic Centre. The subject matter of the data request was a letter by the regional water management directorate containing a statement that the final state planned by the contractor would enable the performance of their specialised tasks in the beach zone. In OVF's view, if it had to presume in all its internal correspondence that it was likely to come to the attention of a third party, the communication would cease to be able to transmit certain data, facts and statement, which would significantly hamper the activities of the organs of public administration or even render it impossible. The Authority does not doubt the public interest in restricting the accessibility of internal communications among organs of public administration. However, the fact whether the organ's decision was already made or not, is of fundamental importance in restricting public access. Based on Section 27(6) of the Privacy Act, they have to assume that even internal correspondence could be accessible to the public if they cannot substantiate why they believe that access to their internal correspondence would jeopardise the lawful functioning of the organ or the performance of duties without undue external influence. Future decisions will also have to be accurately specified and they have to be made within the foreseeable future, so the Authority did not accept OVF's statement that the requested letter "*would qualify as a document serving as the basis for responding to any other requests from citizens*". *(NAIH-3894/2022)*

Another notification objected to the fact that the protocols and testing data from the testing of sub-surface waters by a company and the testing of the monitoring wells located on one of the premises of the company submitted to the Budapest Disaster Management Directorate (hereinafter: Directorate) and the documents of the authority investigations of the company's premises by the Directorate were not issued. According to the information provided by the Directorate, the requested data were uploaded to the OKIR system. Similarly to the notifier, the Authority also experienced that there was no possibility to query the data because the database "*was under development*". The Directorate also explained that with regard to the data uploaded to the OKIR system, the controller according to Section 3(9) of the Privacy Act was not the Directorate, hence it was unable to forward data from the database. Pursuant to Section 2(a) of the Regulation, the results of sub-surface monitoring qualify as environmental information. The Privacy Act does not specify as a condition of fulfilling data requests that the organ performing public tasks determine the purpose of processing the requested data. Furthermore, neither does the convention on access to information, public participation in decision-making and access to justice in environmental matters adopted in Aarhus on 25 June 1998 (promulgated by Act LXXXI of 2001) subject the issue of environmental information to a condition of the same content specified in Section 3(9) of the Privacy Act. The Directorate sent numerous monitoring documents to the Authority, hence these data were processed by the Directorate and were obviously generated in relation to its activities, so they have to be issued to the person requesting them, while blocking the data to be protected in view of the fact that they were not accessible from the public source indicated. Information about the data does not replace the issue of the data. In relation to public access to the requested statements of the specialised authorities, the Authority explained that environmental information in general consists of objective data and facts, in the case of which – particularly once the decision was made – it is highly questionable whether their accessibility would frustrate the efficient implementation of the decisions or jeopardise independent and effective work by civil servants, free from undue external influence. The Directorate should have carried out the balancing test required under Section 30(5) of the Privacy Act and should have presented its criteria and results to the Authority.

The Authority called upon the Directorate to send the monitoring results, the requested protocols and statements by specialised authorities to the notifier. However, the Authority terminated the investigation because in the meantime, the notifier also launched a court procedure. *(NAIH-252/2022)*

The purpose of a *preliminary environmental study* is to enable the environment protection authority to establish whether the implementation of the planned activity could have substantial impact on the environment, and according to this, to decide on additional requirements, or that a permit of implementation may not be issued. Access to the documents of the procedure is of particular importance in order that local residents are allowed to assess what kind of impact the planned activities will have on their living conditions.

The notifier submitted a data request concerning the details of an investment project which pursuant to Section 3(1)(a) of Government Decree 314/2005. (XII.25) on environmental impact assessment and the procedure for granting integrated permit to use the environment (IPPC permit) is subject to preliminary impact assessment. Based on Section 2(c) of Government Decree 311/2005. (XII. 25), the documentation of preliminary assessment contains environmental information. Based on point 3 of Annex 4 to the Government Decree, the data constituting business secrets according to the user of the environment will have to be designated as such and presented separately in the documentation of the preliminary assessment. The Authority found that if the company did not make use of this opportunity, it should have issued the entire document to the person requesting the data. In addition, the investment was financed and supported by the tender submitted under the call for proposal GINOP 7.1.2 -15, , so the Authority called upon the company – with success – to issue the data of the investment implemented through the use of public funds, which do not qualify as business secret, and the data, which do qualify as business secret, but whose disclosure would not give rise to a disproportionate harm to commercial activities, as well as the documentation of the preliminary assessment. *(NAIH-2564/2022)*

In a notification related to another preliminary assessment procedure, the publication practice of a municipality and a government office was objected to in a preliminary assessment procedure for a bicycle path. According to the obligation set forth in Section 3(2) of the Government Decree, the environment protection authority has to publish the application and its annexes electronically in the preliminary assessment procedure. Section 3(3) of Government Decree 314/2005. (XII. 25) requires that the environmental protection authority publish the name and office contact data of the case administrator in its announcement. The announcement of the environment protection authority included information stating that the competent municipal executive provides an opportunity for those concerned to exercise their rights of making statement and inspecting documents and if requested, provides detailed information during consulting hours. Section 3(4) of the Government Decree requires the full publication of the announcement of the environment protection authority, which the municipality failed to comply with and thereby infringed the notifier's right to access data of public interest and also violated this right by failing to publish the announcement in Section II.10 of its general publication scheme. So, the notifier could not obtain information on the option of inspection in person as an alternative to unsuccessful electronic access, or of the contact data of case administrators, who would have been able to help him with downloading the documents. *(NAIH-7524/2022)*

III.12. Public education, higher education

Inquiry into a number of data requests addressed to School District Centres were put on the agenda, which were related to education-related social problems and debates. The most significant of this was the complaint of the Teachers' Trade Union (hereinafter: PSZ) because of rejecting requests for data of public interest – *how many colleagues working in public education and vocational education were on sickness benefit, for altogether how many days they were absent, how many employment relationships were terminated and of this, how many people retired or diseased between 1 January and 30 June 2021* – submitted to the Hungarian Treasury (MÁK), the 60 School District Centres and the 40 Vocational Training Centres. After 90 days, in their letters rejecting the data request, the contacted organs referred to not processing the data in the requested format, they could not be required to generate them, and they also made reference to Constitutional Court Decision 13/2019. (IV. 8.) AB, which stated that *"the controller is not under an obligation to collect data, or to generate new, qualitatively different data or data series by way of the comparison of the data it processes. Furthermore, the person requesting the data may not claim a right to have somebody else query the data, which are otherwise accessible."* In the course of its inquiry, the Authority found that a substantial part of the data requested by the notifier were processed by these organs and the Constitutional Court Decision referred to may not be applied as reason for rejection because the data need not be generated by physically searching one by one for sickness benefit documentation and death certificates and other documents as they have been available electronically and could be obtained from the databases and payroll programs

processed by the employers with a simple IT operation. Moreover, in an earlier period, MÁK already provided the data indicated in the petition for inquiry to the notifier and the legal environment has not changed since then.

In this case, the Authority contacted and sent several calls and orders to the Klebelsberg Centre (KK), the National Office for Vocational Training and Adult Training, MÁK, the Ministry of Human Resources, the Ministry of the Interior, the Ministry of Culture and Innovation, the Office of Education and to all the School District Centres and Vocational Training Centres of Hungary. In its response, the Ministry of the Interior explained in detail that the school district as employer processes the data related to the personal remuneration of teachers; with regard to sickness benefits, the school district as employer records the absence data of public employees (e.g. the fact of incapacity for work and its duration) in the centralised payroll system (KIRA) and forwards the medical documents related to incapacity for work to MÁK.

However, in the absence of legal authorisation, the school district does not record the specific reason for incapacity for work. Thus, concerning the issue of how many employees were on sick leave or received sickness benefit as a result of viral infection, the employer does not have recorded data. The data processed by the school districts can be generated using mathematical and IT operations. The data sets indicated are processed by the organisational unit of the school district in charge of human resources, the average headcount of those working there is 5 to 6 people per centre. The generation of the data by the school district is possible by querying KIRA and the SAP HR module of the KRÉTA administration system and by sorting them in Excel tables. This means that the data that the trade union requesting the data wished to access were existing recorded data actually processed by the school districts, except for whether the reason for the sickness benefit was coronavirus infection, and they can be retrieved from the databases of the school districts by electronic query. In this case, based on the Fundamental Law, the Privacy Act as well as the relevant decision of the Constitutional Court, the school district is under an obligation to meet the request for querying the data according to specific criteria and organising them in a table. Ultimately, the school district centres and the vocational training centres complied with the Authority's call and issued the requested data of public interest to the notifier. *(NAIH-235/2022, NAIH-237/2022, NAIH-3649/2022)*

In the other significant inquiry case, the notifier Member of Parliament objected to the rejection of his request for data of public interest – a comprehensive set of questions concerning motivational awards and festive rewards paid – submitted to the school district centres and the Klebersberg Centre after 90 days with reference to Constitutional Court Decision 13/2019. (IV. 8.) AB and Section 30(2) of the Privacy Act. It should be noted that this section of the law can apply only if the organ performing public duties fulfils the data request by sending an accurate link. The websites provided by the school districts, however, were not accurate and did not contain the requested information. Ultimately, upon the call of the Authority, the requested data were issued. *(NAIH-6111/2022)*

In another group of cases, also a Member of Parliament turned to the Authority because of the negative response of the Ministry of Human Resources (EMMI). The notifier would have liked to know the number of students commencing and successfully completing training, providing the qualifications and skills needed to fill the post of a teacher, and the number of those newly entering the teaching profession in academic years 2020/2021 and 2021/2022 in a breakdown by kindergarten/school. With regard to the first two questions EMMI stated that it did not have the data in the absence of competence and with regard to the third question, it referred to Constitutional Court Decision 13/2019. (IV. 8.) AB. The data requested by the notifier are data of public interest, which the notifier in July 2019 had already received retroactively for 9 years for the period 2010-2019. In the course of its investigation, the Authority found that the notifier was not informed of which organ performing public duties processes the requested data, or of the fact that with regard to the 3rd question the data are available from October. Furthermore, the notifier requested the data not for each kindergarten and each school, but for teachers in kindergarten and school – i.e. he requested two data each with regard to the two years mentioned, , so based on the above, the Authority called upon EMMI to send the latter data to the person requesting them free of charge and without delay. The data in points 1 and 2 of the data request can be requested from the Ministry for Innovation and Technology (hereinafter: ITM), which the notifier did and turned to ITM and the Office for Education.

In its response, ITM explained that according to their position, EMMI informed the Authority not about who qualifies as controller with regard to the requested data, but indicated that the area of higher education and vocational training as a special area now belong to the scope of responsibilities and powers of ITM. So, they again informed the notifier that ITM does not qualify as controller according to Section 3(9) of the Privacy Act with regard to the data requested. After this, the Authority called upon ITM and EMMI to investigate the whereabouts of the data of public interest requested to be accessed by the notifier and asked for information whether the requested data are processed by the two ministries mentioned, to which organ the data requested by the notifier were forwarded from

EMMI and where the notifier can turn to in order to request the issue of the data. Furthermore, the Authority informed the ministries that the capacity of controller according to Section 3(9) of the Privacy Act can only be interpreted in the context of processing personal data; however, this case did not concern the accessibility of personal data. In its response, EMMI informed the Authority that the Office for Education (hereinafter: OH) has the responsibilities and powers with regard to the requested data. At the same time, OH invoked Constitutional Court Decision 13/2019. (IV. 8.) AB and stated that it was unable to produce the data requested by the notifier even with substantial human resources, hence it was not going to alter its position concerning the issue of the data. ITM informed the Authority that the requested data can be obtained from the higher education information system (hereinafter: FIR); OH was responsible for FIR's operation and they ensure the accessibility of data of public interest and data accessible on public interest grounds processed in FIR. Based on the above, the Authority established that the data of public interest requested to be accessed were processed by OH, the data were available electronically and could be obtained with simple IT operation. Based on the above, the Authority called upon OH to send the data of public interest processed in FIR and to be accessed to the notifier without delay. Upon the Authority's call, OH's president issued the data available in OH on 11 March 2022 to the notifier as requested. *(NAIH-7637/2021, NAIH-552/2022)*

Numerous objections were received this year too because of the unlawful publication of the personal data of children – on Facebook or on websites – primarily with in nurseries, kindergartens and baby clubs. The Authority asked the institutions in every case to provide information in writing about the purpose and the legal basis of processing and requested that if they do not have the legal basis appropriate according to the General Data Protection Regulation for the processing of personal data the entries containing personal data (in this case photos) should be removed and they should pay attention in the future to the data protection settings, particularly with regard to the visibility of entries containing personal data. It also called upon the institutions to remove from their social networking site the photos and video recordings of children previously published,, in whose case the parents did not consent to the publication of the images of their children in an identifiable manner. *(NAIH-2885/2022, NAIH-6053/2022).*

The students of the Szeged University of Sciences notified the Authority that the Students Self-Governing Body (EHÖK) failed to respond to their data requests submitted four times in which they objected to the inaccessibility of spending by EHÖK and the student self-governing bodies of the faculties on EHÖK's website. The Authority established an infringement and called upon EHÖK to send

the data of public interest requested to be accessed to the notifiers in the format required by them; the data request can also be fulfilled by publishing the data in EHÖK's website and sending the specific URL addresses to the notifiers. Finally, EHÖK's new president informed the Authority that they fulfilled the notifier's data request. Nevertheless, the Authority called the attention of EHÖK to the fact that as an organ performing public duties, EHÖK has to meet its electronic publication obligations as required by Chapter IV of the Privacy Act and to publish its data of public interest on its website according to the general publication scheme of Annex 1 to the Privacy Act. *(NAIH-3263/2022.)*

A parental forum requested consultation with the Authority concerning the issue of whether data on the qualifications of teachers teaching the children and data concerning their substitution at school, the data on the qualifications of the substituting teacher are accessible. The data requested by the parents are data accessible on public interest grounds, whose accessibility is guaranteed by Section 26(2) of the Privacy Act; furthermore, based on Government Decree 229/2012. (VIII. 28.) on the implementation of the Act on National Public Education, institutions of public education have to publish the data concerning the qualifications of teachers on their websites *(NAIH-6482/2022).*

III.13. Classified data and Authority procedure for the supervision of data classification

In the course of a litigation for the issue of data of public interest, the Budapest Municipal Court initiated an authority procedure for the supervision of data classification by the Authority, in view of the fact that the controller (the respondent of the litigation before the Budapest Municipal Court) refused to fulfil a request for data of public interest, because the requested data were classified.

The Authority established that the purpose of conducting the authority procedure for the supervision of data classification initiated by the Budapest Municipal Court was in actual fact impossible as the conditions of conducting an authority procedure for the supervision of data classification did not exist with regard to the data according to the subject matter of the litigation. Upon the call of the Authority, the controller was unable to show which of the information requested in the complaint was classified data. In this context, it only informed the Authority that the documents with which it could produce the requested data – the filing records kept according to Section 43(3) of Government Decree 90/2010. (III.26.)

on the order of processing classified data (hereinafter: Government Decree) - carried repeated classifications. According to the position of the controller, the filing records can only be used to assist with the handling of documents, the data requested by the petitioner cannot be produced from them.

The Budapest Municipal Court sent extracts of the filing records kept by the respondent to the Authority (excluding the pages which could contain classified data). The Authority reviewed the extracts of the filing records, compared them with the data constituting the subject matter of the litigation and upheld its former position according to which the data request listed in the complaint do not relate to specific information contained in the documents entered into the filing records, but to the fact of general information concerning them. These data do not correspond to the classified data in the documents concerning which the repeatedly classified filing records may contain information.

Based on Section 45(2) of the Government Decree, if any information of merit can be derived from the filing records as to the content of the classified data processed, the classification marking appropriate to the data processed containing the highest level of classification must be repeated on the cover of the filing records. In the course of the examination of the filing records sent, the Authority found that in accordance with the legal regulation referred to, the cover of the filing records bore the repeated classification marking; however, the data recorded in the extracts of the filing records sent do not refer to the classified data in the documents which, according to the evidence of the filing records, were processed by the respondent. They are data, which have to be applied in general when processing classified documents; they represent information concerning the identification of the filed documents, the sending organ and the arrival and filing of the document. From these, no inferences can be made as to the content of the classified data in the documents shown in the filing records.

Therefore, the conditions of launching and conducting an authority procedure for the supervision of data classification did not prevail in view of the fact that the controller (respondent) did not even formally substantiate that the information requested as data of public interest indicated in the complaint were classified, because the data constituting the subject matter of the litigation were not included in the documents bearing the repeated classification marking sent by it.

Pursuant to Section 62(4) of the Privacy Act, the classifier of the data shall be a party to authority procedures for the supervision of data classification. Therefore, as a preparatory question for the authority procedure for the supervision of data

classification, the Authority also wished to clarify who classified the data according to the subject matter of the litigation before the Budapest Municipal Court and what was their classification marking. It was found that the classifiers, shown in the repeated classification marking of the filing records according to Section 7 of the Act on the Protection of Classified Data, classified data other than those constituting the subject matter of litigation, hence they could not become parties to the authority procedure for the supervision of data classification as persons classifying the data that constituted the subject matter of the litigation in progress before the Budapest Municipal Court. At the same time, the legal regulations in force do not enable the Authority to examine the lawfulness of the repeated classification at the controller applying the repeated classification marking under an authority procedure for the supervision of data classification, involving the controller or its representative in the procedure as a party because only the classifier may be a party to an authority procedure for the supervision of data classification.
The Authority continues to emphasize the following in relation to classification and fulfilling requests for data of public interest.
The Fundamental Law protects personal data, but in the case of data of public interest, it endeavours to guarantee access and dissemination, which is a precondition to participation in public affairs and public life. This was confirmed by the Constitutional Court when it declared that free access to information of public interest allows for the control of lawfulness and efficiency of the elected representative bodies, the executive power and public administration and encourages their democratic operation. Because of the complicated nature of public affairs, citizens' control and influence over decision-making by the public power and the administration of affairs can only be efficient, if the competent organs disclose the necessary information. [Constitutional Court Decision 32/1992. (V. 29.) AB]
The classification of data is the most severe restriction of the freedom of information. When in relation to some information reference is made to the fact that it is classified data, the following should be taken into account:

The accurate specification of the classified data is essential because the rules of the protection of classified data are based on the data principle and not on the document principle. Paragraph [49] of the justification of Constitutional Court Decision 29/2014. (IX. 30.) AB expounded this as follows:

"With regard to the extent of the restriction, furthermore, attention must be paid to the fact that withholding information may not apply in general to the documents, hence constitutionally a regulation which withholds documents from publication not according to their content is not constitutionally acceptable [cf. Constitutional

Court Decision 32/1992. (V. 29.) AB, ABH 1992, 182, 184.]. "In the interest of the enforcement of the right to access and disseminate data of public interest, a restriction, which finally withdraws a data or an entire document from publication or which restricts access to a document in full irrespective of its content, cannot be regarded as being in line with the Fundamental Law."{Constitutional Court Decision 21/2013. (VII. 19.), Justification [46]}. Furthermore, it cannot be reconciled with Article I(3) of the Fundamental Law as a restriction of the right to access and disseminate data of public interest cannot be regarded as unconditionally necessary, if in a given case, by citing the reason for restricting access, access to a wider range of data of public interest is forbidden, then what would be necessitated by the reason for restriction provided. In particular, this can be established whenever access to all the data of public interest in a given document is refused simply by reference to the fact that a part of the document is subject to access restriction […]." {Constitutional Court Decision 21/2013. (VII. 19.), Justification [60]}."

According to the provisions of Constitutional Court Decision 13/2019. (IV. 8.) AB and the position of the Authority, a request for data for public interest cannot be refused because the requested data is not available directly or by way of electronic querying. It may be that the data have to be searched, sorted according to specific criteria and organised. The controller is not under an obligation to obtain or collect new data, nor to generate qualitatively new data or an explanation of the data. Nor may the controller rely on the fact that rendering the requested information accessible would require additional work resulting in the expenditure of time and additional costs. The Privacy Act does not include such reasons for refusal. (*NAIH-3055/2022*)

III.14. Other cases commanding substantial public interest

The Authority received several notifications from a person requesting data in relation to a national series of 228 concerts and events called 2021 "Őszi Hacacáré" (free concerts, community events, family programmes, village fetes and arts and crafts activities). The complainant unsuccessfully requested Antenna Hungária Zrt., Visit Hungary Zrt., the Magyar Turisztikai Ügynökség and several subcontractors to send all the contracts and other documents concerning the series of concerts. In view of the amount of public funds used (close to 5 billion forints) it is understandable that the documents and contracts generated in relation to the series of concerts commands substantial interest. According to the facts of the case established in the course of the investigation, the Nemzeti Kommunikációs Hivatal (National Office of Communications) launched a public procurement procedure to provide event organisation services, whose winning bidder, Antenna Hungária Zrt., entered into a general framework contract with Visit Hungary Zrt. Another two actors in this group of cases also concluded contracts with Antenna Hungária Zrt., on performing services for the administration of the concert series. Being called upon to do so, the individual companies sent the contracts to the complainant, blocking the data, which in their view were to be protected; however, the Authority could not accept as reason for rejection that the business organisations concerned in the case were not organs performing public duties and hence the scope of the Privacy Act does not extend to them. At the time of submitting the data request, Antenna Hungária Zrt., was held by the state, hence it is under an obligation to issue the requested data. At the same time, pursuant to Section 27(3)(a) of the Privacy Act, this obligation to provide information also applies to the companies in a business relationship with it. Based on Curia Judgment Pfv.20.904/2021/5 and Decision Pf.20.031/2019/5 of the Budapest Municipal Court, the Authority took the position that a business organisation held by the state belongs to a subsystem of public finances in view of the above provision of the Privacy Act, hence those in a business relationship with it have also to ensure the transparency of the use of public funds. Certain business organisations cited the protection of business secrets (for instance, the name of the person representing the company, contractor's fee, advance payment, penalty for delay) on several occasions and on that basis, refused to issue the contracts and the related documents or blocked data of public interest in the documents. In its call sent to the companies, the Authority underlined that based on Section 27(3) of the Privacy Act access to the data of documents (business secrets) can only be restricted, if it does not prevent access to data accessible on public interest grounds. The guidelines published by the Authority on the limits to access to data of public interest also calls attention to the proper interpretation of this. The amount of the contract cannot be a subject to business secret, the name of the person signing on behalf of the company may not be blocked because it is not personal data to be protected, but data accessible on public interest grounds. Two companies believe to have fulfilled the data request by sending a link pointing to a website, but only certain contractual data were listed on the website. They partially met their disclosure obligations with the data included in the list; this, however, was unacceptable as an answer to the data request. As a result of the investigation, the Authority called upon the companies to fulfil the data request without blocking data of public interest or data accessible on public interest grounds, and at the same time terminated the investigation against Magyar Turisztikai Ügynökség. *(NAIH-998/2022. NAIH-7707/2021, NAIH-7368/2021, NAIH-7367/2021, NAIH-7363/2021)*

III.15. International affairs

Council of Europe Convention on access to official documents (CETS No. 205., promulgated in Hungary by Act CXXXI of 2009) entered into force on 1 December 2020. However, the 10-member independent expert group mandated to monitor the implementation of the Convention (one of whose expert members is NAIH's President) met for the first time in Strasbourg only on 18 November 2022, where they discussed primarily the rules concerning in the procedures of the expert group.

The 13th International Conference of Information Commissioners (ICIC) was held in Puebla (Mexico) in 2023 with the title "*Access to information, participation and inclusion in the digital age*". The most important message of the mutually accepted statement was the joint protection of the autonomy, independence and inviolability of the supervisory authorities.[34]

UNESCO also issued an important statement at the conference organised on the occasion of the International Day of Freedom of Information entitled "*Tashkent Declaration*", in which it calls upon all governmental and non-governmental actors to create and operate a legal, political and institutional environment that ensures the exercise of the right to the freedom of information in accordance with international standards.[35]

III.16. NAIH's freedom of information project

At the end of 2022, the long-term research project that defined the activities of NAIH's freedom of information experts over the past years, in addition to their day-to-day work, was completed. As a general summary, it can be stated that the enforcement of the freedom of information in Hungary shows a rather self-contradictory picture: whereas the Hungarian regulatory system can be regarded as adequate – in some cases outstanding – in an international comparison and the supervisory authorities as well as the agencies for legal remedy carry out their roles appropriately, the research exposed extraordinary deficiencies ("*practice to be vigorously improved*") on the part of controllers in the case of processes affecting compliance with obligations.

34 https://www.informationcommissioners.org/wp-content/uploads/2022/07/Public-Statement_ICIC.pdf

35 https://unesdoc.unesco.org/ark:/48223/pf0000383211?posInSet=1&queryId=c45caa75-e743-402e-be6e-c2320ed7fd24

The way to make freedom of information more effective is not to increase the volume of information available, but to make the information that is actually relevant more accessible and easier to find. Based on their research, the experts recommend the "*smart transparency*" approach rather than the "*widest transparency possible*" and formulated the recommendations largely in accordance with this approach.

The results of the research unambiguously confirm the preliminary assumption that *online publication* is one of the most emphatic instruments in the enforcement of the freedom of information. Hence the reinforcement of proactive publication with guarantees is one of the most important goals as it can powerfully improve the efficacy of the freedom of information in the future. In addition, the research explored some problems that can be traced back to legal regulation, which can be remedied by legislation or by amending legal regulations.

Meeting the requirements related to the freedom of information would be better encouraged by rendering *effective controlling and sanctioning possibilities* applicable. Soft and hard legal consequences, particularly through sanctioning the infringement of publication obligations, contribute to the compliant behaviour and the orientation of organisations subject to disclosure obligations.

In fulfilling individual data requests, it is important to require both actors *to cooperate* and to introduce a *reasonability limit* to be interpreted stricto sensu against clearly excessive manifestations that are disproportionately burdensome. In addition, an attitude stemming from internal conviction is also important, for which the *self-evaluation toolkit* can be useful. However, as long as the *general cultural medium* fails to move towards the importance of transparency, neither of the actors can be expected to make substantial advances in this field. The circle of citizens who make use of their rights related to the freedom of information is very narrow - i.e. there is no general interest on the part of citizens in data of public interest or data accessible on public interest grounds in relation to the operation and activities of organs performing public duties. For the better enforcement of the freedom of information as a fundamental right, substantial changes are needed on the part of both those requesting data and those controlling them: *in the case of citizens, primarily by improving their awareness of their rights, while on the part of the controllers by improving their attitude and commitment.* For this, external support with assistance from the supervisory agency seems to be indispensable. In order to change attitudes, it is recommended that information on the freedom of information should be included in public education.

Independent statements can also be made for certain target groups of priority studies. In the case of *the target group of municipalities*, the research results clearly show that the majority of municipalities fails to appropriately meet their obligations of providing information and transparency as set forth in the Privacy Act either in terms of electronic publication or meeting requests for data of public interest, whereas the municipalities/mayor's offices, where trained and experienced persons are employed in charge of informational rights, perform much better. The existence and especially the quality of websites is clearly correlated to the size of the settlement. Only 47% of municipal websites have search engines (this would greatly assist in the implementation of the freedom of information) and, all in all, only 17% of the websites can be said to be of good standard. In the course of the test data requests, 41% of the municipalities did not answer a single question, while an additional 10% unlawfully rejected every single question. The Guidelines for Municipalities issued is recommended expressly to this target group.

In relation to electronic publication *by the organs of central public administration*, it can be said that all in all in a third of the entire sample, the websites under study did not comply with the requirements of the legal regulation and the conditions of the detailed study. It is recommended to review Government Decree 305/2005. (XII. 25.) establishing the detailed rules of meeting publication obligations and the detailed rules of the electronic publication of data of public interest, the integrated system for querying public data, the data content of the central list and data integration, as well as IHM Decree 18/2005. (XII. 27.) on the publication samples needed for the publication of data in the publication schemes, particularly with regard to the format and location of publication: i.e. what should be shown in what format/structure/template and where they should be shown on a website. The Uniform Public Data Retrieval System (www.kozadat.hu) in its current form fails to fulfil its function: its operation is difficult to understand and manage for controllers; the omissions are not penalised, they remain without consequences, hence the accessible data content is deficient and its quality is unreliable. Furthermore, it would be necessary to create a central governmental website with a view to the better enforcement of the freedom of information. The majority of data subjects would support the creation of such a public central website for monitoring the use of domestic budgetary funds.

In the case of the target group outside the public administration but performing public functions and/or managing public funds, it is the subjects belonging to this "mixed" target group (especially state-owned and municipally-owned companies, public foundations, other non-profit organisations with a state or municipal background, public bodies and higher education institutions) who, according to the research results, are the least compliant.

Based on research results, the least compliant behaviour was exhibited by the *target group outside public administration, but discharging public tasks and/or managing public funds* (a "mixed" target group, primarily business organisation held by the state or municipalities, public foundations, other non-profit organisations backed by the state or municipalities, public bodies and institutions of higher education). In the case of foundations backed by the state or municipalities, the ratio of those absolutely failing to meet their publication obligation is extremely high (95%). Only 2% of these organisations fulfilled the test data request in full, while 58% of these organisations did not respond at all. An absence of endeavour for transparency is unambiguous, which may be attributed to issues of attitude, but perhaps even more so, to a lack of knowledge. In addition, according to the legal entities in this target group, the separation of commercial and non-commercial activities causes difficulties in the context of business secrets in the case of publicly owned business organisations, primarily those held by the state. As the main problem here is the (self-)identification of obligees, the Guidelines "Adatvédelmi kisokos: ki tartozik az infotörvény hatálya alá?" (Data protection smart guide: who is subject to the Privacy Act?) is recommended expressly for this target group.

Detailed information on the project and its outputs (guidelines, municipal indexation, etc) is available on the new freedom of information portal at infoszab.naih.hu.

IV. Cases of litigation for the Authority

In 2022, the Authority had altogether 34 closed cases of litigation at the Budapest Court of Appeal or at the Curia.

Of this, the Authority won 19 cases in full, it was overwhelmingly successful in 3 litigations, the court rejected the petition in 4 litigations, 4 lawsuits were terminated and the Authority lost litigation in 4 cases only.

Based on the Authority's experiences with litigation, it can be stated that the emphasis of litigation shifted towards administrative lawsuits following data protection procedures launched upon request.

Below, we highlight the more interesting cases fundamentally affecting a wider range of data subjects.

IV.1. Failure to take data security measures proportionate to the risks of transferring health-related data

The Authority received a notification in the public interest from the e-mail address of a private individual, to which the notifier attached an e-mail message forwarded to him and an Excel file that was attached to the e-mail message. The original e-mail and the Excel table attached to the notification in the public interest were sent by the controller to family physicians for adults and family paediatricians. The Excel table attached to the e-mail message contained personal data of patients, their complaints and their test results in 1,153 lines.

Based on the text of the e-mail, the Excel table contained the data of samples taken in relation to diseases related to the Covid-19 pandemic by the organisational unit of the controller. According to the e-mail, in view of the volume of the data sent, the individual notification of the healthcare providers could not be ensured, therefore the sender calls the attention of the physicians originally addressed to handling the data in confidence. The Excel file was not access protected (e.g. by password).

The notification in the public interest contained the Excel file attached to the original e-mail, listing the health-related data. The table contained the personal data of 1,153 data subjects without encryption, accessible to anyone:

– full name of patient,
– address (city, district, street, house number, floor, door, in some cases also the number of the bell at the gate, as well as the name on it),
– mobile and/or landline phone number of the patient,

date of birth,

occupation, in some cases indicating the workplace and qualifications,

– name and address and the number of the seal of the district physician,
– result of the Covid-19 rapid test (positive/negative),
– detailed description of symptoms (e.g. fever, a cough for x days, rise in temperature, vomiting, diarrhoea, shortness of breath, loss of smell and taste, body temperature, description of pains, etc.),
– date of testing accurate to the day,
– comments (e.g. "Business trip to Austria 3 weeks ago", "Work done on an ocean liner: USA, several countries in South America", 'Return from Israel', "Father died in Covid-19 over the weekend", etc.).

In view of the notification in the public interest and the special category personal data in the attached table, the Authority launched an authority audit and thereafter an authority procedure ex officio for data protection as the available data were not sufficient to evaluate whether the controller fully met its obligations under the General Data Protection Regulation, in particularly those in Articles 32-34.

Decision of the Authority

The Authority established in its decision that the controller

- infringed GDPR Article 32(1)(a)-(b) and (2) when it failed to apply data security measures proportionate to the risk of transferring health-related data: it transferred the database containing the exceedingly detailed and accurate health-related and contact data processed in relation to the Covid-19 rapid test in an Excel file without breakdown by districts and without access protection or encryption to safeguard the confidentiality of the data in a simple e-mail to the addressee district physicians. By transferring data this way, the controller directly enabled the onset of a high-risk personal data breach;
- infringed GDPR Article 33(1) when it did not consider it necessary to notify the Authority about a high risk data breach because it had not carried out a proper risk assessment, and finally
- infringed GDPR Article 34(1) when it did not wish to notify the data subjects of this high-risk personal data breach.

The Authority ordered the controller to notify the data subjects of the data breach and its circumstances, the range of personal data involved and the preventive measures taken within 15 days from the decision becoming final.

Because of the established infringements, the Authority imposed a data protection fine of HUF 10,000,000 on the controller.

The petition

The plaintiff submitted a petition against the respondent's decision requesting its annulment. Citing the provisions of Section 61(4) of the Privacy Act and GDPR Article 83(1)-(2), the plaintiff pointed out that according to GDPR Article 83(2)(a) and (c) the examination of the damage caused in the course of the personal data breach is of outstanding importance, in the present case, however, no damage was caused, which the respondent should have taken into account in particular when imposing the fine.

The plaintiff underlined that point (b) of paragraph (2) requires that the intentional or negligent nature of the infringement is taken into account. The plaintiff's decision contains that the controller's behaviour could be attributed to inattentiveness, which is the mildest form of negligence, yet the respondent did not appreciate and specify that the extent of the controller's responsibility was less in the present case than in the category of conscious negligence.

Based on point (d), the degree of responsibility of the controller and of the processor should also be examined, but the respondent examined only the responsibility of the former disregarding the fact that the data breach would not have taken place without the transfer of the data.

Despite the requirement of point (f), a proper evaluation of the degree of cooperation by the plaintiff was omitted, even though according to the decision, it cooperated in full, yet the plaintiff did not take that into account as an explicit mitigating circumstance, nor did it take into account that the plaintiff complied with the requirements of point (j) as well. The plaintiff evaluated the fact that it learned of the data breach by way of a notification in the public interest as an aggravating circumstance, which occurred when transferring the data, hence the plaintiff could not have known about it and so could not have notified the Authority.

In the context of point (k), the fact that the data breach took place during the pandemic that lasted for more than a year in the context of measures taken to combat it and, even according to the position of the respondent, it could be traced back to a non-recurrent scramble and inattentiveness. It was not disputed that the data breach took place because of the omission to sort the data, however, at that time there was an emergency situation pursuant to Government Decree 40/2020. (III.11.) on the promulgation of an emergency situation and the plaintiff omitted to evaluate this circumstance, too. As against this, the respondent considered as an aggravating circumstance that the plaintiff deals with the processing of a large volume of health-related data in general, and therefore it can be expected in particular to process those data in a circumspect manner that is appropriate from a data protection point of view.

The judgment of the Budapest Municipal Court

Taking the above into account, the court had to decide whether the respondent lawfully determined the amount of the data protection fine based on the legal regulations infringed by the plaintiff.

The plaintiff objected to the fact that the respondent failed to fully comply with the provisions of GDPR Article 83(2) because despite the mandatory requirement of the regulation, it failed to examine all the conditions under this provision. In this context, the court stressed that – as correctly cited by the respondent based on Curia judgment Kf.III.37.998/2019/10. – the plaintiff had only to evaluate those provisions of GDPR Article 83(2), which were relevant for the given case. This is also supported by the content of GDPR Article 83(2), according to which "due regard" shall be given to the factors listed in this paragraph. This means that when determining the fine, the respondent does not have to assess factors that have no relevance for the given case. Such a factor missed in the petition was, in addition to others, whether the controller or processor adhered to the codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42 [GDPR Article 83(2)(j)]; in this case, however, not even the plaintiff itself cited the specific code of conduct or certification mechanism, so this legal provision must necessarily have been disregarded in the respondent's assessment.

The court found that the respondent evaluated the absence of damage caused by the plaintiff as an explicitly mitigating circumstance when determining the fine; the plaintiff objected to its omission without grounds. The respondent is not under an obligation to apply additional subcategories among the mitigating circumstances by weighing the factors taken into account in this context.

It was also without grounds that the plaintiff missed the detailed evaluation of inattentiveness as a privileged case of negligence, because the decision expressly refers to the fact that the omission "was related to a non-recurrent transfer of data and a single case of scramble and inattentiveness" which was evaluated among the mitigating circumstances.

The plaintiff's objection, according to which the processor was also responsible for the infringement as the data breach could be attributed to the fact that the Excel table sent by the plaintiff was sent on by the addressees was also inadmissible. As against this, it can be clearly seen from the decision – which was not refuted by the plaintiff in the litigation – that the failure to sort the personal data of the natural persons in the Excel table and the failure to provide separate protection for the table resulted in the data breach in themselves. It also includes the unauthorized disclosure of the stored data, i.e. the facts of the case according to the legal regulation came about by the act of the plaintiff himself. When imposing the fine, the respondent lawfully assessed the plaintiff's conduct independently, because it does not follow from the provisions of GDPR Article 83(2)(d) that the plaintiff should have established the degree of responsibility by the controller and the processor relative to one another.

Judicial practice is well established – and the defendant has rightly argued – that cooperation on the part of the plaintiff cannot in itself be regarded as a mitigating circumstance. As against this, the absence of cooperation would have been an aggravating circumstance to be assessed against the plaintiff. Because of this, the respondent acted lawfully when it considered the cooperative conduct of the plaintiff in the course of the procedure only among the other circumstances.

The argument of the plaintiff according to which the data breach took place during the transfer of the data and therefore the plaintiff could not have known of it under any circumstances was also inaccurate. As described above, the respondent correctly established that the transfer of the data in itself by the plaintiff constituted a data breach, so it lawfully assessed the mode of learning of the incident according to GDPR Article 83(2)(h) among the aggravating circumstances.

As to the plaintiff's argument that the data breach took place during the period of the pandemic in the context of measures taken to combat it, the court pointed out that the personal data of a large number of data subjects (1,153), including special category personal data under GDPR Article 9, were disclosed to unauthorised persons in the Excel table sent by the plaintiff. The lawful assessment of this circumstance as an aggravating factor – also in relation to the fact undisputed by the plaintiff that the processing of large numbers of health-related data is part of the plaintiff's basic activities – makes the plaintiff's arguments concerning the pandemic unfounded. Therefore, it had no significance from the viewpoint of imposing the fine that upon the onset of the data breach, there was an emergency situation because of the new coronavirus pandemic pursuant to Government Decree 40/2020. (III.11.) on the promulgation of an emergency situation.

Citing a decision by the Curia, as well as German and Dutch case law, the plaintiff alleged that the respondent should have applied a weighing system when imposing the fine, on the basis of which the amount of the fine the weights of the aggravating and mitigating circumstances taken into account could have been exactly determined. In this context, however, the plaintiff failed to invoke any legal provision breached by the plaintiff, and there is no binding rule that would require the plaintiff to apply the weighing system according to the plaintiff's objection.

All in all, the court established that the circumstances of imposing the data protection fine could be determined from the decision; the plaintiff in compliance with the governing legal regulations appropriately assessed the circumstances listed in GDPR Article 83(2) as aggravating, mitigating or other circumstances, and lawfully disregarded the provisions not considered relevant.

For these reasons, the court established that the respondent's decision was not as unlawful as stated in the arguments of the petition, therefore it rejected the petition as being unfounded based on Section 88(1)(a) of the Administrative Procedures Act *(Budapest Municipal Court 105.K.706.606/2021/4.)*.

IV.2. Statement of the Curia concerning "rich lists" (Kfv. III.37.978/2021/10.)

In 2022, the Curia brought a judgment on the issue of "press exception". The Curia deemed it necessary to underline that the subject matter of this case was not in general the specification of the legal basis of processing activities by the press, but the examination of the range of the processed data and the lawfulness of processing in particular, in the context of the online and printed publications involved in the litigation ("rich lists") issued by the plaintiff of the first order.

The Curia pointed out that Member State exceptions and derogations for journalistic purposes have not been determined by in Hungarian law and it follows that according to the legislator, exceptions or derogations are not needed to reconcile the right to the protection of personal data with the freedom of information and the right to be informed. To be more accurate, GDPR Article 6(2) was enacted with a view to maintaining the powers of Member States; at the same time, the Hungarian legislator did not introduce more specific provisions for the purposes of compliance with paragraph (1)(e) in order to adjust the application of the rules pertaining to processing to more accurately specify the specific requirements of processing. No separate legal regulation was enacted for specific processing operations by the press and Act CIV of 2010 on the Freedom of the Press and the Fundamental Rules on Media Content (hereinafter: Freedom of the Press Act) was not amended to this end. Hence, Member State legislation did not define what exactly is meant by the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller as set forth in GDPR Article 6(1)(e) as part of the legal basis for processing.

In relation to the legal basis set forth in GDPR Article 6(1)(e), the Curia declared that processing can be regarded as lawful, if it 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. However, compliance with this condition cannot be interpreted in general for press activities; the subject matter of the case is not a general assessment of economic journalism for the purposes of data protection; it is always to be examined in specific terms with regard to individual processing activities, taking into account the purpose of processing. Having assessed all of the specific and unique circumstances, the Curia arrived at the conclusion that the legal basis in question was GDPR Article 6(1)(f) as in the present case processing was not necessary for the performance of a task carried out in the exercise of official authority vested in the controller and it did not constitute a task of public interest. The exercise of official authority according to the second part of GDPR Article 6(1)(e) is directly linked to a regulation, which means that the organisation of official authority is created by legal regulation, it is legal regulation that vests it with the power to act and legal regulation specifies the goals to be attained in the interest of which it performs its activity. This is confirmed by GDPR when it stipulates that processing for the exercise of official authority shall have a legal basis laid down by Union law or Member State law. However, the legal basis of legitimate interest may not be applied for processing carried out by official authorities in the course of performing their duties. Therefore, GDPR Article 6(1)(e) is the legal basis of processing based on the legal provisions stipulating the official duties of the controller.

According to the judgment of the Curia, the so-called rich lists created as a result of the processing operations do not constitute public interest according to the above legislation; they were not made as part of the exercise of the public authority vested in the controller, even though they contained data concerning the use of public funds. Producing a publication that contains a compilation of the largest family undertakings and a list of the richest Hungarians is not an official task; it is not an activity in the public interest. The task of the press is to ensure the fundamental constitutional rights protected by the Fundamental Law and this necessarily entails processing. However, these provisions do not determine the legal basis of processing by the press. According to the Curia, the legitimate interest as a legal basis does not impede or prevent the publication of information, but it guarantees the protection of personal that comes in addition to the right to free expression and the right to be informed.

The Curia established that in this case, the legitimate interest as a legal basis does not constrain the freedom of the press; following an appropriate procedure, the plaintiff of the first order has the opportunity to carry out lawful processing, its activities will not become impossible.

IV.3. The DIGI case before the Court of Justice of the European Union (C-77/21)

The Fővárosi Törvényszék (Budapest Municipal Court) addressed two questions to the Court of Justice of the European Union in the DIGI case, in which the Authority imposed a fine of HUF 100 million on the controller in its decision. First, must a concept of “purpose limitation” as defined in Article 5(1)(b) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (hereinafter: General Data Protection Regulation) Article interpreted to mean that storage by the controller in parallel in another database of personal data, which were otherwise collected and stored for a limited legitimate purpose is still consistent with that concept, or is the limited legitimate purpose of collecting those data no longer valid as far as the parallel database is concerned. Second, the referring court wished to know, should the answer to the first question referred be that the parallel storage of data is in principle incompatible with the principle of “purpose limitation”, whether storage by the controller in parallel in another database of personal data, otherwise collected and stored for a limited legitimate purpose, is

compatible with the principle of “storage limitation” established in GDPR Article 5(1)(e).

The Authority was itself represented in the preliminary ruling procedure. A hearing was held before the Court of Justice of the European Union on 17 January 2022, the motion of the advocate general was presented on 31 March 2022.

The Court of Justice of the European Union announced its judgment in case C-77/21 on 20 October 2022. According to the Court, Article 5(1)(b) of the General Data Protection Regulation must be interpreted as meaning that the principle of “purpose limitation” laid down in that provision does not preclude the recording and storage by the controller in a database created for the purposes of carrying out tests and correcting errors of personal data previously collected and stored in another database, where such further processing is compatible with the specific purposes for which the personal data were initially collected, which must be determined in the light of the criteria in Article 6(4) of that Regulation.

Second, according to the Court, Article 5(1)(e) of the General Data Protection Regulation must be interpreted as meaning that the principle of “storage limitation” laid down in that provision precludes the storage by the controller in a database created for the purposes of carrying out tests and correcting errors of personal data previously collected for other purposes, for longer than is necessary for conducting those tests and the correction of those errors.

IV.4. The Budapest Elektromos Művek Zrt. case before the Court of Justice of the European Union (C-132/21.)

In this case, the Fővárosi Törvényszék turned to the Luxembourg Court basically in a question concerning procedure:

Must Articles 77(1) and 79(1) of Regulation 2016/679 of the European Parliament and of the Council be interpreted as meaning that the administrative appeal provided for in Article 77 constitutes an instrument for the exercise of public rights, whereas the legal action provided for in Article 79 constitutes an instrument for the exercise of private rights? If so, does this support the inference that the supervisory authority, which is responsible for hearing and determining administrative appeals, has priority competence to determine the existence of an infringement? In the event that the data subject – in whose opinion the processing of personal

data relating to him has infringed the General Data Protection Regulation – simultaneously exercises his right to lodge a complaint under Article 77(1) and his right to bring a legal action under Article 79(1) of the General Data Protection Regulation, may an interpretation in accordance with Article 47 of the Charter of Fundamental Rights be regarded as meaning:

a.) that the supervisory authority and the court have an obligation to examine the existence of an infringement independently, and may therefore even arrive at different outcomes; or

b.) that the supervisory authority’s decision takes priority when it comes to the assessment as to whether an infringement has been committed regarding the powers provided for in GDPR Article 51 (1) and those conferred by GDPR Article 58(2)(b) and (d).

The court also asked whether the independence of the supervisory authority ensured by GDPR Articles 51(1) and 52(1) must be interpreted as meaning that that authority when conducting and adjudicating upon complaint proceedings under GDPR Article 77 is independent of whatever ruling may be given by final judgment by the court having jurisdiction under GDPR Article 79 with the result that it may even adopt a different decision in respect of the same alleged infringement.

In this case too, the Authority acted on its own behalf before the Court of Justice of the European Union.

In its judgment brought in case C-132/21, the Court of Justice of the European Union decided that GDPR Articles 77(1), 78(1) and 79(1) read in the light of Article 47 of the Charter must be interpreted as permitting the remedies provided for in GDPR Articles 77(1) and 78(1) on the one hand, and Article 79(1) on the other hand to be exercised concurrently with and independently of each other. It is for the Member States in accordance with the principle of procedural autonomy to lay down detailed rules as regards the relationship between those remedies in order to ensure the effective protection of the rights guaranteed by that Regulation and the consistent and homogeneous application of its provisions, as well as the right to an effective remedy before a court or tribunal as referred to in Article 47 of the Charter.

V. The Authority's legislation-related activities

V.1. The statistical data of cases related to legislation

The number of our positions on legislation by level of legislation

Level of legislation/ year	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
Act	85	49	86	33	79	85	82	72	61	73	77	68
Government decree	75	60	89	63	133	98	89	47	49	52	74	56
Ministerial decree	104	70	92	85	126	83	94	55	41	27	15	16
Government decision	26	12	28	21	61	29	33	40	34	22	14	4
Other (Parliament decision, instruction, etc.)	10	16	15	7	27	20	23	17	29	10	16	19
Total	300	207	310	209	426	315	321	231	214	184	196	163

Statistics on substantive observations in opinions of legal regulations

Nature of observations				*Number of observations*								
	No data for the years 2011-2013			2014	2015	2016	2017	2018	2019	2020	2021	2022
Related to data protection				145	298	461	461	487	323	436	488	311
Related to freedom of information				21	53	28	28	22	39	80	89	40
Other				53	137	92	92	79	78	37	9	26
Total				**219**	**488**	**581**	**581**	**588**	**440**	**553**	**586**	**377**

Pursuant to Section 8 of Act CXXXI of 2010 on Public Participation in Developing Legislation, general consultation is mandatory in every case and the drafts and concepts issued for public consultation must be published on the dedicated website maintained by the government. The summary of the prior impact assessment specified in the Act on Legislation will have to be published together with the draft.

In the Authority's experience, the implementation of this provision did not show any improvement in 2022. The ministries preparing the draft legislation regularly set disproportionately short periods for the Authority to provide an opinion on the draft. Unfortunately, there were several cases when the Government invited the Authority's opinion only after the bill was submitted to Parliament when the possibility of altering the text of the bill is much more limited than prior to submission.

V.2. Cameras for facial recognition in penitentiary institutions

The amendment to Act CVII of 1995 on the Penitentiary Organisation (Bvsztv) allows the penitentiary organisation to process the facial images of its staff members and to use them to determine the lawfulness of measures taken by them, and the identification of perpetrators of violations of the law within the institution by connecting the electronic surveillance device installed in the institution with a facial recognition system (Bvsztv Section 12). In its opinion on this amendment to Bvsztv., the Authority stressed that the draft, on the one hand, does not specify the means of processing, in particular what kind of facial recognition system is involved and who operates it, which renders the person of the controller questionable. On the other hand, it is not clear in what way facial recognition would facilitate proving an infringement perpetrated (no information on this was provided in the justification of this provision). A penitentiary guard who commits an offence can be identified using other means: service assignment roster, route, identifier, badge number and the camera recording the offence. In addition, the use of biometrics does not seem to be necessary and proportionate because typically there are fewer guards than convicts in an institution, hence the number of potential perpetrators is much lower, which eases identification. The Authority called upon the submitting ministry to produce a preliminary impact assessment for data protection to examine the issue of necessity and proportionality in relation to the content of the draft.

This same amendment added a new paragraph (2) to Bvsztv. Section 12, according to which staff members of the penitentiary organisation shall keep as a secret, both during and after their employment therein, personal data, classified data and data qualified as secrets protected by law or data covered by professional secrecy, which they learn in connection with their activities and the performance thereof, as well as all data, facts or circumstances, which the penitentiary organisation is not mandated by legal requirement to make accessible to the public. In relation to this, the Authority supported that the regulation contain a

proportionate ex lege restriction on the accessibility of the data. However, in order for the law to be applied for the original purpose of the legislator and not for other purposes, the Authority underlined that Section 30(5) of the Privacy Act must apply also in this case and the controller should carry out a balancing test prior to fulfilling/rejecting the request. Such a balancing test is required because of the constitutionality of the provision, because if the data request is specifically for data in the case of which public interest to be protected by the legislator does not exist, rejection of the specific data request cannot be constitutional. The balancing test has to be directed at whether the public interest in the security of detention and the maintenance of the order of execution takes priority over the public interest in accessing the data. The Authority would consider it fortunate, if the justification of the draft made a reference to these circumstances. In addition, it should also be noted that this provision does not, and cannot, restrict the exercise of the data subject's data protection rights. Moreover, the amendment does not resolve the issue of the possibility to reject (not normative) data requests for internal instructions, circulars and rules of the penitentiary institution only to a limited extent. The purpose of data requests is precisely to enable calling the penitentiary institution to account for compliance with measures and instructions, for which access to their content is indispensable. *(NAIH-8054/2022.)*

V.3. Amendment to the Privacy Act

With a view to arriving at an agreement with the European Commission, several new legal institutions were added to the Privacy Act in 2022. The first such institution is the Central Informational Public Data Register. This is an interface where budgetary organs – with the exception of national security organs – disclose certain data concerning their financial management, the data on budgetary aid provided by them, the data of contracts and payments for reasons other than the discharge of their basic tasks as listed in the Privacy Act. The data disclosed can be queried, extracts can be made from them, they are comparable, they can be sorted and downloaded by groups and they must be accessible on the interface for ten years. In relation to this – when failing to comply with disclosure obligations – a new type of procedure under the Privacy Act is the authority procedure for transparency. The rules of general administrative procedures shall apply to this procedure; the period open for administering the case is forty-five days. In the event that failure to comply with the disclosure obligation is established, the Authority may impose a fine taking all the circumstance into account, ranging from a hundred thousand forints to fifty million forints.

The provisions of the Privacy Act concerning lawsuits that may be initiated in relation to requests to access data of public interest were also amended, with regard to which the rules of civil procedures shall apply with the differences specified in the Privacy Act. The purpose of these new rules of the Privacy Act is to enable the rapid and effective conduct of litigation. *(NAIH-7944/2022., NAIH-8534/2022., NAIH-8879/2022.)*

V.4. Pseudonymised publication

It is important to mention the new paragraph (2) of Section 817/C of Act XC of 2017 on Criminal Procedure. The provision requires that, in the absence of a motion for review, the prosecution or the investigating authority should publish their decisions and the list of case documents for a month with the personal data therein pseudonymised. The place of publication is the website of the prosecution or the investigating authority and any other interface specified by the Government. It must be possible to query the published decision and the list of case documents at least on the basis of the name of the prosecution or investigating authority, the case number, and the date of publication and the description of the criminal offence. *(NAIH-8179/2022.)*

V.5. Open Data Directive

As of 20 December 2022, the amendment to the Act on National Data Assets and the Act on the Reuse of Public Data has been in force; the purpose of the amendment was the transposition of the Open Data Directive – *Directive (EU) 2019/1024 on open data and the reuse of public sector information.* The primary purpose of the new regulatory elements introduced by the Open Data Directive is to promote the data economy of the European Union. In this context, secondary utilisation of the data assets produced and processed by the public sector should be made even more widely available and digitalisation should be used more effectively than ever before to facilitate its implementation.

As a result of the amendment for law harmonisation purposes, the range of data that can be made accessible for reuse was expanded to include the data of research financed by public funds, which have already been published; and those

data of public undertakings in water management, the energy sector, public transport and the postal sector, which relate to the discharge of these sectoral public tasks. New rules apply to the mode and format of the transfer of data and the act designates the main collective categories of public datasets, whose economic and social significance is outstanding (high-value datasets: geo-spatial data, earth observation and environmental data, meteorological data, statistical data, mobility data). Based on the authorisation conferred upon it by the Open Data Directive, the European Commission will define accurately in an implementing act which specific datasets will have to be regarded as high-value datasets within these categories. A high-value dataset defined in the implementing act will have to be made accessible to those requesting them free of charge, in real time and electronically for the purposes of reuse. *(NAIH-7647/2022.)*

V.6. The Authority's recommendation to amend the Privacy Act

The Authority submitted a recommendation to the administrative state secretary of the Prime Minister's Cabinet Office concerning the review of national classified data. Section 38(4)(a) of the Privacy Act authorises the Authority to make recommendations with respect to new laws and to the amendment of laws on the processing of personal data, access to data of public interest and data accessible on public interest grounds.

Pursuant to Section 63(1)-(2) of the Privacy Act, in its decision adopted in authority procedures for the supervision of data classification initiated ex officio or by a court, the Authority shall, in the event of any infringement of the laws on the classification of certain national classified data, require the classifier to modify the level or term of classification of the national classified data in accordance with the law, or to have it declassified, or establish whether the classifier has proceeded in accordance with the laws on the classification of national classified data.

The classifier may contest the decision within sixty days following the date of its communication. The submission of the statement of claim contesting the decision shall have suspensive effect on the entry into force of the decision. If the classifier does not turn to the court within sixty days of the communication of decision, the classification of the national classified data shall cease on the sixty-first day following the communication of the decision, or the level or term of classification shall be modified in accordance with the decision.

According to Section 8(2)-(3) of Act CLV of 2009 on the Protection of Classified Data (Classified Data Protection Act), as a result of the review, the classifier or its legal successor shall maintain the classification of the national classified data within its scope of authority, if the conditions of their classification continue to obtain, or reduce the level of classification or its term, or terminate the classification. Every addressee and their legal successors must be notified of the termination of classification or the modification of the level or term of classification to whom the national classified data were forwarded; however, this applies to the decision made in the course of the review of national classified data within the scope of authority of the classifier and not to the decision made by the Authority in its authority procedure for the supervision of classified data. For this reason, the Authority made a recommendation that an amendment to the Privacy Act should require the notification of every addressee and their legal successor of the termination of classification or the change in the level or term of classification to which the national classified data were forwarded. *(NAIH-7906-2/2022. and NAIH-8643-2/2022.)*

VI. Annexes

VI.1. Statistical data of reports on requests for data of public interest rejected in 2022

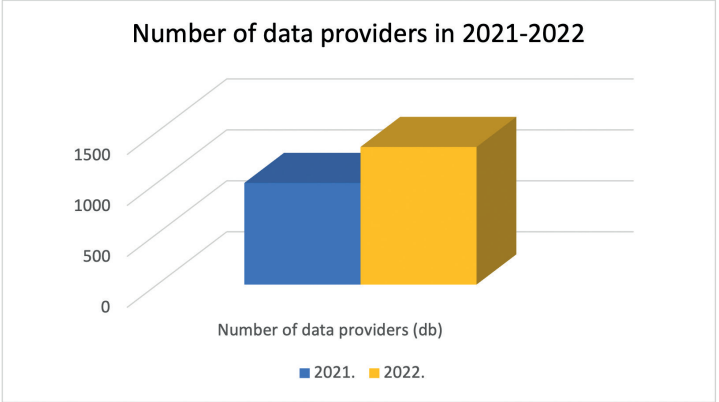
In 2022, NAIH filed 71 case documents as requests for data of public interest, in which the Authority identified 173 requests for data. Of the 173 request for data, 133 were granted, while the Authority refused to issue the data in 40 cases as detailed below.

Reasons for rejection:

- Privacy Act Section 27(1): 12
- Privacy Act Section 27(2)(c): 1
- Privacy Act Section 27(2)(g): 3
- Privacy Act Section 27(5): 1
- not data of public interest: 4
- data not available, no data: 15
- the submission is not a data request: 1
- irregular exercise of right: 3

VI.1.1. General informational data series

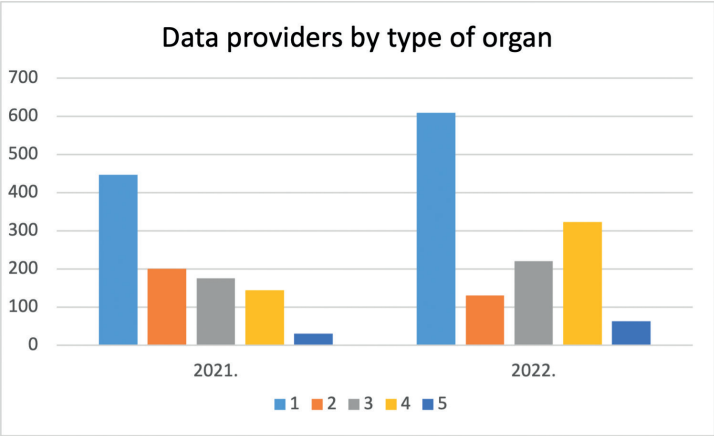
Year	Number of data providers	Number of requests for data of public interest (total)	Granted	%	Refused, partly refused	%
2021	997	11,019	7,127	65%	3,881	35%
2022	1,350	9,739	6,479	67%	3,260	33%



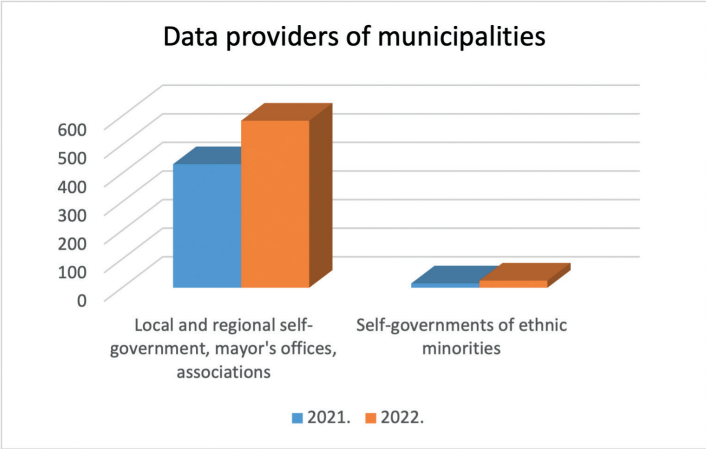
VI.1.2. Distribution of organs meeting the reporting obligation in a breakdown by type of organ

	Type 1[36]	Type 2[37]	Type 3[38]	Type 4[39]	Type 5[40]
2021	447	200	176	144	30
2022	609	130	221	323	63

36 local and regional, self-governments of ethnic minorities
37 central and regional organs of public administration
38 organs mandated to publish outside public administration, public bodies
39 institutions of education and culture
40 healthcare and welfare institutions

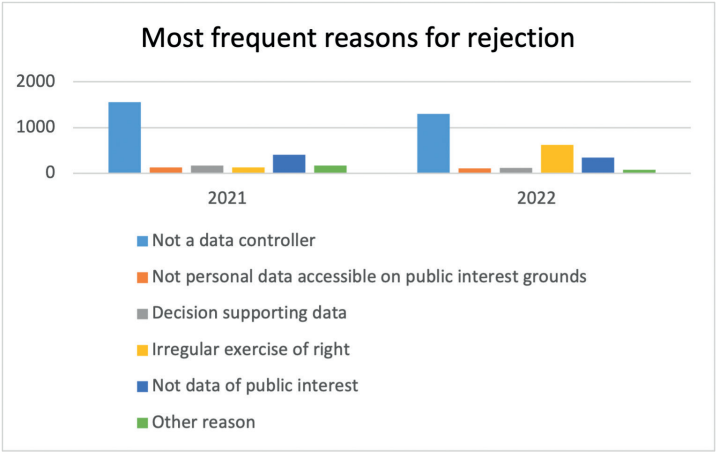


Data providers of municipalities	2021	2022
Local and regional self-governments, mayor's offices, associations	432	584
Self-governments of ethnic minorities	15	25



VI.1.3. Most frequent reasons for rejection

Year	Reasons for rejection (total)	Does not qualify as controller	Not personal data accessible on public interest grounds	Decisions supporting data (Privacy Act Section 27(5)-(6)	Irregular exercise of right	Not data of public interest	Other reason
2021	3,881	1,558	121	164	128	401	167
2022	3,260	1,297	104	114	615	346	70



VI.1.4. Characteristics of the reports on data requests rejected in 2022

The data of Table 1 reveal that the number of those submitting reports increased substantially by 353 new data providers. Despite the positive change, the main data of the report – such as total number of data requests, number of data requests granted and rejected – were lower than in 2021. The possible reason for this may be the large number of negative reports with regard to the submitted data requests.

Outside central public administration, the number of data providers increased in the case of the organ types shown in Table 2. Outstanding differences could be observed in the municipal sectors in the case of business organisations held by municipalities/the state, and education and healthcare/welfare institutions.

The number of rejected data requests declined relative to 2021 and, in line with this, the various reasons for rejection – except for rejection on grounds of irregular exercise of right – were less frequently chosen by data providers. Irregular exercise of rights was cited as a reason for rejection five times more often [128 < 615].

Better compliance with the reporting obligation and the reduction in the rejected data requests can be assessed as a consequence of the priority project KÖFOP-2.2.6-VEKOP-18-2019-00001 “Mapping out the domestic practice of the freedom of information and enhancing its effectiveness in Hungary”.

VI.2. The financial management of the Authority in 2022

The Hungarian National Authority for Data Protection and Freedom of Information closed the 11th year of its operation and financial management as of 31 December 2022. Below, there is a brief presentation of the data related to its financial management.

VI.2.1. Revenue estimate and the data of its performance in 2022

The Authority received and accounted for other aid for operation and accumulation to finance the priority project “Mapping out the domestic practice of the freedom of information and enhancing its effectiveness in Hungary*”.*

Of the revenue data, the operating revenue of the Authority does not show any significant change whether in composition or value relative to the financial year 2021. There was, however, an outstanding item, the reimbursement of the operating costs transferred by KEF to a value of close to HUF 18,602,000, as part of the post-clearance of 2021.

The accumulation revenue of the Authority stemmed from the sale of one official vehicle.

Converting the budget fund remaining from 2021 into a revenue estimate increased the original revenue estimate by HUF 505,806,000.

VI.2.2. Expenditure estimate and the data of its performance in 2022

By providing competitive salaries and creating new dignified working conditions, NAIH was able to reduce the extent of labour fluctuation and successfully retain highly qualified specialists. Expenditure on payment to personnel and related employers’ contributions was only 7.9% higher than last year. The increase was affected by a further rise in the headcount, a minor general pay rise, an increase in the cafeteria allowance up to the legally allowed level subject to the preferential tax rate and another reduction in the rate of the social contribution tax.

In 2022, there were two factors that had a real significance for the budget of the Authority: the cost savings monitored on an ongoing basis and the financing of suppliers stemming from the above-mentioned project. Disregarding the paid expenditures of the project, it can be seen that the value of facility management and maintenance work within the Authority’s material expenses was less than in 2021.

Based on experience from previous years, particular attention was paid to the cost optimisation of individual works. Of the operating expenses, HUF 333.025 million was spent on the project.

On analysing the accumulation expenditure, the Authority rescheduled several works for 2022 for the restoration of the original condition (capacity, accuracy) of the building and value increasing investments, which support the secure and satisfactory operation of the Authority’s basic activities over the long term. These activities were carried out with the permission of Magyar Nemzeti Vagyonkezelő Zrt.

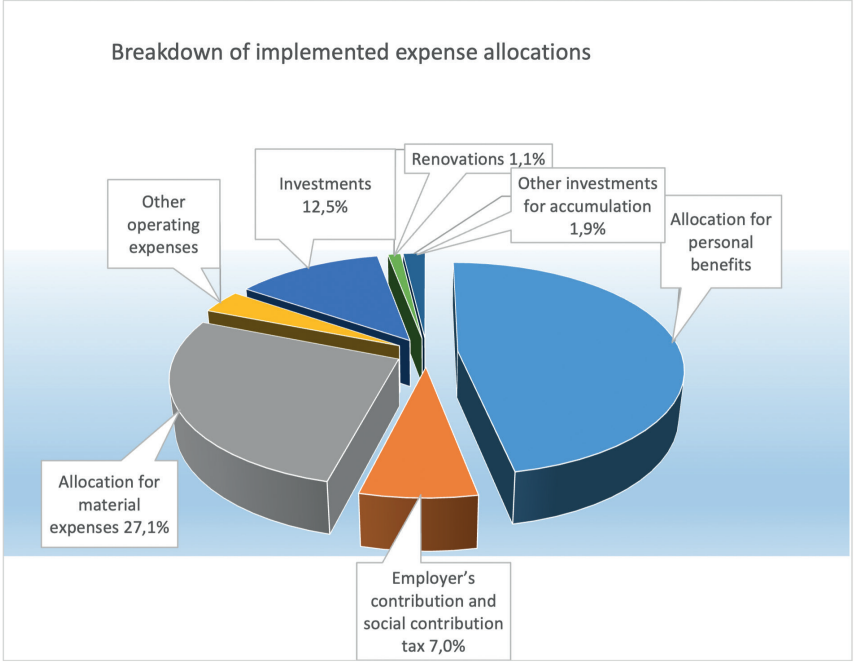
In the early days of January 2022, the Hungarian State Treasury (MÁK) introduced a new multi-currency account management system, because of which the methodology of extraordinary advances on wages (HUF 45,520,000) had to be used at the end of December 2021. In January 2022, MÁK lifted the advance on wages from the Authority’s account.

Funds remaining from the Authority’s budget related to its basic activities in 2022 amounted to HUF 92,976,000, the total amount of which is subject to liabilities.

The following table presents the figures for NAIH'S 2022 budget (in HUF '000):

Description	Original estimate	Amended estimate	Performance	Residue from basic activities in 2022
Operational other support from chapter		246,793	246,793	
Cumulation other support from chapter		161,759	161,759	
Receipts acting as Authority		3	3	
Value for mediated services		1,933	1,933	
Invoiced VAT		3,508	3,508	
Exchange rate gain		216	216	
Damages paid by insurer		629	629	
Other operational revenues		22,638	22,638	
Sale of tangible assets		11,024	11,024	
Recovery of loan for non-operational purposes		1,629	1,629	
Funds remaining from the 2021 budget		505,806	505,806	
Grant from central budget from Managing Authority	1,555,600	1,558,285	1,558,285	
Revenue estimates total:	***1,555,600***	***2,514,223***	***2,514,223***	-
Estimates for payments to personnel	1,030,800	1,135,838	1,135,838	-
Employers' contribution and welfare contribution tax	163,100	170,238	170,238	-
Estimate for material expenses	361,700	737,974	655,120	82,854
Other operational expenses		89,791	86,056	3,735
Investment		308,563	302,176	6,387
Renovations		26,299	26,299	-
Other non-operational expenditure		45,520	45,520	-
Financing expenses	***1,555,600***	***2,514,223***	***2,421,247***	***92,976***

The following graph shows the actual expenditures of the modified estimates in a percentage distribution:



VI.2.3. Changes in the headcount of the Authority

As of 31 December 2022, the Authority's headcount according to labour law was 115.

Human resource management is based on positions according to the Act on Organs of Special Legal Standing, namely, the Authority has five administrative (councillor, lead councillor, main councillor I, main councillor II, head main councillor), and two managerial (one heading an independent organisational unit and one heading a non-independent organisational unit) job categories. With salaries becoming competitive since the introduction of the Act on Organs of Special Legal Standing, fluctuation declined: during the year, 9 people left the Authority and 20 new colleagues entered. In 2022, 11 people were on long-term leave, and 2 returned from long-term leave.

VI.2.4. Changes in revenues from fines

The amount of the fines paid to the Authority's account totalled HUF 387.272 million, a record amount relative to the average of preceding years. It should, however, be noted that receipts from fines constitute the revenues of the central budget, not of the Authority.

VI.3. Participation of the President of the Authority in Hungarian and international conferences and events of the profession in 2022

February 24 2022 – Budapest – "Deloitte Data Protection and Technology 2022" conference – "*Evaluation of 2021 at NAIH"*

28 February 2022 – Budapest – Adatvédelmi.hu conference - "*NAIH's activities – experiences of the past 10 years and 2021"*

22 March 2022 – Budapest – National Public Service University Ludovika Free University programme series – "*Data protection and freedom of information in the 21st century"*

23 March 2022 – Budapest – Péter Pázmány Catholic University Faculty of Law and Political Sciences, Student Government event: Facebook vs EU, or is Facebook leaving Europe? – *"Is Facebook leaving Europe?"*

May 4 2022 – Budapest – Conference inaugurating the project "*Mapping out the domestic practice of the freedom of information and enhancing its effectiveness in Hungary*" - opening address

23 May 2022 – Budapest – Légtér Klub - Studio discussion *"Drone data protection*"

25 May 2022 – Budapest – Constitutional Protection Office – conference "Economic security and information protection – The dangers of social media and its preventative protection" – *"Who guards the guards?"*

5 June 2022 – Budapest – Magyar Jogász Egylet semi-annual closing studio discussion *"The public figure and accessibility"* – round-table discussion

27 September 2022 – Budapest – International Child Rescue Service – conference "The impact of the media and the internet on children and the young" – "*NAIH's role in child protection"*

30 September 2022 – Veszprém – Conference "*Data protection in education*" hosted by the Department of Pedagogy of the Archiepiscopal College of Veszprém *"Data protection and freedom of information in public education"*

5 October 2022 – Budapest – Conference "2022 GDPR PRACTICE" - Current issues presented by the Hungarian National Authority for Data Protection and Freedom of Information and other renowned experts" – "*NAIH's activities - Current issues 2022*" hosted by Adatvédelmi.hu

12 October 2022 – Budapest – 1st National Regulatory Conference hosted by the Supervisory Authority of Regulated Activities – Panel discussion: *"Digital sovereignty – Shall we have an embassy in metaverse?"*

4 November 2022 – Debrecen – Scientific conference of HTE EIVOK, HTE Debrecen and the IT Department of the University of Debrecen – *"Tasks of the Hungarian National Authority for Data Protection and Freedom of Information, interesting cases from the recent past"*

10 November 2022 – Budapest – Hosted by Ernst & Young Tanácsadó Kft. "IT breaches – straight path to GDPR fines? Conference "Authority procedures for data protection from the viewpoint of the types of data breaches with case studies" –*"Personal data breaches"*

8 December 2022 – Budapest – Hosted by NAIH "DPO Conference 2022" – *"Current issues – 2022"*

13 December 2022 – Budapest – National Police Headquarters – annual data protection conference – *"Novelties concerning informational rights"*

14 December 2022 – Budapest – Closing conference of the project *"Mapping out the domestic practice of the freedom of information and enhancing its effectiveness in Hungary"* - opening address

VI.4. Recipients of the NAIH medallion

Based on NAIH's Rule 19/2012 on the Donation of the "*Medallion of the National Data Protection and Freedom of information Authority*", this medallion can be donated to whoever has reached high-level, exemplary achievements in the field of data protection, the right to informational self-determination and the freedom of information or has substantially contributed to the achievement of such results. The medallion, made of silver, is the work of goldsmith Tamás Szabó. It is donated annually on the occasion of the Day of Data Protection and Freedom of Information.

On the occasion of the "Human Rights Day", 10 December 2022, the silver medallion was donated to *Dr. Urszula Góral*, the data protection officer of *Sejm,* the Polish Parliament, in recognition of her fifteen years of work for the Polish Data Protection Authority. The recipient of the medallion has great merit in deepening professional relations between the Polish Data Protection Authority and the Hungarian National Authority for Data Protection and Freedom of Information, facilitating international as well as regional cooperation, and her outstanding activities in mutually presenting the practical experiences of supervision.

VI.5. List of legislation abbreviations mentioned in the report

- Data Governance Act: Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and the amendment of Regulation (EU) 2018/1724
- Ákr., General Administrative Procedure Act, Act CL of 2016 on General Administrative Procedure
- Fundamental Law of Hungary (25 April 2011)
- General Data Protection Regulation: see: GDPR
- BBtv., Act XXIX of 2020 promulgating the Convention on the rebuilding investment of the Budapest-Belgrade railway line
- BCR: Binding Corporate Rules
- BRFK: Budapest Police Headquarters
- Be., Criminal Procedures Act, Act XC of 2017 on Criminal Procedure
- Bv. Institute: penitentiary
- BVOP: National Command of the Prison Service
- Bvsztv., Act CVII of 1995 on the Penitentiary Organisation
- Bvtv. - Act CCXL of 2013 on the Enforcement of Sentences, Measures, Certain Coercive Measures and Detention for Misdemeanours
- Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and on the free movement of such data and repealing Council Framework Decision 2008/977/JHA
- Charter: European Union Charter of Fundamental Rights
- CIS: Customs Information System
- CSC: Coordinated Supervision Committee (carrying out the joint supervision of the large information systems of the European Union)
- DMA: Digital Markets Act, Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828
- DSA: Digital Services Act, Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a single market for digital services and amending Directive 2000/31/EC
- EEA: European Economic Area
- ECB: Europol Cooperation Board

- ECRIS-TCN: centralised system for the identification of Member States having information on judgments against third country nationals and stateless persons
- EDPB: European Data Protection Board
- EDPS: European Data Protection Supervisor
- EES: European Entry/Exit System
- EESZT: Healthcare Service Space
- EHÖK: Student Self-Government
- EIDAS: Regulation (EU) 910/2014/EU of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
- EMMI: Ministry of Human Resources
- EPPO: European Public Prosecutor's Office
- EPRIS: European Police Records Index System
- ETIAS: European Travel Information and Authorization System
- CJEU: Court of Justice of the European Union
- Eüaktv., Health Data Act, Act XLVII of 1997 on the Processing and Protection of Health and Related Personal Data
- Eüsztv., Act CCXXII of 2015 on the General Rules for Electronic Administration and Trust Services
- Eütv., Act CLIV of 1997 on Healthcare
- FIR: Higher Education Information System
- FÖRI: Policing Directorate of the Municipality of Budapest
- 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. To be applied from 25 May 2018
- IIOF: International Intelligence Oversight Forum
- IKSZR: Integrated Traffic Management and Regulatory System
- IMI system: Internal Market Information System
- Privacy Act, Act CXII of 2011 on the Right of Informational Self-Determination and the Freedom of Information
- IRMA: specialised internal administrative system
- ITM: Ministry of Innovation and Technology
- KAK: Governmental Data Centre
- Kbt., Public Procurement Act, Act CXLIII of 2015 on Public Procurement
- Cost Decree, Government Decree 301/2016. (IX. 30.) on the extent of cost reimbursement to be set for granting requests for data in the public interest
- Kgttv., Act CXXII of 2009 on the More Economical Operation of Business Organisations in Public Ownership

- Kiberbiztonsági Jogszabály, Cybersecurity Act, Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cyber Security) and on information and communications technologies cyber security certification and repealing Regulation (EU) 526/2013
- KIRA: centralised paybill system
- KKMI: Central Institute of Examination and Methodology
- Knyt., Act CLXXXI of 2007 on the Transparency on public grants from public funds
- KSH: Hungarian Central Statistical Office
- MÁK: Hungarian State Treasury
- Mavtv-. Classified Data Act, Act CLV of 2009 on the Protection of Classified Data
- Mötv., Municipalities Act, Act CLXXXIX of 2011 on Hungary's Municipalities
- NEAK: National Health Insurance Fund Manager
- Nektv., Act CLXXIX of 2011 on the Rights of Ethnic Minorities
- NNK: National Public Health Centre
- Open Data Directive: Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the reuse of public sector information
- NVR: National Election System
- OGYSZ: National Child Protection Service
- OH: Office of Education
- OKFŐ: National Directorate General for Hospitals
- OSZIR National Professional Information System for Epidemiology
- OVF: General Directorate of Water Management
- Prüm decision, Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of crossborder cooperation, particularly in combating terrorism and crossborder crime
- PSZ: Teachers' Trade Union
- Rtv., Act XXXIV of 1994 on the Police
- Ptk., Civil Code, Act V of 2013 on the Civil Code
- 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
- Smtv., Press Act, Act CIV of 2010 on the Freedom of the Press and the Fundamental Rules of Media Content
- Támtv., Agri Aid Act, Act XVII of 2007 on Certain Issues of the Procedure Related to Agri and Rural Development and Fishing Grants and Certain Measures

- Tromsø Convention, Council of Europe Convention on access to official documents (CETS No. 205., promulgated in Hungary by Act CXXXI of 2009)
- Ve., Election Procedure Act, Act XXXVI of 2013 on the Election Procedure
- VIS: Visa Information System
- 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
- VJT: boards with alternating signals

Other legal regulations:
- Decree 1/2014. (I. 16.) EMMI on the order of reporting infectious diseases
- Act CLV of 1997 on Consumer Protection
- Act LXIII of 2012 on the Reuse of Public Data
- Decree 7/2013. (II.26.) NFM on organisations using centralised IT and electronic communication services based on individual service agreements and IT system operated or developed by the central service provider
- Act LXIII of 1999 on the Supervision of Public Areas
- Government Decree 90/2010. (III.26.) on the order of processing classified data
- National Security Services Act, Act CXXV of 1995 on National Security Services
- Government Decree 229/2012 (VIII. 28.) on the implementation of the Act on National Public Education
- Government Decree 311/2005 (XII. 25.) on the order of public access to environmental information
- Government Decree 382/2022 (X. 10.) on the amendment of Government Decree 301/2016. (IX. 30.) on the extent of cost reimbursement to be set for granting requests for data of public interest (Cost Decree)
- Government Decree 499/2022 (XII. 8.) on the detailed rules of the Central Information Public Data Register
- Government Decree 521/2020. (XI. 25.) on derogation from certain data request provisions at times of emergency
- Decree 20/2019. (VII. 30.) IM on the detailed rules of the implementation of the tasks within the scope of authority of election offices and the forms to be used in the election procedure at the elections of municipal representatives and mayors and the representatives of ethnic minority self-governments
- Act CXXXI of 2010 on Public Participation in the Development of Legislation
- Government Decree 314/2005 (XII.25) on the procedures for environmental impact assessment and the IPPC permit

- Decree 17/2013 (VII. 17.) KIM on keeping the central register on voters and other electoral registers
- Act XCI of 2021 on national data assets
- Act LXVI of 1992 on the Registration of the Personal Data and Addresses of Citizens
- Decree 16/2014 IM on the detailed rules of the enforcement of imprisonment, detention, pre-trial custody and detention in lieu of a fine
- Council Regulation (EU) 2022/922 of 9 June 2022 on the establishment and operation of an evaluation and monitoring mechanism to verify the application of the Schengen acquis and repealing Regulation 1053/2013
- Act CLVI of 2016 on the State Tasks of Developing Touristic Regions
- Government Decree 94/2022 (III. 10.) on derogations from the application of Act CXXX of 2021 on Certain Regulatory Issues in the Context of Emergency Situations
- Government Decree 40/2020. (III.11.) on the announcement of an emergency
- Act LXXXI of 2001 on the Promulgation of the Aarhus Convention
- Act C of 2020 on the Legal Relationship of Healthcare Service
- Act XLVII of 1997 on the Processing and Protection of Health and Related Personal Data
- Act LXXXIV of 2003 on Certain Issues of Performing Healthcare Activities
- Act CLIV of 1997 on Healthcare
- Act CXII of 2009 on the More Economical Operation of Business Organisations in Public Ownership
- Decree 44/2004 (IV.28.) ESzCsM on the prescription and issue of medication for human use
- Government Decision 1538/2018 (X. 30.) on the establishment of a working group coordinating government measures necessary for the development of the European Entry/Exist System (EES) and the European Travel Information and Authorization System (ETIAS)
- Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC
- Act XXVIII of 2022 on the Audit of the Use of European Union Budgetary Funds
- Government Decree 333/2021 (VI. 10.) on the detailed rules for certain pandemic evaluation registers for epidemic control
- Act LIV of 2018 on the Protection of Trade Secrets

Table of Contents

Nemzeti Adatvédelmi és
Információszabadság Hatóság

1055 Budapest, Falk Miksa utca 9-11.
Postal address: 1363 Budapest, Pf. 9.

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)

Nemzeti Adatvédelmi és Információszabadság Hatóság

1055 Budapest, Falk Miksa utca 9-11.
Postal address: 1363 Budapest, Pf. 9.

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

**Published: a 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)**