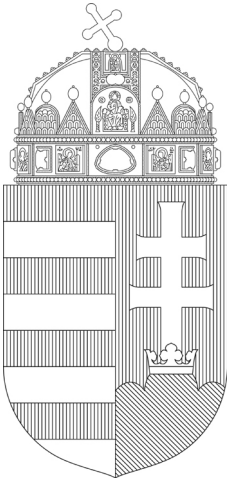
National Authority
for Data Protection
and Freedom of Information


# ANNUAL REPORT OF THE HUNGARIAN NATIONAL AUTHORITY FOR DATA PROTECTION AND FREEDOM OF INFORMATION (NAIH) 2024

# Report of the Hungarian National Authority for Data Protection and Freedom of Information on its activities in 2024

B/10548

Hungarian National Authority for Data Protection and Freedom of Information
Budapest, 2025.



# Introduction

*Greetings Dear Reader*

In the seventh year of applying the General Data Protection Regulation, we see that the Hungarian Data Protection Authority has to respond to increasingly complex data protection issues and the same is noted in the activities of the courts in applying the law. The increase in the number of lawsuits for the court review of the Authority's administrative decisions was a clear-cut tendency until 2023, obviously related also to the increasing amounts of the fines levied by the Authority. In 2022, the Authority had altogether 34 closed lawsuits before the Budapest Municipal Court and the Curia, of which the Authority won 22 cases in terms of the merits of the case. In 2023, the number of closed cases rose to 47, of which the Authority won 35 cases. These data indicate that the Authority's decisions are more and more aligned with the practices of the courts. I find it encouraging that the trend of increase in the number of court cases to review the Authority's decisions came to a halt in 2024. As against the 37 cases launched in 2023, altogether 22 cases of litigation were launched in 2024, of which 6 were already closed. We attribute this change in part to the enhanced data protection awareness of controllers, who rather than challenging the Authority's decisions preferred to comply with them; this also points to the greater professional prestige of and respect for the decisions of the Authority.

Artificial intelligence is one of the greatest technological achievements of recent decades, which has radically transformed numerous industries, including health care, finances, logistics and even education. The rise of AI has been accelerated by breakthroughs achieved in machine learning, natural language processing and image recognition, with important areas of applications such as personalised recommendation systems or self-driving cars. As world leaders and researchers attempt to manage the social impacts of AI development, the ethical and regulatory issues of AI move increasingly to the foreground. AI is a key driver of both technological innovation and the future of the global economy, constantly creating new challenges and opportunities. Last year, a number of measures were taken to manage data protection challenges, over and above the GDPR, an AI Act was adopted in the EU in 2024, which is to become applicable in stages; in addition to its existing forensic lab, the Authority began building up a new AI lab with a view to more efficiently monitor and analyse processing operations using AI; furthermore, one of the major themes of the recently adopted 2025 work programme of the European Data Protection Board will also be the AI.

In 2024, making covert sound recordings and the issue of the lawful use of public area space surveillance systems of municipalities commanded a great deal of attention.

The Authority called attention to the negative impacts of making covert sound recordings on the right to informational self-determination and the protection of privacy and the proliferation of this unlawful practice. Pursuant to the General Data Protection Regulation, the voice of a natural person and any recording thereof constitutes the personal data of the data subject and any operation carried out on personal data, such as making, using and publishing sound recordings qualifies as processing. Although the objective scope of the GDPR may in certain cases allow for the making of a sound recording to be considered as "household processing", to which the provisions of the GDPR do not apply, it has stringent conditions. According to the Authority's consistent practice, if the audio recording is made in the context of other activities, even on a stockpiling basis, or is used or disclosed, for example as evidence in judicial or administrative proceedings, this processing falls within the scope of the GDPR and its provisions apply. According to the consistent practice of the Authority, if the sound recording is made in the context of some other activity, even on a stockpiling basis, or if it is used or disclosed, for instance, as evidence in a court or authority procedure, such processing is subject to the objective scope of the GDPR and its provisions shall apply. It follows that the person carrying out any operation with the recording becomes a controller subject to the scope of the GDPR, they will have obligations arising from this, hence they have to ensure the full enforcement of all the principles and provisions concerning the processing and the protection of personal data, and are responsible for the consequences of failure to do so.[1]

Currently, there are several procedures in progress before the Authority, where the public area surveillance system of a municipality is operated by a person other than the one specified by Act LXIII of 1999 on Public Area Supervision – the public area supervision or public area supervisor, in their absence, a civil servant designated by the municipal executive or the body of representatives, employed by the municipality – hence the data protection guarantees set forth by the act are not enforced.

This year, we arrived at an important milestone: the first data protection commissioner was elected in 1995; hence we celebrate the 30th anniversary of the existence of a data protection institution in Hungary in 2025. In order to duly celebrate this jubilee,

1 The full statement can be found here: https://www.naih.hu/tajekoztatok-kozlemenyek?download=975:hatosagi-kozlemeny-a-leplezett-hangfelvetelek-keszitesenek-az-informacios-onrendelkezesi-jogra-es-a-maganszfera-vedelmere-gyakorolt-negativ-hatasairol-jogellenes-gyakorlatanak-elharapozasarol

NAIH organises an international conference in Budapest on 15-16 September 2025 to present and discuss the past, present and future of informational rights.

Budapest, 20 February 2025

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

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

## *I.1. Statistical characteristics of our case*

In line with the goals of the National Digitalisation Strategy (2021-2030), the administrative field of the Authority continues to be committed to increasingly greater digitalisation, enabling paperless operation as much as possible.

The new system commissioned in 2025 is appropriately flexible and scalable, enabling expansion or modification adjusted to the Authority's continuous expansion of tasks, often taking place during the year. This includes weighted cost-effective operation, cost planning and efficient support for internal (human) resource allocation.

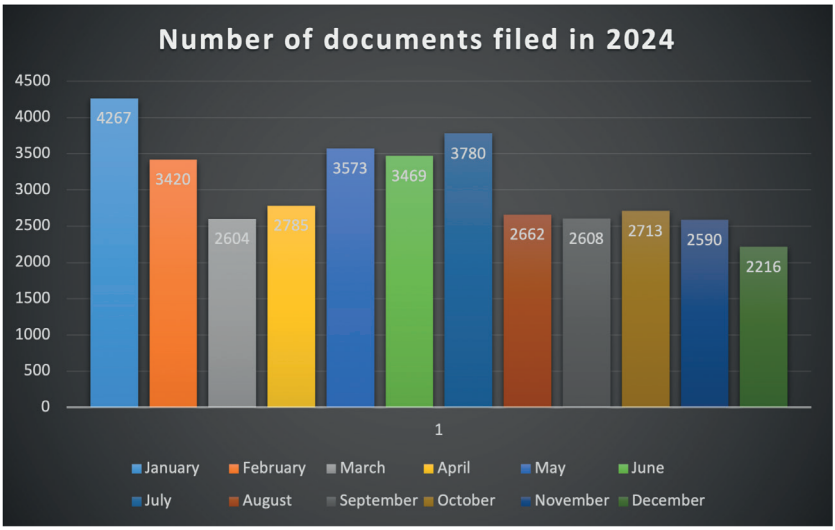
The ongoing modernisation of the Authority's administrative activity aims for the development of a complex, thoughtful and dynamic system that can adjust to the new challenges posed by technological development, providing new opportunities for the improvement of the efficiency of classical authority operation on an ongoing basis.

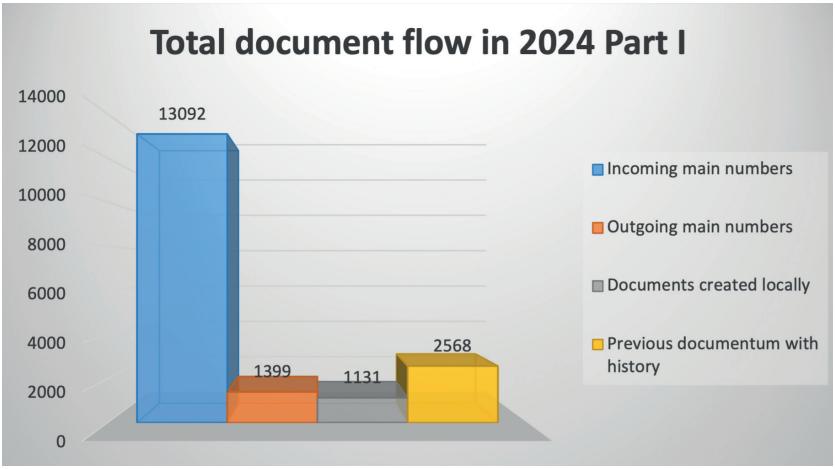
In 2024, 13,054 new cases were filed in the Authority's internal case administration system. Together with cases from earlier years (2,568), altogether 18,190 cases were in progress. The number of cases substantially rose above last year's numbers exceeding them by more than 65% (7,176).

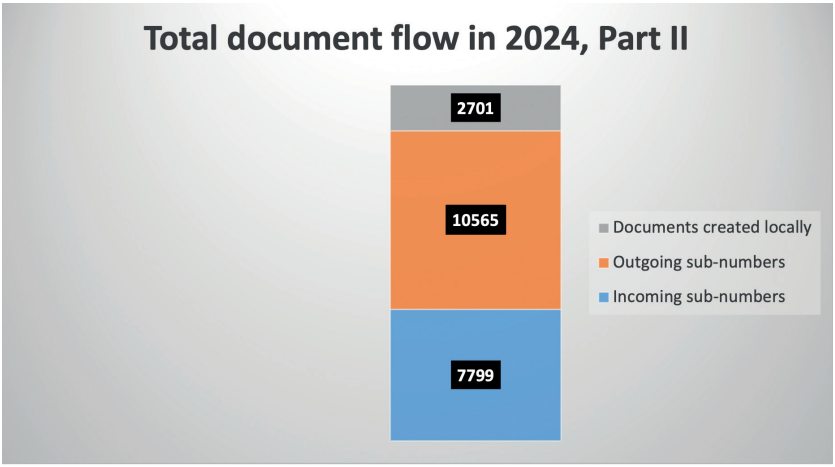
A comparison of the data series reveals that the number of investigative cases increased by close to 25 percent (from 2,894 to 3,561) relative to the preceding year. The ratio of the number of cases related to authority procedures, consultation cases, authority audits and cases related to GDPR cooperation (IMI) was in line with that of the previous year.

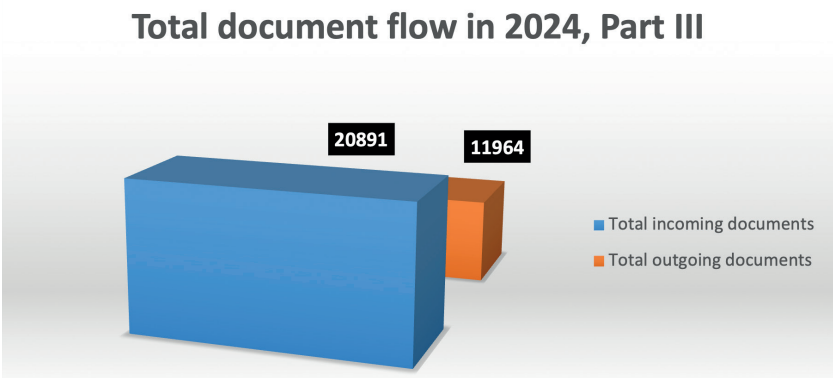
In 2024, the Authority's customer service received 5,802 phone calls, close to the number of calls administered last year. The number of face-to-face client appointments increased to 144. Within this, there were 71 document inspections, which can be requested in administrative authority procedures as against the 55 document inspections in 2023.

**Document statistics of the Authority in 2024**





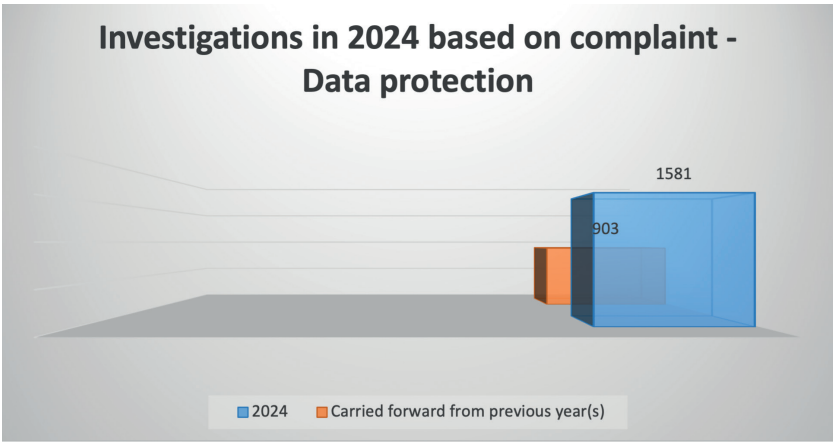

**The Authority's case types of the most significant case numbers in 2024:**

| | |
|---|---|
| Authority cases | **1069** |
| Investigative procedures | **3561** |
| Consultative procedures | **1390** |
| Authority investigation | **587** |
| Providing opinion on legal regulations | **176** |
| GDPR cooperation(IMI) | **1736** |

## Investigative procedures in 2024 – Data protection

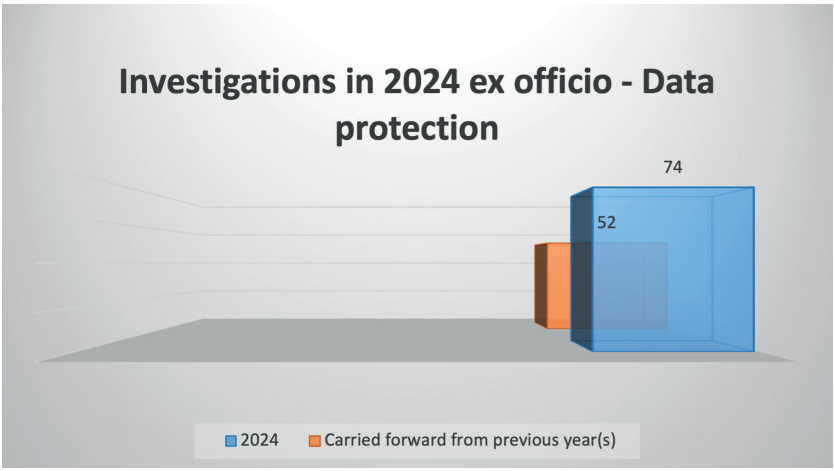
**Investigated cases based on complaints in 2024:**

| 2024 | **1581** |
|---|---|
| Carried over from previous year(s) | **903** |




**Investigated cases ex officio in 2024:**

| 2024 | **74** |
|---|---|
| Carried over from previous year(s) | **52** |



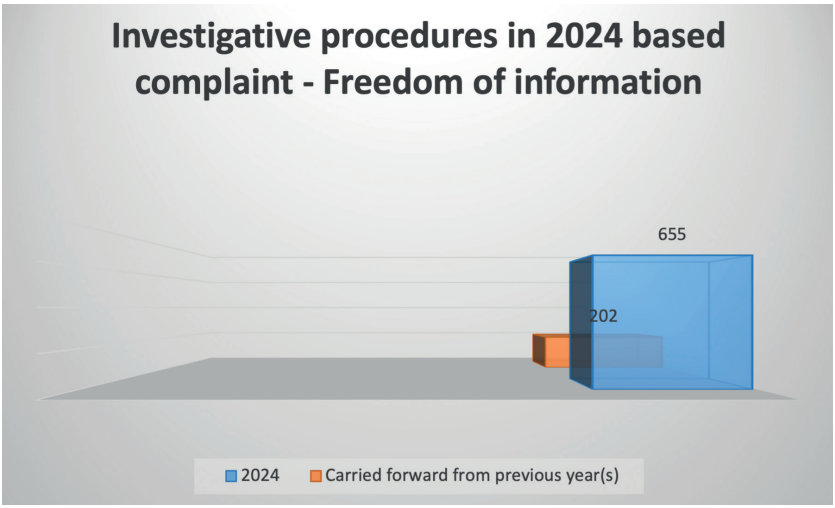
**Data protection investigative procedures in 2024 per case type**

| Case type | Total | Carried over from previous years | New cases |
|---|---|---|---|
| **Investigative procedure ex officio** | **126** | **52** | **74** |
| Investigative procedure ex officio in data protection case – Law Enforcement Directive | 21 | 1 | 20 |
| Investigative procedure ex officio in data protection case – GDPR and other | 104 | 51 | 53 |
| Investigative procedure ex officio in data protection case – GDPR and other - data breach | - | - | 1 |
| **Investigative procedure based on complaint** | **2484** | **903** | **1581** |
| Investigative procedure based on complaint in data protection case – data breach | 245 | 67 | 178 |
| Investigative procedure based on complaint in data protection case – Law Enforcement data breach | 5 | 2 | 3 |
| Investigative procedure based on complaint in data protection case – Law Enforcement Directive | 80 | 30 | 50 |
| Investigative procedure based on complaint in data protection case – GDPR and other | 2154 | 804 | 1350 |

## Investigative procedures in 2024 – Freedom of information

**Investigated cases based on complaints in 2024**

| 2024 | **655** |
|---|---|
| Carried over from previous year(s) | **202** |



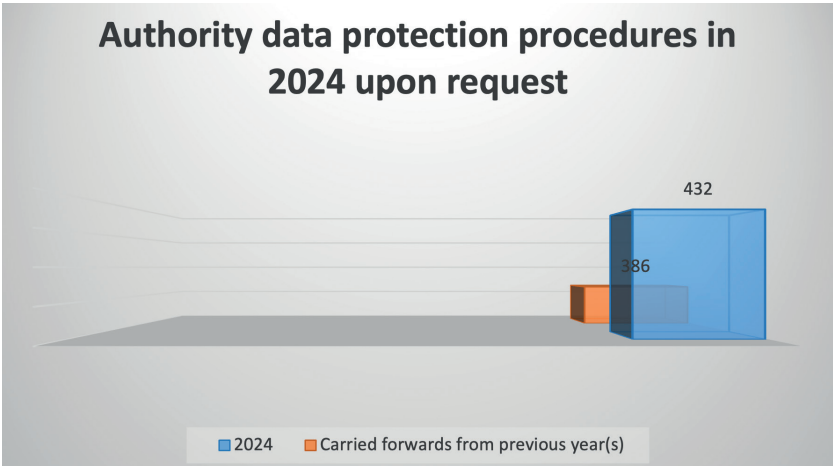

**Investigated cases ex officio in 2024**

| 2024 | **92** |
|---|---|
| Carried over from previous year(s) | **2** |

## Number of the Authority procedures for data protection in 2024

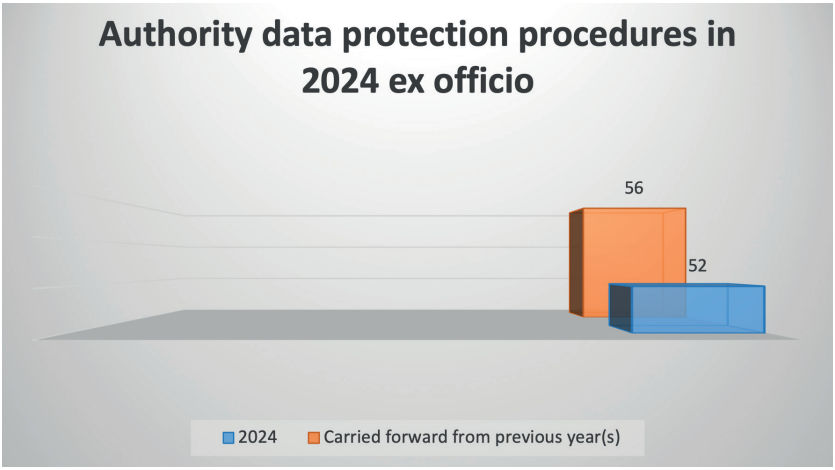
**Number of the Authority procedures for data protection based on petition in 2024**

| 2024 | **432** |
|---|---|
| Carried over from previous year(s) | **386** |




**Number of Authority procedures for data protection ex officio in 2024**

| 2024 | **52** |
|---|---|
| Carried over from previous year(s) | **56** |

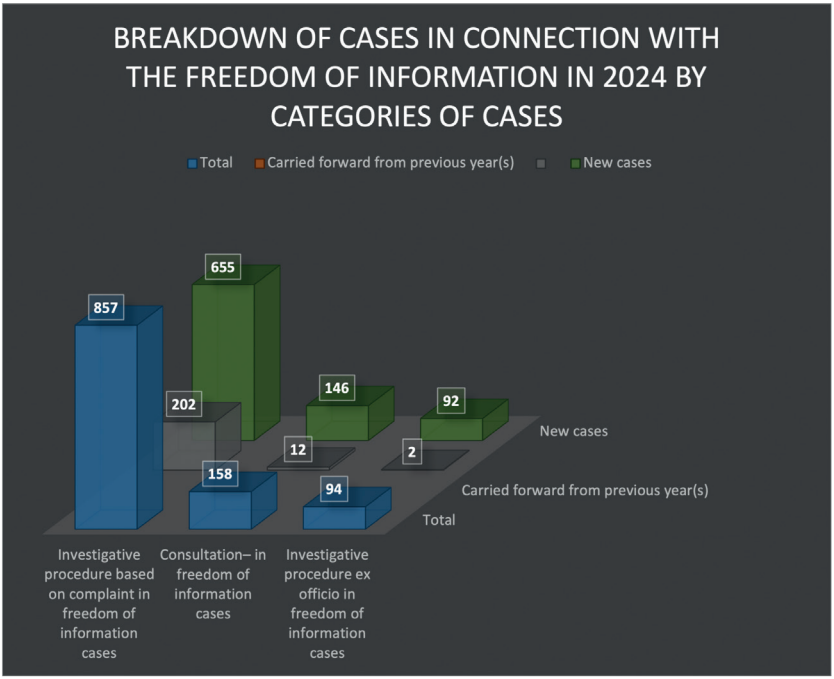


**Authority procedures for data protection per case type in 2024**

| Case type | Total | Carried over from previous years | New cases |
|---|---|---|---|
| **Authority procedures for data protection ex officio** | **108** | **56** | **52** |
| Authority procedures for data protection ex officio – Law Enforcement Directive | 3 | 2 | 1 |
| Authority procedures for data protection ex officio – Law Enforcement Directive - data breach | 2 | - | 2 |
| Authority procedures for data protection ex officio – GDPR and other | 68 | 37 | 31 |
| Authority procedures for data protection ex officio – GDPR and other – data breach | 35 | 17 | 18 |
| Authority procedures for data protection ex officio – GDPR and other – freedom of the press and expression | - | - | - |
| **Authority procedures for data protection based on petition** | **818** | **386** | **432** |
| Authority procedure for data protection based on petition - Law Enforcement Directive | 28 | 12 | 16 |
| Authority procedure for data protection based on petition – Law Enforcement Directive – data breach | 2 | 2 | - |
| Authority procedure for data protection based on petition - GDPR and other | 731 | 346 | 385 |
| Authority procedure for data protection based on petition – GDPR and other – data breach | 55 | 25 | 30 |
| Authority procedure for data protection based on petition – GDPR and other – freedom of the press and expression | 2 | 1 | 1 |

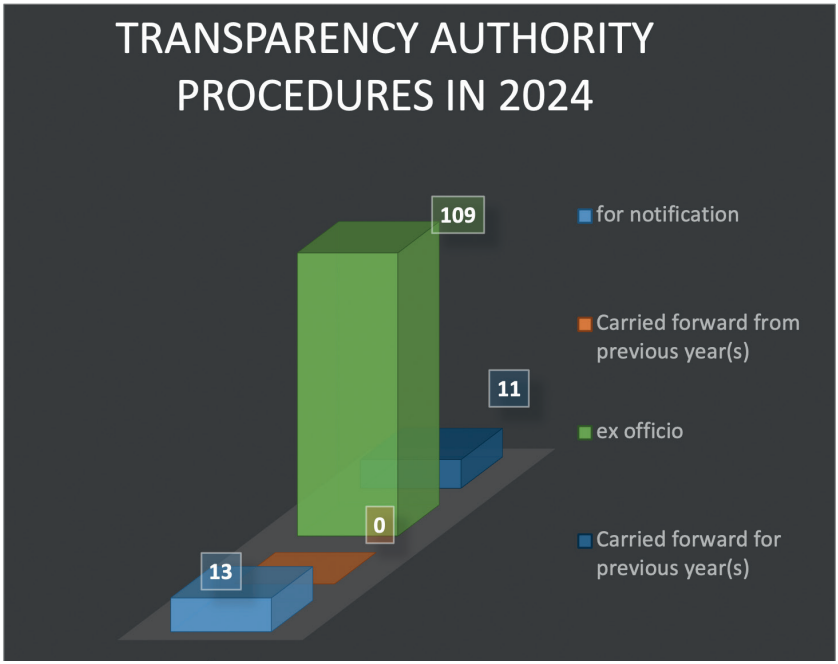
**Distribution of freedom of information cases in 2024 by case type**

| Case type | Total | Carried over from previous years | New cases |
|---|---|---|---|
| Investigative procedure based on complaint concerning freedom of information | **857** | **202** | **655** |
| Consultation – freedom of information | **158** | **12** | **146** |
| Investigative procedure ex officio – freedom of information | **94** | **2** | **92** |



**Changes in the number of authority procedures for transparency in 2024**

| | |
|---|---|
| Ex officio authority procedure for transparency launched upon notification | **13** |
| Ex officio authority procedures for transparency | **120** |




**Changes in authority investigations in 202**

| | |
|---|---|
| Investigations in 2024 | **455** |
| Carried over from previous year(s) | **129** |

| Case type | Total | Carried over from previous years | New cases |
|---|---|---|---|
| Authority investigation for data protection – Law Enforcement Directive | - | - | - |
| Authority investigation for data protection – Law Enforcement Directive – data breach | 28 | 10 | 18 |
| Authority investigation for data protection – GDPR and other | 30 | 6 | 24 |
| Authority investigation for data protection – GDPR and other – data breach | 526 | 113 | 413 |

**Number of opinions on legal regulations in 2024**

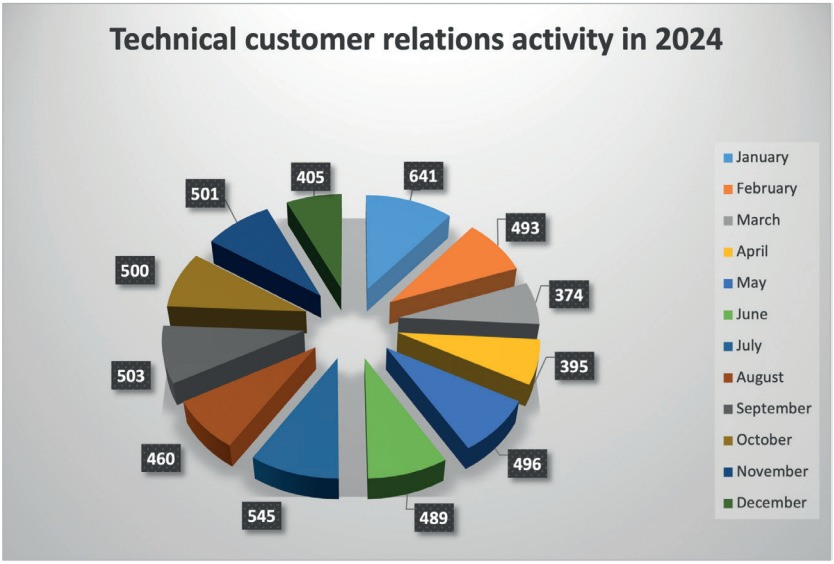
| 2024 | 173 |
|---|---|
| Carried over from previous year | 3 |

| Case type | Total | Carried over from previous year | New cases |
|---|---|---|---|
| Opinions on regulations upon request (opinions and consultation on draft legal regulations) | 172 | 3 | 169 |
| Recommendation for legislation (draft regulation, opinion, own, initiated by those applying the law) | 4 | - | 4 |

**mportant areas of international cooperation in 2024 (GDPR, IMI)**

| | |
|---|---|
| 2024 | **1228** |
| Carried over from previous year | **508** |

| Case type | Total | Carried over from previous year | New cases |
|---|---|---|---|
| Cooperation with other EEA supervisory authority as authority concerned – data breach | **9** | **8** | **1** |
| Cooperation with other EEA supervisory authority as authority concerned GDPR 56, 60, 61, 62, 64, 65 | **1718** | **499** | **1219** |
| Cooperation with other EEA supervisory authority as authority concerned – freedom of the press and expression | **9** | **1** | **8** |



## *I.2. Annual conference of data protection officers*

The Authority held the Annual conference of data protection officers on 3 December 2024, which thanks to the cooperation of MTVA was accessible through the Authority's website online for anyone; the recordings of the presentations were made public in the website of the Authority.

At the beginning of the Conference, **Dr. habil. Attila Péterfalvi**, President, welcomed the participants, presented the speakers and the themes, as well as the main statistics concerning the Authority's activities.

In her presentation, **Dr. Júlia Sziklay**, deputy president for international affairs, presented opinion 08/2024 on the "Pay or O.K." model of outstanding significance among the opinions of the European Data Protection Board published in 2024 and its possible afterlife.

At the 2024 conference, several presentations addressed the issues of data subjects' rights, specifically the issues of ensuring the right to access and its limitations.

**Dr. Gergely Barabás**, the Authority's Bar legal counsel and the head of the Legal Counsel Department, analysed the possibility of inquiring into the motivation and objectives of data subjects when exercising the right to access. The reason for the choice of the theme was that the two Chambers of the Curia (civil and administrative) and the Court of Justice of the European Union have published several decisions on how best to reconcile the enforcement of one of the most fundamental rights of data subjects, the central core of data protection law, with the rising trend that some data subjects do not exercise their rights "properly", i.e. when a data subject's exercise of their rights can be declared excessive or manifestly unfounded.

The controller may have an opinion on why a data subject may wish to make use of their right to access, but the controller still has to facilitate the exercise of the right and any reason for rejection may only be an exception; if the controller wishes to use this, it will be its responsibility to demonstrate its applicability. Failure to respond in the context of the exercise of data subject's rights is unlawful even in such cases. In terms of Recital (63) of the General Data Protection Regulation, the speaker contrasted the decisions of the Curia with the legal practice of the Court of Justice of the European Union highlighting in their justification that there

was no difference in them that the motivation of the data subject could not be investigated, but in the Curia's interpretation, its goal had to be investigated; in contrast to this, the Court of Justice of the European Union does not regard the rejection of a request for the right to access lawful even in the case when the right of access is exercised for a different reason. At the same time, the abuse of the exercise of rights also arises in the practice of the Court of Justice of the European Union: decisions are expected in two other cases awaiting preliminary ruling in the near future.

**Dr. Noémi Nagy-Borsy**, representative of the Data Protection Department, addressed certain issues of the transparency of processing operations by health care providers and the exercise of the right to access in her presentation. A larger percentage of submissions received by the Authority concerned the enforcement of rights related to processing operations in the course of caring for patients and in related areas. She addressed the obligations of controllers arising in the course of providing health care and the rights of patients, i.e. the data subjects of health-related processing in detail. She emphasised that in the case of health-related documentation a request for a copy appears not only a check on the lawfulness of processing, but also as a quasi-patient right. She explained that in the Authority's experiences, larger private healthcare providers generally have Privacy Statements and they also facilitate access to it when concluding contracts; in the case of smaller service providers, however, the provision of information is frequently absent and consequently the enforcement of rights is often impeded.

The presentation by **dr. Dóra Jeszenszky**, the information rights expert of the Data Protection Compliance and Public Relations Department, ended the series of addresses on the enforcement of the right to access, who presented the results of the survey conducted by the Authority as a participant of the European Data Protection Board's Coordinated Enforcement Framework 2024 (CEF).

In her presentation, **Dr. Éva Tóth**, head of the Transparency Authority Department, explained that the amendment to the Privacy Act regulating the transparency of the use of public funds stipulates an obligation for budgetary organs to publish their financial management data in the Central Public Data Information Register. Acting within its powers as authority, the Authority may check the disclosure obligation and even levy a fine of HUF 50,000,000. Currently, this obligation applies to budgetary organs but not to municipalities; it, however, does apply to budgetary organs founded by municipalities. As of 1 January 2025, the legislator also requires treasury registered legal entities, including municipalities and public bodies to publish their data. She also reported on the problematic issues of legal

interpretation in 2024 and presented the experiences of the authority procedures for transparency and clarified the due dates for reporting for the obligees.

**István Csajági**, head of the Department for Freedom of information, spoke about reporting concerning freedom of information to be submitted to the Authority and the related monitoring procedure. He presented the range of data to be reported, the form to be completed for reporting and called attention to the guidelines assisting the completion. As to the monitoring procedure, he mentioned that one of its bases is the reporting obligation referred to. The Authority supervises the practice of the obligee organs concerning compliance with individual data requests and the publication of data of public interest.

**Dr. Dániel Eszteri**, head of the Department for Data Breach Notification and Forensic Analysis, presented the typical cases of data security infringements. Generally, the reason for the highest risk data breaches from the viewpoint of data subjects is some kind of data security problem or deficiency hence, when examining the management of any incident, the Authority always evaluates the data security measures brought and applied prior to the incident. One typical problem is that although the controller is responsible for assessing risks to the privacy of natural persons and to implement appropriate technical and organisational measures to address them, this is frequently not done; however, the controller cannot pass the responsibility for meeting data security obligations to data subjects.

He illustrated another typical omission substantiated by legal cases why it is a serious problem when the controller fails to keep the systems used to process personal data up-to-date, perform vulnerability scanning, test the new systems planned to be implemented and use two-factor identification. He underlined that surveying the impact of a data breach, drawing conclusions and identifying the areas of the data security system to be improved was possible only if the events could be traced back through appropriate logging.

**Dr. Norbert Vass**, head of the Department for European Union Digital Data Strategy, gave a presentation on the new tasks and powers of NAIH. The “fuel” for most new technologies is data and it is important who disposes over these data – this is referred to as data sovereignty. This may be jeopardized by foreign data monopolies, which have a major advantage. It is not possible to help the small and medium-sized enterprises of the EU, if they set out from a major disadvantage; furthermore, the existence of a large number of sensitive data abroad and their inaccessibility in the given Member States also gives rise to questions

of national security. The protection of fundamental rights is substantially encumbered if legal regulations need to be enforced against an offshore controller or one established on another continent. Online identification within the EU is the precondition to implementing data sovereignty; this, however, has not been resolved to date.

He underlined the importance facilitating access by EU enterprises to private and public data, while attention also has to be paid to data security. The EU wished to resolve this set of problems with a complex legislative package: the Data Governance Act, the Data Act, the Regulation on Artificial Intelligence, the amendment to EIDAS and the Regulation on digital services. The Authority is responsible for registering and supervising data intermediation services and data altruism organisations and participating in the work of the European Data Innovation Board; furthermore, its responsibilities will include the performance of authority functions related to the new EU digital regulations linked to the data regulation and conducting the procedures related to the protection of personal data in the context of processing involving new technologies.

In Hungary, the National Data Asset Agency (Nemzeti Adatvagyon Ügynökség) was designated as the one-stop information point and the competent organ, while the Authority was designated as the competent authority.

On closing the conference, **Dr. Attila Kiss**, head of the Department for Data Protection Compliance and Public Relations, responded to questions sent in advance in writing to the Authority affecting a wide range of data protection officers. Several questions addressed the legal basis that could be cited in the context of performing public tasks, the obligation to report data breaches, the performance of the controller's obligation to provide information in relation to the exercise of data subject's rights and the possibility to exercise the right to obtain from the controller the erasure of personal data. He also mentioned the ruling of the Court of Justice of the European Union in the Másdi case concerning the interpretation of Article 14(5)(c) of the General Data Protection Regulation.

# II. Data protection cases

## *II.1. Application of the General Data Protection Regulation*

### *II.1.1. Political issues*

#### *1. Data protection issues of phone-based campaigns*

The Authority posted a report on its website on the findings of the investigations of data processing operations related to campaign calls during the parliamentary elections in the spring of 2022[2]. The information, inter alia, concerned an ex officio investigation against a limited liability company (hereinafter: Ltd.). The procedure was launched because the Authority received altogether 112 complaints in 2022, in which the complainants objected to the processing of their phone numbers not included in public phone directories for the purpose of political calls without their consent. The investigation explored several data processing problems; hence an authority procedure for data protection was launched.

According to the facts of the case found, the Ltd. and an association (hereinafter: Association) concluded a contract in which the Ltd. undertook to call at least 2.5 million phone numbers in the period between 29 March and 3 April 2022 with the purpose and at the times specified by the principal, for which the sound recording to be played was provided by the principal. The Authority established that the Ltd. obtained roughly 2.5 million phone numbers from a foreign individual whom the Authority could not contact despite several attempts to do so and the phone-based campaign was conducted using these numbers. According to the Ltd.'s statement, the database only contained phone numbers which could be used for direct business acquisition; the subscribers did not prohibit their use for such purpose. Other than the phone numbers, no personal data were processed – no other information to that effect surfaced in the course of the procedure and at the end of the campaign the list of phone numbers was deleted. The Ltd. did not send personal data to the Association, only the summary statistics of successful and unsuccessful calls. According to the statement of the Association, it did not give any specific instruction to the Ltd. concerning the database, it had no information on the foreign individual, it did not process any data that could be linked to a third-party natural person in relation to the campaign, the Association did not possess the list of phone numbers and never received such a list from anyone.

2 https://www.naih.hu/adatvedelmi-jelentesek/file/866-a-hatosag-altal-folytatott-vizsgalatok-megallapitasai-a-2022-tavaszi-parlamenti-valasztasokkal-kapcsolatos-kampanyhivasokkal-osszefuggo-adatkezeleseirol

When examining the personal nature of the data, the Authority explained in its decision that in determining the identifiability of a natural person, all methods should be taken into account which could be reasonably assumed to be used by the controller or another person for the indirect identification of a natural person. In the C-582/14 Patrick Breyer case, the Court of Justice of the European Union examining dynamic IP addresses declared that to qualify some information as personal data it was not a requirement that all the data enabling the identification of the data subject be held by a single person; this interpretation was confirmed also in the C-434/16 Peter Nowak case. So, based on indirect identification, the person concerned could be identified, if the specific information linked to other information (whether or not the controller has this other information, but it can be lawfully accessed) distinguishes the individual from others.

Based on the practice of the Authority, the phone number qualifies as personal data in itself as a main rule. In this case, the expressed purpose of the use of the phone numbers by the Ltd. was that they should be linked to working phones used by natural persons. Identification based on a phone number can be carried out through the public telephone directory or in other ways. For instance, by calling the phone number without knowing any other data, the person taking up the phone tends to present himself or herself at the beginning of the call as part of the usual greeting, or the phone service provider as third party could link these data to the given person at any time. Pursuant to Article 4(2) of the General Data Protection Regulation, any operation carried out on personal data, such as calling a phone number, qualifies as processing, to which the General Data Protection Regulation applies.

The Authority established that there was a contract between the Ltd. and the Association for the administration of the phone-based campaign (hereinafter: Campaign); the Association determined the purpose of the Campaign and its means (entrusting the Ltd.), hence as far as the Campaign was concerned, the controller was the Association. However, the subject matter of the procedure was not the entire campaign, but expressly the data compliance of the source and legal basis of the database that contained the personal data used by the Ltd. in the Campaign.

Based on the contract, the Ltd. “could initiate involvement of subcontractor(s)”; however, the Ltd. was as responsible for them as if it had acted itself. According to the Association’s statement, the Association received no information whatsoever on the use of a subcontractor (the individual of foreign domicile) by the Ltd.

Based on all the circumstances of the case, it was found that the involvement of the subcontractor (sub-processor) by the Ltd. took place without notifying the original controller, i.e. the Association, either in advance or subsequently; the Ltd. did not initiate the involvement of the subcontractor in any verifiable manner and the original controller had no knowledge of it. Based on the contract and Article 28(10) of the General Data Protection Regulation, the Ltd. was the controller in the context of the lawfulness of the given processing (processing the phone number database) and the supply of information to the data subjects, hence the Ltd. was responsible for the lawfulness of the given processing and providing information to the data subject, which was separate from the general legal compliance of the Campaign, for which the Association as controller was responsible.

The Authority found that the Ltd. itself acquired the list of phone numbers; it reassured itself of its lawfulness merely on the basis of an oral statement made by a private individual who was staying at an unknown place and was inaccessible and unable to substantiate it with anything when called upon by the Authority to do so. The Ltd. did not take any steps of merit in order to find out whether the list of phone numbers complied with the provisions of Section 162(2) of Act C of 2003 on Electronic Communications and provided no information of merit to the data subjects about the personal data processed, while it was only in a position among the actors of processing (in contact with the data subjects) to be able to do so. For these reasons, the Authority established the infringement of GDPR Article 5(2) as the Ltd. was unable to verify an appropriate legal basis not only because of the erasure of the data, but because demonstrability according GDPR Article 5(2) did not obtain even when the data were not yet erased. In addition, the Authority established that the absence of appropriate information to the data subjects infringed GDPR Article 14(1)(a), (c), (d) and (e), as well as Article 14(2)( a),( c), (e) and (f). [NAIH-1536-7/2024]

*II.1.2 Processing affecting minors*

*Emergency call prior to crisis placement*

In the case under investigation, a mother with her two-year-old child asked for help through a telephone helpline with a view to being placed in a secret shelter for battered women because of an abusive relationship. The Company running the helpline which is an organ pursuing tasks in the public interest supported by

the central budget keeps internal records of the emergency calls, which includes the content of the request and the measures taken.

Later, the father, who exercised parental rights over the child jointly with the mother, requested the Company on several occasions to give him a copy of the data processed on him and on the child. It was the position of the Company that it responded to every request considering also the enhanced protection of the institution of crisis accommodation, but it refused to issue the data on the child. According to their position, public interest linked to the proper exercise of the fundamental human rights to life, body and dignity and the protection of personal data can be identified against a data request aimed even indirectly at personal data in relation to (protected) data processed in the context of their tasks related to the prevention of violence amongst relatives, in this case data related to the whereabouts of the child, and this public interest was considered by the Company to be in contrast with the social interest linked to the data subject's right to access. Furthermore, based on their knowledge, the Company arrived at the conclusion that the father attempted to learn the place of stay of his family members placed in a crisis centre using individual requests, for instance, by masking his interest as an indifferent request for information, or by feigning the exercise of data protection rights or request for data of public interest.

As stated by the Company, in many cases, they do not record the name of the calling party, in other cases, they do not record any identification data other than the name, and thus identification of the person making the request requires careful consideration in every instance. According to GDPR Article 4(1), a person can be identified on the basis of several factors, in the present case based on the content of what was said, the information could be clearly linked to a single person. In this context, the Authority noted that according to its position, it would be expedient for the Company to carry out its activities processing as few personal data as possible. As the service works also through accepting anonymous calls, in the cases where the identification of the person of the caller is not absolutely necessary, it is best to avoid recording the name in view of the purpose limitation, data minimisation and storage limitation principles as set forth in the GDPR.

As to the data processed on the father, the Authority established that they originate partly from the calls made by him when he made inquiries at the Company; the data recorded on these calls can be issued to him because his person could be identified based on his name, which he disclosed. However, another part of the data processed about him originates from what the mother presented during the emergency calls. For this, it is necessary to interpret the notion of the so-

called shared personal data. Based on the GDPR concept of personal data, the same data may apply to several persons, typically when a statement made by a person refers to another person/other persons – that is when we speak about shared personal data. In this case, what the mother said could be the shared personal data of the mother and the father, or the mother and the child, or the father and the child as well. In such cases, every data subject is concerned and has the right of access to the data. However, when examining access rights, the rights and legitimate interests of every person concerned should be assessed and in the event that interests clash, it is necessary to adjudge which data subject's rights enjoy greater protection over the other data subject's right to access. In this case, the Authority found that the person taking refuge has the right that the information concerning the circumstances explaining the need for help and outlining their life situation, which also happened to be personal data of another person – in this case those of the father – should not be among the accessible data by reason of the functions of the emergency call and the shelter.

When balancing the obvious clash of interests, the Authority arrived at the conclusion that the fundamental rights of the person asking for help as an alleged victim are stronger than the other person's right to informational self-determination. Society has a more powerful interest in assuring that anyone should be able to call the emergency helpline believing that whatever is said there, remains confidential and should not fear that the party against whom help is required could learn whatever was said and of whom this communication carries information. However, if a police, authority or court procedure should be launched at a later date, the statements would have to be proven and verified when clarifying the facts of the case, and a discovery process would be conducted to expose the circumstances, so the other party exercising his procedural rights would learn the information arising about him in the course of the procedure, but prior to such procedures, the confidential nature of the request for help ensuring the fundamental interests of the person asking for help cannot depend on weighing what information may be disclosed by the calling party in the course of the call.

Based on all of this, the Authority deemed that the refusal to issue the data recorded based on the mother's statement was lawful on the basis of Article GDPR 15(4).

As to the data of the child, the Authority established that as legal representative, the father – alone without the consent of the other parent – is entitled to submit a request to access on behalf of the data subject child to the controller; if, however, the issue of the data would jeopardise the interests of the child that could restrict

access to the data because in such a case, based on Section 4:163 of the Civil Code, the legal representative may not represent the child, hence he cannot take action in the course of accessing the child's data. The Authority interprets this provision of the Civil Code as meaning that the "case" in which the legal representative is a party whose interests are contrary to those of the child, is itself the exercise of the right to access.

Therefore, the Company had to assess the clash of interest with respect to every processed data, because it may be possible that the disclosure of one data may be injurious, while not so in the case of another data and the Company also had to consider GDPR Article 15(4) with respect to the rights of another person as well. The Authority examined the information made available to it and found that apart from a single piece of information on the child, the Company did not record any data, which would not also be a personal data of the mother as they were recorded based on what the mother stated and in accordance with the above the father was not entitled to access such data based on GDPR Article 15(4).

As established by the Authority, the father is not entitled to access the information on the whereabouts of the child even as part of an access request, as none of the data of the shelter are public, access to the data is excluded by Section 98(6)(b) of Act XXXI of 1997 on the Protection of Children and the Administration of Guardianship. So, the father is not entitled to access the data in the context of the right to access exercised on behalf of the child because it is obviously contrary to the very essence of the shelter as an institution; disclosure of the data to the party against whom assistance was sought is excluded; this restriction can also be deducted from the provisions of GDPR Article 15(4).

In view of the reasons explained, the Authority took the position that the Company lawfully restricted the father's access to the child's place of stay data because of the clash of interest set forth in the Civil Code, hence in this context the Authority did not establish any infringement of the GDPR.

In terms of the legal regulations, the Authority found that while the provisions of the Act on the Protection of Children shall apply to institutions for sheltering people in a crisis – shelter, crisis centre – so the data processing rules of this Act govern processing by these institutions; however, this Act does not apply to the provision of assistance preceding crisis placement examined in this procedure. According to its Privacy Statement, the Company running the helpline refers to several legal bases for its processing of data; however, according to the position of the Authority, it would be justified to settle processing by organisations pro-

viding assistance prior to crisis placement in view of the fact that they perform tasks in the public interest. According to GDPR Article 6(1)(e) and (2)-(3), processing for the performance of tasks in the public interest shall be stipulated by legal regulation and also the eventual restriction of data subject's access to the processed data also requires legislative consideration in view of the fact that a minor is concerned in the present case. On account of this, the Authority called the attention of the Minister of Justice in charge of assistance to victims to this issue. [NAIH-4839/2024]

### *II.1.3. Processing by the public sector*

#### *Contradictions between the Act on the Protection of Children and the established practice*

During the investigation of a case, the Authority arrived at the finding that the Act on the Protection of Children and the protocol on the processes of the monitoring and signalling system run by the family and child welfare service drawn up and ordered to be applied in accordance with the authorisation granted under this Act and published in the website of the Ministry of the Interior (hereinafter: Protocol)[3] are not aligned in terms of the processing of law enforcement-related personal data and they order to process different ranges of data, which clashes with the principle of transparency under the provisions of GDPR Article 5(1)( a).

In the specific case, a child welfare service (hereinafter: Service) obtained criminal personal data on the applicant. The Service contacted the local police asking them for data on the applicant because as far as they knew, the applicant perpetrated a theft. The four underage children of the applicant had previously been placed in temporary care and the Service was collecting data on the life situation of the applicant to review the temporary placement of the children. The police informed the Service that they were conducting a procedure against the applicant because of the misdemeanour of theft.

Pursuant to Section 3(4) of Act CXII of 2011 on the Right to Informational Self-Determination and the Freedom of Information (hereinafter: Privacy Act), the

3 Section 17(3)(a) of the Act on the Protection of Children requires with mandatory force that members of the child protection signalling system take action according to the professional methodology on the operation of the signalling system drafted by the Minister with a view to preventing jeopardy to children. This professional methodology or protocol is to be published by the competent minister on the website of the Ministry he directs. The protocol on the processes of the monitoring and signalling system operated by the family and child welfare service is accessible on the website of the Ministry of the Interior.

information that the applicant is subject to a criminal procedure in progress qualifies as criminal personal data. The Service forwarded this criminal personal data to the Guardianship Department of the District Office of the competent Government Office (hereinafter: Guardianship Department). The applicant did not consent to the collection and forwarding of his criminal personal data by the Service and objected to the processing of the data, as well as the fact that the Service did not take into account the principle of the presumption of innocence until proven guilty to which he was entitled, handling his guilt as a fact.

It should be underlined that Section 5(7) of the Privacy Act stipulates that the rules relating to the conditions for processing sensitive data shall apply to the processing of criminal personal data, i.e. in view of GDPR Article 9(1), the processing of criminal personal data is prohibited as a main rule, and such data can be processed only if the processing has a legal basis in accordance with GDPR Article 6(1), or if a condition according to GDPR Article 9(2) exists.

In the absence of an express consent of the applicant, the Authority reviewed the cases of mandatory processing. Chapter XXI of the Act on Child Protection entitled "Processing of Data" authorises the head of the institution providing primary care for child welfare and its professional staff to process the criminal personal data of the parent or legal representative in two cases: according to Section 135(2)(b)(be) and (4)(b) of the Act on the Protection of Children they may process data concerning no criminal records and data concerning a criminal act by a parent against a child, the other parent bringing up the child, the person taking care of the child and any other person living in the same household with the child, respectively.

The wording of the text makes it clear that it authorises the processing of data only on criminal acts on which a final verdict has already been issued. The Act on the Protection of Children does not provide authorisation for the processing of data related to ongoing procedures aimed at the investigation of criminal liability.

Version 2[4] of the Protocol in force at the time of processing groups the factors indicating the jeopardy to the child and classifies them by severity. The problems taken into account when assessing the factors endangering the development of children in the course of risk analysis can be severe or expressly severe. The severe problems include: "Criminal procedure against a family member living together with a minor child". The Protocol specifies that the problems must

4 The problem referred to obtains also with respect to the Protocol currently in force.

be documented. So, the Protocol regulating the operation of the signalling system in detail requires the processing of the data concerning a criminal procedure in progress against the parent as family member living together with the child among the factors of severe jeopardy in which case the members of the signalling system have obligations to take action and to signal and hence also to process the data.

Although the Protocol as internal professional regulatory tool does not qualify as a legal regulation, its chapter entitled "The use of the Protocol, its connection to other professional regulatory documents", the Protocol declares that compliance with it is mandatory and people are accountable for it. According to Section 105 of the Act on the Protection of Children, the state is responsible for the supervision of guardianship tasks specified in this Act, and the operation of the system ensuring the protection of children. These tasks are overseen by the Minister.

Based on the above, the Authority established that the legal regulation, the provisions of the Act on the Protection of Children and the professional requirements of the Protocol, which are to be applied mandatorily with regard to the possibility to process the criminal personal data of the parent, are not aligned. While the specific legal regulation does not allow for the processing of data concerning a criminal procedure in progress against the parent, the Protocol requires it. It is, however, the responsibility of the legislator[5] to ensure the alignment of the legal regulations and the framework of professional cooperation determined by it in such a way as to guarantee the enforcement of children's rights, the pre-eminent interest of the child and the exceptional possibility of processing criminal data. To that end, the Authority issued a recommendation based on GDPR Article 58(3) (b) and according to Section 38(4) of the Privacy Act to the Minister of the Interior to remedy the deficiencies of the legal regulation of processing to be carried out in the course of the processes of the child protection monitoring and signalling system operated by the family and child welfare service. [NAIH-691-2024]

### *II.1.4. Processing personal data and privacy*

#### *Right of access and the attorney-client privilege*

5 According to Section 66(1) 27 of Government Decree 182/2022 (V.24.) on the responsibilities and powers of the members of the Government, the Minister of the Interior is the member of Government responsible for the protection of children and youth.
According to Section 90(1): In the context of his responsibility for the protection of children and youth, the Minister shall prepare the legal regulations concerning the protection of children and guardianship.

Several data subjects submitted petitions for authority procedures for data protection to the Authority on account of the infringement of their right of access by attorneys-at-law or law offices. In one such case, the data subject who was the adverse party in a civil litigation against a client represented by the attorney submitted a petition for an authority procedure for data protection because the attorney infringed his right of access by not responding to his request for access. Responding to the call of the Authority, the attorney cited his obligation of confidentiality, which in his view was absolute, extending to all the data related to the case. In his answer, he also referred to GDPR Article 14(5(d), under which – as he interpreted it – he did not need to make information related to processing available to the data subject in cases where the personal data must remain confidential, subject to an obligation of professional secrecy, regulated by Union or Member State law, including a statutory obligation of secrecy. The attorney underlined that the Petitioner has never been his client, but was an adverse party. According to the attorney's position, it follows from the above provision of the law that he had no obligation to inform the Petitioner and the Petitioner had no right of access.

Furthermore, the attorney stated that he responded to the Petitioner's request for access by letter; however, the delivery of the letter was unsuccessful. After this, he sent the letter to the Petitioner's e-mail address. Referring to his confidentiality obligation, the attorney did not give a full answer as to what personal data of the Petitioner he processed for what purpose and for what period. The attorney indicated GDPR Article 6(1)(c) and (f) as the legal basis of processing the personal data.

Taking the arguments of the attorney into account, the Authority pointed out in its decision that should there be a clash between the obligations set forth in the GDPR and the provisions of Act LXXVIII of 2017 on the Activities of Attorneys (hereinafter: Attorneys Act) concerning attorney-client privilege, then this apparent conflict is resolved by the principle of the primacy of EU law, according to which the GDPR has to be applied as against the legal regulation of the Member State, in this case the Attorneys Act.

The decision also stated that generally attorneys carry out processing subject to the GDPR, which is supervised by the Authority. From the viewpoint of establishing the capacity of controller, it is irrelevant whether the data subject exercising his right of access is a client of the attorney or an adverse party. The determination of the controller is governed by the GDPR and not the provisions of the Attorneys Act. It follows that the attorney is bound by the controller obligations

according to the GDPR, including the appropriate evaluation of the data subject's requests (for access).

In its decision, the Authority pointed out that differences between the right to prior information according to GDPR Article 13 and 14 and the right of access according to GDPR Article 15, and underlined that Article 14(5)(d) referred to by the attorney does not constitute a restriction on the right to access, in view of the fact that the provision referred to clearly calls for applying the exception concerning the confidentiality obligation to GDPR Article 14(1)-(4) and not to Article 15.

With regard to data processed in relation to the litigation, the attorney cited GDPR Article 23(1)(j), as in his view, the restriction was necessary with a view to the enforcement of civil law claims. With regard to the extra-judicial procedure related to the civil law claim, the attorney pointed to GDPR Article 23(1)(i) and (j) implying that the restriction was necessary for the protection of the right of the principal and the enforcement of civil law claims.

However, the Authority established that the restriction according GDPR Article 23(1) does not constitute a general restriction with regard to GDPR Article 15. The right according to GDPR Article 15 may be restricted as necessary and proportionate for the protection of interests listed in GDPR Article 23(1), provided that such a restriction respects the essence of the fundamental rights and freedoms.

The Authority accepted the attorney's reference to attorney-client privilege according to Section 9(1) of the Attorneys Act as a reference to a restrictive measure by a Member State with regard to GDPR Article 15(1)(b), (c) and (g), and (2) and (3) according to Article 23. If an acting attorney was to provide information to the adverse party subject to the above attorney-client privilege and gave a copy of the data processed by the attorney, it could have an actual impact on the outcome of legal procedures related to the enforcement of civil law claims, or other legal procedures and could jeopardize the enforcement of interests to be protected as set forth in Article 23(1) [particularly Article 23(1)(f), (i) and (j)] of the General Data Protection Regulation.

In this regard, the Authority took the position that it was irrelevant that the procedures in relation to which the attorney has processed the personal data of the Petitioner were already closed in view of the fact that the right of access according to GDPR Article 15 can still be restricted in the interest of the protection of the rights and freedoms of the attorney's client. The Petitioner's right of access

was restricted as detailed above based on GDPR Article 23(1)(i) with a view to protecting this interest of the Petitionee's client.

However, in view of the fact that the procedures, in relation to which the attorney has processed the personal data of the Petitioner were already closed, the information to be provided on the purpose of processing [GDPR Article 15(1)(a)] is not attorney-client privileged information because the attorney independently determined the purpose of the continued processing of the personal data related to closed procedures, so, these are not items of information of which the attorney had learned in the course of exercising his activity.

With regard to the subsequent points of GDPR Article 15(1), i.e. points (d), (e), (f) and (h), the reference to attorney-client privilege according to Section 9(1) of the Attorneys Act as a Member State restrictive measure according to Article 23 is not acceptable. In addition, the attorney has an obligation to inform the Petitioner also on the issue of whether the processing of his personal data is in progress.

In its decision, the Authority pointed out the following with regard to GDPR Article 15(1)(d), (e), (f) and (h) in view of the statement made by the attorney during the proceedings.

- Under GDPR Article 15 (1)(d), the data subject is entitled to obtain information on the envisaged period for which personal data will be stored, or if it is not possible, on the criteria used to determine that period. In this context, the attorney stated that in a lawsuit it is not possible to know how long it will last; moreover. it was not at all certain that the case would end with a final judgement from the viewpoint of the attorney. In addition, the period could be influenced by the minimum retention dates as well. The Authority pointed out that under GDPR Article 15(1)(d), the controller has to provide information to the data subject not only in the case when he knows the final date of processing because if it is not possible to provide information on this, he has to provide information to the data subject on the criteria used to determine that period.
- Under GDPR Article 15(1)(e), the data subject is entitled to receive information whether he has the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject, or to object to such processing. GDPR Articles 16 17 and 21, respectively, regulate the right to rectification, the right to erasure and the right to objection. Consequently, the data subject's right to rectification, erasure and objection should be interpreted within the frame-

work of these legal provisions and not without limitation. GDPR Article 17(4)(d) excludes the onset of the case cited by the attorney, namely that the adverse party requests the erasure of his data, which would thwart the enforcement of the legitimate claim of the principal. Consequently, the attorney should have provided appropriate information to the Petitioner on the right to rectification, erasure and objection according to GDPR Articles 16, 17 and 21, which does not mean that the attorney would have had to erase the personal data of the Petitioner in the case of an eventual erasure request in every case without limitation.

– Under GDPR Article 15(1)(f), the data subject is entitled to receive information on the right to lodge a complaint with the supervisory authority. In contrast to what the attorney stated, this is not an obligation to provide information in advance by the controller; instead it is only subsequently that the controller has to inform the data subject on the right to complaint in the context of his right of access upon the express request of the data subject.
– Under GDPR Article 15(1)(h), the data subject must be informed of the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4), and at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

The above constitutes information related to the general operation of the attorney and other technical information, which the attorney as controller had to determine unilaterally prior to the commencement of processing, even prior to entering into an assignment with a specific client.

Based on the above, the Authority established that the information sent by the attorney to the Petitioner was inadequate as instead of providing the information according to GDPR Article 15(a), (d), (e), (f) and (h), he failed to comply with the Petitioner's request to access with reference to GDPR Article 14(5)(d) and Section 9 of the Attorneys Act in view of the attorney-client privilege.

In view of the above, in particular, the fact that the exception according to GDPR Article 14(5)(d) is not applicable to the right to access according to GDPR Article 15, the Authority established an infringement of GDPR Article 15(1) and based on GDPR Article 58(2)(c) ordered the attorney to answer the Petitioner's data subject request with respect to GDPR Article 15(1)(a), (d), (e) (f) and (h) and whether the processing was in progress.

In its decision, the Authority called the attention of the attorney also to the fact that more than five years have passed since the entry into force of the GDPR, so it is not acceptable for somebody not to know and not to apply the GDPR, particularly in the case of those who practice as an attorney and refuse to grant a data subject's access request in full with reference to attorney-client privilege. The Authority underlined that infringements related to non-compliance with the provisions of the GDPR continued to be frequent among practising attorneys. The Authority pointed out that an authority procedure for data protection allows for levying fines and in the event of similar infringements to be exposed in the future, it will consider the imposition of a data protection fine in view of GDPR Article 83. [NAIH-186/2024]

### *II.1.5. Video surveillance at the workplace*

#### *1. Video surveillance in a swimming pool*

The Authority received a report objecting to processing carried out using a set of cameras operated in the building of a city swimming pool. According to the balancing test carried out by the controller, the purpose of processing using the electronic surveillance system was the protection of human life and health and the protection of assets. The controller applied GDPR Article 6(1)(f) as the legal basis of processing using the video surveillance system, which also monitors employees. The Authority regards the application of this legal basis as generally acceptable in the context of video surveillance systems for the purpose of the protection of persons and assets; however, the processing by the controller also extended to areas where the purposes specified by the controller had no verified basis, or where the surveillance was not absolutely necessary to achieve the declared purpose.
According to the controller's statement, the purpose of surveillance in the case of the camera operated in the sauna was on the one hand to check compliance with the house rules, and the exclusion of foul play in the event of fainting. The Authority regarded the fact that the controller monitored the guests of the swimming pool in their swimming costumes while resting and relaxing as disproportionate to the purpose to be achieved and on that basis established that the controller infringed GDPR Article 6(1) and ordered it to cease processing.

In the case of the cameras monitoring the buffet and the two cash desks of the swimming pool, the purpose of asset protection indicated by the controller could be verified, at the same time, the cameras' angle of view was restricted to the

assets to be protected allowing the ongoing surveillance of the guests eating in the buffet and the employees working there. According to the position taken by the Authority, it would have been possible to place the cameras in such a way as to reconcile surveillance with the original purpose of protecting persons and assets, so the Authority established that the placement of the cameras infringed the principle of purpose limitation according to GDPR Article 5(1)(b).

Employees received oral information on the surveillance system in the swimming pool when entering into their employment relationship. The controller put up pictograms at the entrances to the swimming pool and within the building; however, it produced a detailed written Privacy Statement containing the information according to GDPR Article 13 as a result of the Authority's procedure. Based on the above, the Authority established that the controller failed to provide appropriate advance information to the data subjects on processing using the video surveillance system infringing GDPR Article 13(1) and (2).

The Authority also established that the controller determined the 30-day storage period disproportionately to the purpose to be achieved, infringing the principle of storage limitation according to GDPR Article 5(1), so the Authority ordered the controller to reduce the storage period of the video records to the period necessary for achieving the purpose of processing. Because of the established infringements, the Authority imposed a data protection fine of 3 million forints on the controller. [NAIH-614/2024]

2. *Unlawful video surveillance of the workplace by a company pursuing asset protection*

Following the lodging of a complaint by an employee, the Authority launched an authority procedure for data protection ex officio against the company pursuing asset protection. According to the complaint, the controller carried out unlawful video surveillance in the operator's rooms using several cameras, allowing it to continuously observe the activities of the operators working there. According to the complainant, the video surveillance was in actual fact to control the behaviour and communication of the employees, which was permanently monitored by the executive officers of the company partly using the office monitors and partly with the help of a mobile phone application.

In its answer, the controller confirmed that it operated 5 cameras, the legal basis of the operation of which was the legitimate interest of the controller. The pur-

pose of processing was the facilitation of the protection of human life, health, business secret and assets, and the investigation of complaints.

In the course of the procedure, following a detailed examination of the documents related to the cameras and the angles of view of the cameras, the Authority established that the mode of processing failed to comply with the principle of proportionality, the purposes of processing referred to could be achieved using less intrusive methods, including by modifying the cameras' angles of view.

Based on the above, the Authority established that the client infringed the principle of data minimisation according to GDPR 5(1)(c) and also the rights to receiving information and access to personal data according to GDPR Article 13(1)-(2) by failing to provide appropriate information about the processing and related matters to employees. In its decision, the Authority ordered the controller to dismantle the cameras in the operator's rooms, or to modify their angles of view so as to be appropriate to the processing purposes referred to. The controller complied with the above order. [NAIH-123/2024]

*3. Unlawful processing related to the access control system of a hospital*

In their complaint, doctors working in a hospital presented that an access control system functioning with a chip card was installed in their hospital, which also takes a snapshot of the entering person when allowing entry. The doctors employed by the hospital found the snapshots taken upon entry to be unlawful because they were identified several times during entering, apart from this.

According to the hospital's statements, the hospital made a decision on installing an access control system at its headquarters acting in its capacity as controller and in its powers as employer in the autumn of 2021. They indicated Article 6(1)(c) GDPR as the legal basis of processing, i.e. processing was necessary for compliance with a legal obligation to which the controller is subject; however, the hospital was unable to provide accurate legal references in the individual legal regulations despite being called upon to do so several times. The storage period for the data processed by the access control system is 60 days. The snapshots could be viewed by the head of the institution and a person granted supervisory powers under the rules with a view to achieving the purpose of processing only if suspicion arose that the actual user of the RFID tag is not its holder. The cameras connected to the access control system were placed in the access control units (access control boxes). The cameras did not observe a specific area; they only made snapshots when the RFID device was used (at the moment of click-

ing). The hospital was unable to point out any specific and proven documented case of abuse of the access cards but they "had heard" of such cases earlier.

In its decision, the Authority established that the hospital infringed GDPR Article 5(1)(e) ("storage limitation") with the access control system applied by it in the context of the storage period of the snapshots taken of the entering employees as the relevant documentation did not reveal why the period for storing the data was determined in 60 days.

In its decision, the Authority also established that the hospital infringed GDPR Article 5(1)(c) ("data minimisation") because of the unjustifiably wide angle of view of the area recorded by the snapshots taken of the entering employees using the access control system.

In addition, the hospital infringed Article 6(1) GDPR, when it based its processing related to the access control system on an inappropriate legal basis as the provisions referred to by the hospital on which it based the processing under investigation do not specifically require either an access control system, or the taking of snapshots of the employees in relation to this. Also the hospital infringed GDPR Article 13(1)(2) as it failed to provide information to the employees on the processing related to the access control system appropriate to the General Data Protection Regulation.

Based on the above, the Authority called upon the hospital that if it wishes to use the suspended snapshot function of the access control system again to reconsider the period of storing the snapshots and to apply a technological solution, which would only record the data of the employees to be checked in the course of entering and to amend the information on processing, particularly with regard to the legal basis of processing. [NAIH-1099/2025]

4. *Unlawful video surveillance at the premises of a catering company, which continuously monitors employees even in the rest room*

The Authority received a complaint in the public interest, in which the Complainant objected to the continuous surveillance of employees even in the rest room using a video surveillance system at the premises of a catering company. The employees received no information on the operation of the cameras. In the wake of the complaint, the Authority carried out an onsite inspection in September 2023, in the course of which it observed the following: there were two cameras in the manager's office, one of which was directed at the workplace of the financial staff

member working there, his desk. There was one camera in the left corner of the rest room monitoring the entire room. A pictogram informed the persons staying in the rest room of the video surveillance. The computer in the rest room could be used for private purposes. The Privacy Statement for employees hung in the rest room did not provide information on the video surveillance. There was a locker with separate keys for storing valuables in the room. The keys could be obtained from the business manager/shift manager, which was recorded. Employees work in the restaurant 0-24 hours and the cameras operate on an ongoing basis. Apart from the pictogram calling attention to video surveillance located on the entrance door, there was no information (such as Privacy Statement) concerning the video surveillance in the guest space. The controller later supplemented what was stated at the onsite inspection with the statement that the purpose of video surveillance in the rest room was the supervision of the locker for storing valuables and the protection of electric equipment, the protection of the life and health of the data subjects and in the event of complaints or criminal acts, their efficient investigation. The period of storage for the camera records is 30 days from the day of recording. At the time of the procedure, there were 26 cameras in the restaurant. The documents providing information to employees are accessible to the employees in the guest space, so that they could be accessed also by the guests.

In the case of the camera placed in the rest room, the Authority did not regard the purposes of asset protection to be acceptable, in view of the fact that there was a lockable safe with keys and based on the experiences of the onsite inspection, there were no assets of any major value, hence ongoing video surveillance was neither necessary, nor proportionate processing, so the Authority established the company infringed GDPR Article 6(1) with the video surveillance of the rest room.

The camera's view angle in the rest room covered its entire area. According to the statement of the controller, the assets to be protected were a television, a microwave oven, a refrigerator and a personal computer. The assets listed are generally used kitchen utensils, whose value and number do not reach the level that their protection would take precedence over the level of protection of the privacy of employees. The protection of the personal computer is similarly evaluated in view of the fact that it is not related to the business of the company as it can be used by employees for private purposes. The controller has operated the video surveillance system since 2007; and the two examples cited by the controller (previous atrocities among employees) do not justify, in terms of their number, frequency and severity, to have continuous surveillance in a room intended fundamentally for rest and breaks from work.

The angle of view of the cameras in the manager's office is directed not only at checking cash flow, procedures for sorting money into bags and cash counting processes, but cover a much wider area, because of the small size of the room, enabling the full observation of the room, so according to the position of the Authority, this processing infringed the principle of data minimisation under GDPR Article 5(1)(c).

The Authority found that the cameras in the rest room and in the manager's office are suitable for the unwarranted observation of employees, which is not reconcilable with the original purpose of protecting persons and assets. The placement of the cameras infringes the principle of purpose limitation according to GDPR Article 5(1)(b) , hence the Authority called upon the client to remove the cameras from the rest room and cease video surveillance and to alter the angle of view of cameras in the manager's office, so that they should not be able to unjustifiably and continuously monitor employees and be consistent with the asset protection purpose of installing the system.

The Authority established that the client infringed the principle of fair processing according to GDPR Article 5(1)(a) by the surveillance of the employees' rest room used for eating and resting.

Although the controller did have various documents to inform employees, there was no single transparent document covering all the details of the video surveillance available to them, so the Authority established that the client failed to bring appropriate measures to provide all the information mentioned in GDPR Articles 13 and 14 concerning the processing of personal data in a concise, transparent, comprehensible and easy to access form, worded clearly and in an easy to understand manner, whereby it infringed GDPR Article12(1).

Because of the established infringements, the Authority imposed a data protection fine of HUF 30,000,000 on the controller. [NAIH-1405-6/2024]

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

*1. Investigation of the general processing operations of a real estate franchise network*

The Authority investigated the general data processing operations of a real estate franchise network related to real estate brokerage.

According to the Authority's findings, the franchise holder and its partners carry out their activities in various processing roles. This includes joint controlling, independent controlling and data processing on the part of the partner. As the franchise holder failed to differentiate the various processing roles when designing its data processing operations, neither a joint controller contract, nor a processing contract was concluded and the information provided on processing could not be regarded as adequate. In addition, the franchise partners only received deficient, sketchy instructions from the franchise holder concerning the granting of data subject requests. Finally, it was also established that the Privacy Statement developed by the franchise holder and used by the entire franchise network was inadequate in the context of submitting data subject requests, and the controller failed to facilitate the exercise of data subject rights.

In addition to establishing the above infringements, the Authority imposed a data protection fine of HUF 50,000,000 on the holder of the franchise network. [NAIH-910-7/2024]

*2. Disclosure of the religious affiliation of staff members of a television company*

The Authority received a notification in the public interest because a public figure disclosed the religious affiliation of several staff members of a television company on his social media site, giving their jobs, but not disclosing their names.

The Authority established that the persons indicated in the published post without their names were identifiable by their shows. Consequently, the controller published information on identified persons, i.e. data subjects in his post. The published post included special category data concerning religious affiliation and belief.

In the course of the procedure, the Authority established that the disclosure of the data of the religious affiliations of certain staff members of the company is not appropriate for the purpose of processing to demonstrate that the television

company was allegedly not “independent”. The issue of independence is determined not by the religious affiliation of individual staff members, but the broadcast content. It follows that the processing did not serve the achievement of the purpose, thus it infringed the principle of data minimisation.

According to the Authority’s position, in this case no legal basis other than the consent of the data subjects could be cited; however, they obviously never gave their consent. In addition, the condition of the lawfulness of processing special category data did not obtain. It follows that the controller disclosed special category data of the data subjects in his post without a legal basis. [NAIH-9022/2024.]

*3. Roles of the controller and of the processor in relation to data forms required to submit requests for payment facilitation in cases before municipalities*

In this procedure, the Authority examined the roles of controllers and processors in the context of the data forms required for the submission of requests of payment facilitation in cases before municipalities accessible on the E-municipality portal (hereinafter: OHP) used uniformly nationwide.

The development of the forms and the specification of their data content are done centrally based on the decision of the Hungarian State Treasury (MÁK). The municipality decides whether to use the datasheet published by MÁK in their own area of competence. Through the fact that the municipality decides on the use of forms designed and published by MÁK in dealing with local municipal cases, both MÁK and the municipalities are to be regarded as independent controllers.

On account of the deficiency of legal regulation, the Authority deemed it necessary to have a clear regulation of the roles in processing related to the development of datasheets and, because of this, issued a recommendation to the competent Ministry. [NAIH-12304/2024.]

*II.1.7. Authority procedure for data protection in borderline cases*

The right to the protection of personal data is not an absolute right; it has to be enforced in conjunction with other fundamental rights. Pursuant to Recital (153) of the General Data Protection Regulation, “Member States law should reconcile the rules governing freedom of expression and information, including journalistic, academic, artistic and/or literary expression with the right to the protection of personal data pursuant to this Regulation”. In its legal practice, the Authority

regularly encounters cases, in which the main issue is how to reconcile the right to the protection of personal data with the right to access and propagate data of public interest, or the right to the freedom of expression. In these so-called borderline cases the application of the law is focused on resolving the clash of fundamental rights and ensuring constitutional balance. The Authority investigates these cases, similarly to data protection cases under investigative (complaint) or authority procedures.

*1. Cases of borderline investigative procedures*

The data subjects objected to the controller posting a video recording of them to a YouTube channel without their knowledge and failed to grant their request for erasure. The Authority established that in view of the provisions of Constitutional Court Decision 3145/2018. (V.7.) the data subjects were so-called exceptional public figures due to the fact that they were activists of a social movement who, by virtue of their statements and the events regularly organised by them on a specific subject matter, are influencers of public debate.
According to the Authority's findings, even though the data subjects undoubtedly qualify as exceptional public figures, what was said on the recording could not be qualified as public debate. The Authority concluded that the mere fact that the data subjects are exceptional public figures does not in itself constitute a basis for sharing the recording with the public. The reason partly is that the recording was made of them as private individuals at a beach and partly because it recorded an altercation between the data subjects and members of the controller organisation, which could not be defined as a public debate. The Authority established that neither sharing information related to private life, nor the debate between the parties contributed to the discussion of public affairs; it did not serve any interest of society, nor was there a legitimate interest in this case. The Authority found that the arguments of the controller were unfounded and accordingly ordered it to grant the erasure request without delay. [NAIH-4895/2024]

*2. Cases of borderline authority procedures*

As a result of its procedure launched ex officio, the Authority condemned a private individual controller for having infringed GDPR Article 5(1)( a), (b), (c), Article 5(2) and Article 31 by publishing the personal data of staff members of the Magyar Nemzeti Bank performing an onsite audit through the YouTube video sharing portal. The Authority ordered the controller to erase the personal data from the video and also levied a data protection fine because of the infringement. The controller did not cooperate with the Authority at all, hence a procedural fine

in substantial amount was also imposed in the course of the procedure; also, the Authority ordered the enforced recovery of the data protection fine and the execution of the erasure of the personal data as specific acts. The controller erased the video in the course of the enforcement procedure. [NAIH-3089-7/2024.]

A former local entrepreneur (local public figure) contacted the Authority because he unsuccessfully objected to the processing by a county library because the library did not erase the search results of searches for the name of the Petitioner in their online catalogue (search result). The Petitioner verified that according to his certificate of good conduct, he had no criminal record, however, some of the hits pointed to articles published in the press 15-20 years ago concerning his criminal cases and cited the disadvantages affecting him because of this.

The Authority agreed with the library insofar that the legal basis of processing personal data in the online catalogue was GDPR Article 6(1)(e) in contrast to the Petitioner's claim according to which the processing was based on the legitimate interest of the library according to GDPR Article 6(1)f) , because the processing of personal data took place within the framework of discharging its tasks in the public interest as defined in Sections 65(2)(c), 66(a), 66(m) and 55(1)(f) of Act CXL of 1997 on Museum Institutions, Public Libraries and Local Socio-Cultural Activities (hereinafter: Act on Culture). However, the Petitioner is entitled to the right to object to processing, as well as the right to be forgotten even in this case, based on the General Data Protection Regulation. In the course of designing and operating its online catalogue, the library qualifies as controller, in view of the fact that it independently determines the design and operation of the online catalogue in its rules on the catalogue and the rules on the range of collections constituting a part thereof.

With regard to the hits pointing to criminal cases, the Authority found that the inclusion of special category data in the online catalogue was not compliant with the rules on the range of collection and also pointed out that as a main rule, the discharge of tasks in the public interest according to the Act on Culture does not constitute a legal basis for the publication of search results concerning special category data of data subjects and just because these data had once been published in the press they did not become data accessible on public interest grounds. No public interest in the publication of the search results concerning the Petitioner's criminal cases could be identified, whereas the processing put him at a substantial disadvantage as he had no criminal record as verified by his certificate of good conduct, so if he was not condemned in the cases described in the article(s), such disclosure infringes the right of the Petitioner to the pre-

sumption of innocence as set forth in Article XXVIII. (2) of the Fundamental Law, while in the cases with regard to which the Petitioner may have been exempted from the legal consequences of having a criminal record, he has to account for his condemnation despite the exemption. Because of this, the Authority ordered the library to permanently erase the search results from its online catalogue on the Petitioner's criminal cases as a result of searches for the Petitioner's name in accordance with Article 17(c) of the General Data Protection Regulation. [NAIH-1283-20/2024]

Photos of the family home of a public figure politician and some construction e-logged data of the house were published in articles without the consent of the politician. In its authority procedure for data protection, the Authority found that the personal data published in these articles concerned the private life of the Petitioner politician. However, it was precisely this segment of private life, which was the subject matter of a public debate: to what extent do the allegedly unlawful construction projects of public figures remain without legal consequences and whether they are assisted in this by their contacts in decision-making position. As a public figure, the Petitioner had to expect that in the public debate he had started his credibility would be scrutinized in relation to the subject matter of the debate and the public would be informed of the results thereof. A public figure does not have to expect that certain areas of his private life would be disclosed to the public in the case of every public debate. However, if a public debate started by the given public figure is on the unlawful construction project of a public figure – that is a question concerning privacy – then he has to expect that the lawfulness of his own construction project. i.e. this part of his own private life could become embroiled in the public debate. The Authority established that the processing operations objected to did not constitute an unnecessary and disproportionate intrusion into the private life of the Petitioner as the processing was indispensably linked to the public affair addressed in the articles and the articles only disclosed the photos of the property and the e-logged data intended to support the alleged unlawfulness of the construction project and no other moments of his private life, which were not necessary for substantiating the creditworthiness of the Petitioner. Because of this, the Authority rejected the Petitioner's request to establish that the Petitionee unlawfully processed his personal data. [NAIH-5461-2/2024]

*II.1.8. Recommendations and statements issued by the Authority*

*1. The Authority's recommendation concerning issues of data protection related to the election campaign*

Similarly to earlier years, the Authority published its current recommendation addressed to political parties on its website in the spring of 2024[6], where it called the attention of political parties and political organisations to the data protection requirements prior to the campaign period; the current recommendation primarily addressed issues of political marketing.

First, the Authority called attention to the importance of providing information in advance, which had to contain the identification of the sender and principal of the message, the source of the data processed, the legal basis of processing and the accessibility of additional information in detail. According to the Authority's experience, in the absence of such information, citizens tend to become increasingly suspicious that the party contacting them obtained their contact data unlawfully.

The Authority also shared its experience according to which it frequently occurs during the campaign period that the senders of campaign messages collect certain data of the voters from non-legal sources in order to reach as many voters as possible. So, for instance, the Authority deems it unacceptable if purchased databases are used unlawfully, if data or databases obtained earlier with data provided for a different purpose are used for campaign purposes, or if they wish to reach persons in the existing database of another company or call centre without a proper legal basis. In such cases, the provision of information on the source of the personal data may be particularly important; for this, an accurate record of the source of personal data is necessary.

The Authority underlined that the principles of purpose limitation and data minimisation have an outstanding role to play also when building up sympathiser databases, so that only the data necessary for the achievement of the given purpose (delivering a message, campaign) are recorded. For instance, there is no need to request an ID number for the purpose of political marketing or keeping in contact as the provision of this data is governed by legal regulation: it may be requested to be given only by organs collecting signatures for the initiation of referenda or European citizen initiatives and collecting nominations in an elector-

6 https://www.naih.hu/adatvedelmi-ajanlasok?download=915:ajanlas-valasztasi-kampannyal-kapcsolatos-adatvedelmi-kerdesekrol

al process and the citizens have to provide it only when exercising their right to make civil initiatives or nominate persons.

The recommendation separately addressed the roles in the processing of data, such as the responsibilities of the controller and the role and responsibilities of the processor. So, as a main rule, a political party qualifies as a controller even if it only “gives its name” to the achievement of the processing purposes determined by it and cooperates with others to that end, even if it does not personally take part in the execution of the processing operations. The Authority underlined that it is not possible to wiggle out of the responsibilities of controller by attempting to dodge controller responsibility through various pseudo-assignments, multi-level contract arrangements, essentially through a chain of contracts or attempt to mask their role in processing by hiding behind an organisation that is less financially accountable. Actual controllers must bear the responsibility it entails. In the case of joint control, the agreement must extend to issues of responsibility because it is not necessarily divided equally among the parties in practice.

In relation to consent which is the most frequently applied legal basis, the Authority called the attention of the parties to the fact that the controller must be able to demonstrate that the data subject has actually consented to the processing of their personal data and that the processing complies with the conceptual elements of consent; furthermore, the controller must ensure that consent can be withdrawn as simply as giving it, hence the Authority recommended that controllers include a link for the withdrawal of consent in every electronically sent newsletter.

In view of the fact that more and more controllers use various applications, create or use individual subscription websites and collect data through them, the Authority emphatically drew the attention of parties and political organisations to the fact that they need the digitally documented consent of the sympathising voter to save any data. It is desirable that parties and campaign organisations provide information also on the technology and methods applied (for instance, when Facebook and Messenger are used as campaign devices) in such a way that it can be reviewed simply by an average person without using technical terms.

2. *Recommendation on the processing of calls to the central emergency call number (1830) for emergency primary care by family doctors, family paediatricians and dentists*

The Authority sent a recommendation to the Ministry of the Interior requesting them to settle the guarantee rules for processing in relation to calls to the 1830 emergency primary care number, determine the mandatory period of storing the records and the addressees of the data. The Ministry of the Interior accepted the recommendation and stipulated the guarantee requirements in Section 10(3)-(6) of Act CXXIII of 2015 on Primary Healthcare. According to the new provisions which entered into force on 1 January 2025, in the case of calls received by the state ambulance service via the central emergency call number related to primary care provided by family physicians, family paediatricians and dentists, it has to record the phone communication as well as the identified data of the phone used by the calling party in a traceable manner using sound recording or other electronic means and it has to process the data for five years from the date of the call received. The provision sets forth that if telemedicine care is provided through the call, its data need to be processed not only through the recording, but also as part of the healthcare documentation.

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

### *II.2.1. The lawfulness of forwarding criminal personal data in the course of criminal proceedings and the scope of the power of attorney*

Upon request, the Authority investigated the lawfulness of the procedures of the police headquarters and the police station in relation to the processing of the personal data of the Petitioner in an authority procedure for data protection. In his submission, the Petitioner objected to the fact that the police headquarters forwarded his personal data processed in relation to a criminal proceeding (decision made on a motion to exclude, hereinafter: Decision) to his former legal representative (hereinafter: Attorney). The Petitioner explained that the Attorney did not have a power of attorney in force at the time of the delivery of the decision because the Attorney represented him only with regard to certain procedural acts, hence he was not authorised to have access to the personal data included in the Decision. According to the Petitioner's position, a data breach according to Section 3(26) of the Privacy Act took place.

The Petitioner issued powers of attorney to the Attorney on two occasions in the course of the criminal proceedings for representation in certain procedural acts – with full rights in the course of a psychiatric examination and during a witness hearing.

The Petitioner submitted a motion to exclude to the police station taking action in the basic case, which the police station sent up to the police headquarters for adjudication indicating the Attorney as the legal representative of the Petitioner. The police headquarters rejected the motion with its Decision and delivered the Decision also to the Attorney.

In the course of its authority procedure for data protection, the Authority established beyond any doubt that there was no data breach. The decisive conceptual element and condition of a data breach is that its result – accidental or unlawful annihilation, loss, modification, unauthorised forwarding, etc. – stem from a breach of security. As far as the facts of this case are concerned, the Decision was delivered to the Attorney as a result of a deliberate decision, which took into account procedural rules and was in compliance with the case management pro-

tocol. At the same time, the fact that there was no data breach does not mean that there could not have been unlawful processing.

Pursuant to Section 34(5) of Act LXXVIII of 2017 on the activities of attorneys "the client may withdraw or restrict the power of attorney at any time. The restriction of the power of attorney is in force with regard to a court, other authority or any third person, if the restriction is revealed from the power of attorney itself".

The power of attorney given by the Petitioner to the Attorney was linked not to a specific event – e.g. specified by a date – but to a procedural act, namely full representation according to the Attorneys Act in the course of a psychiatric examination. The psychiatric examination was still in progress when the motion to exclude was submitted. According to the position of the Authority, the power of attorney of the legal representative authorised for the psychiatric examination – unless a contrary circumstance can be clearly identified from the power of attorney itself – can be interpreted as extending to the entire examination. The basis of this interpretation stems precisely from guaranteeing and protecting the rights of the person concerned in the proceedings. In view of this, in its authority procedure for data protection, the Authority established that the police station had grounds to regard the Attorney as a legal representative having a power of attorney in force in the course of its proceedings, so it lawfully forwarded the data of the Attorney to the police headquarters with the submission to adjudicate the motion to exclude, and the police headquarters forwarded the Decision containing the personal data of the Petitioner to the Attorney with the appropriate legal basis. [SZTF-284/2024]

*II.2.2. Unlawful processing of personal data by checking the documents of a detainee*

Following a notification, the Authority launched an investigative procedure against a penitentiary institution (hereinafter: Controller) because the Complainant complained against unlawful processing by staff members of the institution. The Complainant presented in his submissions that his documents, which he lawfully kept with him, his correspondence with authorities and his attorneys were subjected to content checks during the security inspection of his cell on two occasions; three documents were placed in secondary deposit and were returned to him only eleven days later. Because of these measures, he lodged a complaint first with the Controller and then with the Budapest Prosecutor's Office. In both cases, the Budapest Prosecutor's Office established the infringement of Section 174(4) of Act CCXL of 2013 on the Implementation of Sentences,

Measures, Certain Coercive Measures and Detention for Misdemeanours (hereinafter: Sentences Act) with regard to the prohibited content checking of the Complainant's correspondence.

In its answer sent to the Authority, the Controller acknowledged the fact of the security inspections and the placement into a deposit. The enclosed documents from the Prosecutor's Office verified to the Authority that the Complainant's statements concerning the unlawful checking of his documents and correspondence were correct. The investigation by the Prosecutor's Office exposed that staff members of the Controller took the documents and letters of the Complainant out of their envelopes and folders; studied certain documents for an extended period of time or read in part or in full. This was evident from the video recordings viewed by the prosecution. In this way, they accessed the personal and criminal personal data of the Complainant, but also those of other data subjects, which in addition to being prohibited by the provisions of the Sentences Act also clashed with the rules of data processing. Checking the content of documents and letters received from persons and organs specified in Section 174(4) of the Sentences Act despite the prohibition of the law also infringes the right to the protection of personal data, because access to and processing of the personal data contained therein is unavoidable during the content check. In the case under investigation, the persons doing the checking unlawfully accessed the personal data of the Complainant, those of the attorneys of the Complainant acting in certain procedures and other persons who are party to the criminal procedures conducted against the Complainant and other procedures launched by the Complainant. The Authority established that an injuria related to the processing of personal data took place on the part of the Controller as members of its staff infringed Section 4(1) and Section 5(1) and (2) of the Privacy Act through the processing of the personal and criminal personal data in the checked documents located in the cell of the Complainant without an appropriate purpose and legal basis. Based on Section 56(1) of the Privacy Act, the Authority called upon the Controller to transform its practices concerning the checking of documents kept by detainees in the course of its security checks so as to comply with the protection of personal data and the provisions in Section 174(4) of the Sentences Act. Accordingly, when objects kept in the cells are checked, the documents of correspondence with persons and organisations subject to Section 174(4) of the Sentences Act (which may contain personal data) should be checked only to aim at establishing the sender and the addressee of the document. When the addressee is not the detainee concerned in the checking, additional checking may only aim at establishing whether the document was obtained by the detainee lawfully (e.g. in the

course of a court procedure as a result of disclosing documents to the detainee). [SZTF-149/2024.]

*II.2.3. Investigation into the lawfulness of the refusal of a request related to data requested from the Special Service for National Security for producing a private expert opinion*

A private expert notified the Authority that his principals requested him to produce a private forensic expert opinion as part of a criminal procedure, which necessitated contacting the Special Service for National Security (hereinafter: SSNS); the private expert requested SSNS to send various regulations, instructions and documents, (such as:

- rules of data protection and data security,
- rules on data security measures/instructions for IT security rules,
- rules for the organisation and operation, etc.).

To conduct the expert study, the private expert sent the following questions to SSNS:

- "Please, provide information on what technical device was used to make the sound recording as part of the technical data collection (secret surveillance of the IT system and its recording using technical devices) and what SSNS rules governed the transcription of a sound recording?
- What system do you use for forwarding data and in what way do you ensure data integrity and authenticity in the system?
- What technical errors may occur resulting in missing data from a report?
- In what way do you identify persons involved in the collection of data beyond any doubt?
- Are the original sound recordings deleted and if so, when, what is their storage period?"

According to the submission, SSNS refused access to the requested data and documents citing national security interests on the basis of Section 48(1) of Act CXXV of 1995 on National Security Services (hereinafter: National Security Services Act)[7].

The private expert requested an investigation whether SSNS acted lawfully by not making available the data and documents indicated in his requests and also requested the position of the Authority if this procedure of the SSNS can be re-

7 For reasons of national security interests or to protect the rights of others, the Director General of the National Security Service may reject requests to provide information on data processed by the national security services upon the request of the data subject, to erase their personal data from the records of data forwarding specified in Section 46, as well as requests for access to data of public interest processed by the National Security Service.

garded as lawful, in what way can a private forensic expert acting on the basis of an assignment have full access to the data needed to prepare his expert opinion, or whether it can be declared that access to data processed by SSNS is restricted by legal regulations.

SSNS notified the Authority that in his capacity as private expert, he requested organisational documents (e.g. data processing contracts), classified data (e.g. internal norms of regulations. statutes), and non-public data/data to be protected (e.g. data forwarding records) and finally, information to be protected in the national security interest (e.g. IT system "technical device used in the case of covert surveillance" from SSNS. According to SSNS, first and foremost it should be underlined that under Section 193(1) of the Criminal Procedures Act, the expert produces the expert opinion on the basis of the examination of data, documents and other means of evidence made available to him by the principal, and that SSNS is not party to the criminal procedure above referred to, and furthermore that the persons having commissioned the private expert – as persons otherwise having a wide range of rights as accused in a criminal procedure – have the legal opportunity to provide the information needed for drafting the expert opinion to the private expert within the framework of the procedure. In addition, according to the SSNS statement, it is clear that private experts have no power to make requests of mandatory force to organs or persons. However, the contacted party has the right and also the obligation to consider whether the requested information and documents can be issued based on a request from a citizen.

When adjudging the submission of the private expert, SSNS took the following criteria into account:

- From the viewpoint of the SSNS, the private expert sent his submission in a non-relevant role without any entitlement, requesting the transfer of documents containing in part or in full classified data or documents that were not public, access to which is restricted by law. In the case of classified data, it can be clearly established that the discharge of state/public tasks is conceptually excluded in the case of private experts, and the principle of need-to-know is also out of the question.
- In the case of certain documents, through which the private expert partly attempted to assess the national security activities of SSNS, the reason for rejection set forth in Section 48(1) of the National Security Services Act clearly prevails.
- Acting within its capacity as service provider, SSNS is not entitled to provide information related to personal and criminal personal data obtained as a result of the covert collection of information even for the purpose of

preparing a private expert opinion. This holds in particular with regard to the fact that the confidentiality of operative records is a prerequisite for secret service activities under the priority of the national security interest.

– The right to the protection of personal data is not an absolute right and therefore, in accordance with the principle of proportionality, a risk assessment was carried out by examining the reasonableness of the fact restricting the exercise of the right to access, on the basis of which SSNS decided to reject the request.
– According to SSNS's position, information obtainable from its records cannot be provided because it would jeopardise national security interests, which constitutes a sufficient basis for refusing to provide the information even in a case when the data request is made with a view to the preparation of a private forensic expert opinion.
– In summary, therefore, according to SSNS, the request for the documents and information was not related to the criminal procedure concerned, the private expert in this capacity has no powers to contact SSNS and, furthermore, this request to the SSNS was not made for the purpose of requesting data in the public interest and the request also affected classified data.

Pursuant to Sections 8(1) (a)[8] and (b)[9], 61 (1)[10], (2)[11] and (4)[12] of the National Security Services Act and the interpretative provisions of the Privacy Act concerning controllers and processors, SSNS participated in the criminal proceedings referred to above as a processor and not as controller, consequently, the organ commissioning SSNS qualifies as controller of the data SSNS obtained, to which the data request can be submitted. Pursuant to Section 61(2) of the National Security Services Act, SSNS forwards the data obtained to the principal organ and it has to erase the forwarded data from its records. In this context, it should be mentioned that the rights enshrined in Section 14 of the Privacy Act are also rights to which the data subject is entitled and according to Section 3(1)

8 The Special Service for National Security shall provide services, upon written request, within the limits of the relevant legal regulations, with the special means and methods of intelligence gathering and covert data acquisition, in support of organisations authorised to gather intelligence and acquire data covertly under the law.

9 As required by the organisations authorised under the law, the Special Service for National Security shall provide the special technical means and materials needed for intelligence gathering and covert data acquisition activities.

10 If secret intelligence gathering and the use of covert means is carried out as specified under Section 8(1)(a), obtaining the authorisation needed for carrying out the secret intelligence gathering and the use of covert means is the responsibility of the agency ordering their application. The ordering agency is responsible for the lawfulness of the application, while the Special Service for National Security is responsible for its implementation.

11 As part of its services, the Special Service for National Security forwards the data obtained as a result of the secret intelligence gathering or the use of covert means exclusively to the ordering agency and the forwarded data has to be erased from the records of the Special Service for National Security.

12 The provider of the data is responsible for the integrity of the communicated data, while the organ ordering the secret intelligence gathering and the use of covert means is responsible for the use of the data and for taking or failing to take the measures based on them.

of the Privacy Act, the data subject is a natural person identified or identifiable on the basis of any information. Pursuant to Section 17(3) of the Privacy Act, the controller may restrict or refuse granting the data subject's right to access under Section 17 of the Privacy Act in proportion to the objective to be achieved, provided that this measure is indispensable for securing an interest (such as the national security interest) specified in Section 16(3)(a)-(f) of the Privacy Act.

The Authority regarded the legal arguments of SSNS related to the refusal to issue the data and documents requested by the private expert as well-grounded and accordingly established that SSNS acted lawfully when rejecting the request. According to the Authority's position, Section 193(1) of the Act on Criminal Procedures provides the legal basis to the private expert acting on a commission to obtain the data needed for the preparation of his private expert opinion; however, the disputed data request exceeded its scope. In the absence of an injuria, the Authority terminated the investigation. [SZTF-407/2024.]

*II.2.4. Subpoena in a criminal procedure through personal delivery at the address of a close relative*

In a case, the Complainant presented that a police station delivered an "open document" on paper containing a subpoena addressed to him with a view to his interrogation as suspect in a criminal procedure (hereinafter Subpoena) to his mother living in a separate household, through which his personal data were disclosed to a person unauthorised to process them despite his intention and will, particularly in view of the situation that an interrogation as suspect and criminal proceedings were envisaged against the Complainant. The Complainant requested the establishment of the infringement of Section 113(2) and Section 130(1)(e) of the Act on Criminal proceedings by the police station through delivering the Subpoena as an official document not in a closed envelope and not to the registered address of the Complainant, but to his relative, which caused disadvantage and injury to the Complainant. In the course of its investigation, the Authority found that the police did not deliver the Subpoena to the Complainant's official address or an address provided by the Complainant in the course of the criminal proceedings, or to an address that could be defined as specific contact/place of delivery according to legal regulations. Furthermore, the Subpoena was not delivered to the Complainant in person, but to his mother at the mother's address, however, the Authority has not obtained clear evidence that would verify beyond any doubt that the Subpoena was delivered in a closed or open envelope, or in an envelope at all, hence it did not take a position on this issue. According to the statement of the police, the mother could not have access to

any personal data of the Complainant when processing the Complainant's personal data, which she would not have had already as a parent. According to the Authority's position, a mother naturally knows the personal data of her child (such as name, place and date of birth, etc.), but in this case the Complainant objected to his mother having access to his criminal personal data according to which the Subpoena was issued against him as a person reasonably suspected of having committed a criminal offence.

Section 3(4) of the Privacy Act clarifies the concept of criminal personal data[13], according to which all data relating to the data subject, i.e. to an identified or identifiable person who can be linked to the information, which is generated by organs authorised to conduct criminal proceedings or to detect criminal offences, can be considered criminal personal data,, so based on Section 5(7) of the Privacy Act, the rules on the conditions for processing sensitive data shall apply to the processing of criminal personal data. Based on the definition of criminal personal data it can be established that if a person, among others, is reasonably accused of having committed a criminal offence, he is subpoenaed as a witness or he is the injured party in the given case, qualifies as criminal personal data. It follows, therefore, that contrary to the statement of the police station, the mother gained access to criminal personal data by delivering the Subpoena to the mother, whose knowledge did not derive from her capacity as parent and, furthermore, the mother was not entitled to access such data.

The Complainant also requested the establishment of an infringement by the police station of Section 130(1)(e) of the Act on Criminal Proceedings by delivering the Subpoena not to the address of the Complainant, but to the Complainant's mother. Section 130 of the Act on Criminal Proceedings clearly requires the investigative authority to delivery subpoenas to the addressee when delivered by a courier. In the course of the criminal proceedings, the Complainant disclosed his registered address to the police station, i.e. the address to which delivery should have been made.

The police station claimed that there was no legal regulation prohibiting the delivery of an official document to a close relative. However, the imperative rules in the Act on Criminal Proceedings clearly determine the modes of delivery. Section 130(1)-(2) of the Act on Criminal Proceedings specified the modes of delivery to the addressee, while Section 131(1)-(7) of the same act presents the ex-

13 Criminal personal data means personal data, which can be linked to the data subject concerning his criminal records, generated by organs, authorised to conduct criminal proceedings or to detect criminal offences, or by the prison service during or prior to criminal proceedings in connection with a criminal offence or criminal proceedings.

ceptions to these rules in the context of which it should be mentioned that based on Section 131(3) the exceptions in Section 131(1)-(2) cannot be applied to this Subpoena. Section 136 of the Act on Criminal Proceedings provides for the delivery agent and cases of delivery to him. However, these rules of exception cannot be applied to this case and in the course of the criminal proceedings the Complainant had not designated a person who would have been authorised to receive his official documents instead of him. In the case of delivery by mail, the Act on the Post[14] and the Decree on the Post[15] specify the rules concerning receipt, including also the persons authorised to receive the mail, the possibilities of refusing receipt and the requirements of the documentation of receipt or refusal.[16] It is an incorrect argumentation on the part of the police station that there is nothing to prohibit delivery to a relative when the imperative rules concerning delivery were clearly stipulated. An overall assessment of the relevant rules reveals that in the case of delivery by an entity other than the mail service provider, there is no legal basis for delivering any package containing personal data to a person other than the addressee at an address other than the address in the public register (place of residence, place of stay, delivery address) or the contact specified by the person affected in the Subpoena and the specifically defined place of delivery (e.g. by way of a penitentiary institution[17], or service superior[18]) defined by legal regulations. In addition, the Act on Criminal Procedures also provides for the establishment of the personal and contact data of the participants of the procedure (such as the accused) and the Complainant provided the contact data to the police station in the course of the criminal proceedings.

The infringement of Section 130(1) of the Act on Criminal Procedures and Section 5(2) of the Privacy Act was established. In view of all this, the Authority called upon the police station to refrain from delivering official documents in a manner to a place of delivery as required by legal provisions and not directly to the addressee, or in the case of relevant specific authorisation by legal regulation through the persons specified therein. In addition, the Authority called upon the police station that in the event of the personal delivery of a Subpoena by the investigative authority to deliver the personal data included in the official document in the manner and to the person specified by the relevant legal regulations as a closed package and ensure the appropriate documentation of receipt, which it should store for the period set forth in the relevant filing rules with a view to

14 Act CLIX of 2012 on Postal Services (Post Act)
15 Government Decree 335/2012. (XII.4.) on the detailed rules for the provision of postal services and postal services in connection with official documents, as well as on the general terms and conditions of postal service providers and on items excluded from or conditionally delivered by postal services (Decree on the Post)
16 Decree on the Post: Sections 15(4), 16(3), 16(4), 19 and 20.
17 Act on Criminal Procedures Section 131(6)
18 Act on Criminal Procedures Section 131(7)

enforce accountability as a principle of processing. The police station complied with the call and notified the Authority of the measures taken in this context. [SZTF-427-2/2024.]

*II.2.5. Investigation into measures taken by the police and the subsequent procedures, police information provided to the press and processing by the healthcare institution providing care on the occasion of the measure*

The Complainant objected to the fact that during the hospital treatment of his injuries suffered in the course of measure applied by the police as a result of his physical resistance to the identification of his person, the police were present, they consulted the physician on duty and one of them took a photo of his medical record using his mobile phone without his consent. He also objected to the fact that the photo became part of several procedures, (such as misdemeanour proceedings, investigation by the commander, etc.), so the participants of these procedures also had access to its content. He disputed that the police measure taken against him was part of his identification. He also lodged a complaint that he did not receive information on the processing of his personal data in advance and also because the police made some of his data available to members of the press.

The Authority launched an investigation against the following controllers: Police Station 1 identifying the Complainant and in relation to this applying coercive measures, Police Station 2 performing the individual procedural acts and Police Station 3 conducting the procedure because of violation of obligations related to the verification of personal identity and the Hospital providing treatment to the person subject to the coercive measure. Although the Complainant disputed it, the Authority based the facts of the case on the documents of the police and the hospital in the course of its investigation that staff at Police Station 1 attempted to verify the identity of the Complainant on the date in question and eventually they did identify him. The Complainant also objected to the fact that policemen were present when he was receiving medical care without his consent.

According to the police controllers concerned, legal regulations render police presence mandatory in the course of medical treatment in such cases, as well as access to and processing of the medical records, for which they had another legal basis in compliance with legal regulations.

The Authority found that Sections 17(2) and 18(2) of Act XXXIV of 1994 on the Police (hereinafter: Police Act) provide appropriate legal basis for the police ob-

ligations related to the medical treatment of the Complainant. Also in view of the authorisation set forth in Section 81 of the Police Act, according to which the police shall process the data of the natural person affected by the measure linked to the case, the lawful purpose of the processing, including access to the data and the necessary forwarding of the data, can be established and the legal basis for the processing exists, The medical data accessed and processed by the police were related to the measure taken. The Authority also established that these provisions of the Police Act are in line with the provisions of Section 4(2)(h), (j), (k) and (l) of Act XLVII of 1997 on the Processing and Protection of Medical Data and Related Personal Data. Based on these provisions, medical data can be lawfully processed in the cases specified by law, such as law enforcement and under the authorisation granted by Act XXXIV of 1994 on the Police to discharge specific tasks for the purposes of crime prevention, administrative authority procedure, misdemeanour procedure and prosecutorial procedure. Accordingly, the medical data of the Complainant could be lawfully used in both the administrative authority procedure investigating the complaint against the identification and the coercive measure, and in the prosecutorial procedure launched subsequently.

Furthermore, the Authority examined other provisions of the Health Data Act and established that Section 14(1) authorises the presence of persons other than the physician and care providers in the course of treatment without the consent of the data subject, hence according to Section 14(1)(b) a regular staff member of the police may be present if the patient is a detainee and in view of the fact that the Complainant was still subject to a coercive measure restricting personal freedom at the time of the medical examination, the provision referred to also applies to the circumstances of his medical care.

The Complainant also objected to the consultation, which the police officers escorting him had with the physician treating him without his consent. In this context, the Authority established that the legal provisions already referred to authorised the transfer to and the processing of the data by the police, consequently, the transfer of the data and the fact of receiving the data without the consent of the data subject cannot be regarded as processing without a legal basis. The Complainant also objected to the fact that this consultation took place without his presence. In view of the fact that this was contradicted not only by the statements of the police controllers, but also by the content of the document submitted by the legal representative of the Complainant soon after the event, the Authority could not establish that this took place in the absence of the Complainant as part of the facts of the case. At the same time, the Authority pointed out that in view of the legal provisions, the presence or absence of the data subject is an irrelevant cir-

cumstance, the relevant legal regulations render the possibility of obtaining the data contingent not upon the presence or consent of the data subject.

The Complainant also objected to the fact that one of the police officers escorting him made a photo of his medical record. In view of the concordant statements of the Complainant and the police controllers and the documents substantiating these statements and enclosed by them, the Authority did not accept the Hospital's statement as the basis of the facts of the case, according to which the Hospital had no knowledge of the making of the photo, or of any data request concerning it; instead it was established as a fact that one of the police officers present at the examination made a photo of the medical record using his service mobile phone in order to obtain the data on it; however, no written request was drafted for this purpose and no such a request was given to the Hospital.

The Authority also pointed out that in the absence of searchable documentation (records), neither of the controllers, nor any staff member of the controllers can be expected to remember every single processing operation carried out after an extended period. However, in view of the fact that this natural human characteristic of the staff member acting on behalf of the controller cannot be the basis of depriving data subjects' rights of their substance, it is indispensable to document processing operations in such a way that they could be clearly traced back even after a longer period of time. Furthermore, the Hospital as controller can only verify the lawfulness of permitting the making of the photo as a processing operation constituting data transfer only if it is documented in accordance with the principle of accountability of the General Data Protection Regulation. It is for these reasons that the existence of a written request is necessary together with its receipt by the controller concerned and its documented (searchable) granting or rejection. After this, the Authority examined the provisions of the Health Data Act and found that they constituted the appropriate legal basis for obtaining the data in the course of the administrative authority procedure investigating the lawfulness of the police measure. The Health Data Act regulates the mode of the request and its granting; according to this, the purpose of requesting data and the range of the requested data must be indicated and making the photo without such a written request failed to comply with these legal requirements.

The Complainant also objected to the fact that the police processed his medical data not related to the case in question. In the context of the processing these medical data by the police, the Authority found that they carried information to be taken into account and to be evaluated in the course of the police and prosecution investigations of the injury caused in the course of the identification; conse-

quently, their processing by the police is compliant with the principle of purpose limitation. In view of all this, the Authority established that the police was authorised to process the data in the medical records; at the same time, it stated that the method applied to obtain the data and the information was not compliant with the provisions of the data protection and procedural regulations and do not enable the exercise of data subject rights and it also infringes the principle of accountability.

The Authority also examined whether the photo of the medical record was still accessible on the service mobile phone and whether it was accessed by any third person. According to the statement of the police controller, nobody other than the police officer making the photo had access to it, and it was erased following the drafting of the report, but it was not documented. No evidence to the contrary was furnished in the course of the procedure, and the Authority accepted the content of these statements as factual as the basis of the facts of the case. In view of the fact that the circumstances of erasure (e.g. its time, mode, etc.) may have significance in a given case, it is necessary to draft a document concerning the erasure even if erasure is an operation easy to carry out in practice. The Authority noted that the necessity to draft documentation does not necessarily mean that a separate protocol should be made up, and in the given case, after considering the circumstances by the controller, it may be appropriate to include the relevant data in a document, such as a police report documenting the downloading of the photo and enclosed with that file, which qualifies as a public deed.

The Complainant also objected to the fact that an unauthorised journalist learned of the event from the police officer concerned and their legal representative, after which the journalist contacted the press officer of the police headquarters, detailing the case, which was confirmed by the press officer of the police headquarters. He also complained that several other media outlets also had access to this information, which they published after or without contacting the press officer of the police headquarters. Similarly to the information provided to the Complainant, the police headquarters stated to the Authority that the Communications Department of the police headquarters did not disclose the personal data of the Complainant (including the data with which the Complainant could have been clearly identified, excluding his name) to the representatives of the press; they provided information only about the fact that there was a case, of which the journalist obtained the news. The investigation found that the journalist obtained the information from the representative of the police union, who was contacted by the police officers requesting help for themselves. The police

officers requesting help from their trade union obviously did not act on behalf of the police headquarters or any other police organisation, hence what they said could not be regarded as an official statement by the police, consequently, it could not be established whether the trade union or the representatives of the press were informed of the case of the Complainant by the police headquarters or any other police organisation. The Complainant also objected to the fact that he did not receive information on the processing of his personal data in advance. In this context, the Authority found that the link to the Privacy Statement was available at the end of the letter written by the data protection officer of the police headquarters to the Complainant, through which the Privacy Statement could be accessed by type of case; hence the information became available to the Complainant at the latest at this time. Nevertheless, the infringement of the right to prior information was established in the course of the investigation, as the said subsequent information was provided at the request of the Complainant. Based on Section 16(1)-(3) of the Privacy Act, the prior information should have been provided when the police took the measure, in such a way that the information on the processing is shown on the document handed over by the police officers concerning the measure or at least a reference to the electronic accessibility of the content of the processing in relation to the given procedure is available on the police website. The investigation did not establish any infringement in relation to processing by the Police Headquarters and it found that the Police Headquarters informed the press of the case in question without disclosing the personal data of the Complainant.

As to processing by Police Station 2, it was found that as the police officers taking action against the Complainant for his refusal to identify himself took him to Police Station 2 for the purpose of short-term arrest, the staff of this police station doubtless processed certain personal data of the Complainant in relation to the tasks they carried out. These did not include the medical data of the Complainant. According to the data available to the Authority, the processing complied with the principles of lawfulness and purpose limitation and had the appropriate legal basis under Section 5(1)(a) of the Privacy Act and Section 1(1), 2(2) and (5), and Section 13(1) of the Police Act. In view of the above, the processing by the Police Headquarters and Police Station 2 did not result in an infringement, nor was there an immediate threat thereof, hence the Authority closed the investigation vis-à-vis these two controllers.

With respect to Police Station 3, it was found that the use of the medical data of the Complainant was not necessary in the misdemeanour procedure conducted by it, and they were not used. The legitimate purpose of processing health-relat-

ed personal data in the documents sent to Police Station 3 by another controller (in the absence of competence) was exclusively compliance with the provisions of the Archives Act with respect to documents sent by another controlling police organ and its legal basis was Section 5(1) of the Archives Act. All this can only mean the safekeeping of these data in accordance with the archive rules for the appropriate period and then the annihilation of the documents. To that end, the Authority called upon Police Station 3 to terminate the risk of infringement by blocking the documents containing medical data among the documents of the misdemeanour case until they are annihilated and not to perform any processing activity on them apart from storing them and annihilating the data carriers.

The Authority established that making a photo of the document containing medical data using a service mobile phone, the undocumented erasure of the photo, allowing for all this by the Hospital as data transfer infringed the law. The Authority called upon the Hospital not to allow for the direct recording of the personal data of a person undergoing treatment by another person without information on the purpose of use in an undocumented manner, instead to inform the person wishing to record the data that a written request to that effect would be accommodated, provided that the conditions set forth in legal regulations are met. Because of the unlawful processing operation implemented by making a photo of the medical data of the Complainant and the infringement of the right to receive prior information, the Authority also called upon Police Station 2 to transform its procedures so as to discontinue the infringing practices established by the investigation. [SZTF-339/2024.]

*II.2.6. Ex officio audits*

In the first half of 2024, the Authority carried out ex officio audits at the 5th District Police Station of the Budapest Police Headquarters and at the Airport Police Directorate; the purpose of these supervisory activities was not only to examine compliance with the Schengen acquis and the national rules, but also to prepare both the controllers and the staff of the Authority for Hungary's Schengen evaluation concerning data protection in July 2024.

At the 5th District Police Station, the staff of the Authority inspected the advanced Nova Mobil, with which search for various categories can be run (e.g. person, vehicle, document, subject matter) in the Schengen Information System. In addition to the issues, which are mandatorily checked at supervisions on the use of the SIS system, the Police Station's staff delivered a presentation on SIS query process. Searches for facial images can be carried out only on the basis

of Section 29(4) of Act XXXIV of 1994 on the Police (hereinafter: Police Act) and Act CLXXXVIII of 2015 on the facial image analysis records and the facial image analytical system if personal identity cannot be established or credibly verified in any other way. In other words, searches may be run exclusively to establish or verify personal identity and only linked to a specific measure. The query process in the Nova Mobil application was also presented. Searches for facial images are rarely run, only if a person cannot be identified in any other way, or obviously erroneous data are provided in the course of the verification of identity.

In the course of the onsite inspection of the Airport Police Directorate, the Authority's staff was primarily interested in the development projects taking place since the last supervision whether the transition to the new Schengen Information System was successfully implemented with regard to all elements of the system and whether any security event concerning personal data took place in the SIS system in the period following the SIS recast (7 March 23). The staff of the Airport Police Directorate reported on the development of the NHERR system and on the development plans for the so-called Automatic Border Control (ABC) gates and that they expected to acquire additional camera towers for the Entry-Exit System (EES) and the ETIAS system. In relation to the planned implementation of EES, they explained that third country citizens will have to create a personal folder upon entering the Schengen area for the first time with the help of the dedicated KIOSKs; this will require the recording to two biometric data; as from the second entry, only the existing data will have to be reconciled and one biometric data will have to be recorded. On site, the Authority's staff observed the operation of the ABC gates, the use of the SIS and VIS systems, as well as the processing of passports in the course of admissions.

## *II.3. Reporting data breaches*

This year, the Authority received 577 new data breach reports, showing a minor increase relative to the preceding year.

### *II.3.1. Significant data breaches subject to the General Data Protection Regulation*

*1. Data breach in the course of processing by a healthcare institution*

The Authority learned from the press that a substantial quantity of medical records including personal data are stored in a closed building of a healthcare institution, and has therefore launched an authority procedure for data protection ex officio.

Earlier, the controller noticed that there have been presumably regular unauthorised intrusions in the closed building and some of the medical records were scattered in the building. The controller lodged a data breach report with the Authority; however, seven days passed between the identification of the event as a data breach and its reporting to the Authority. In view of the sensitivity and the volume of the personal data concerned, the data breach was qualified as high risk, which warranted that the data subjects should also be notified. However, the controller did not take care of this without undue delay referring to the absence of the data necessary for the identification of the data subjects. The Authority did not accept the reasons of the failure to provide information.

In its decision, the Authority established that the controller failed to meet its obligations set forth in GDPR Articles 32(1)(b) and (2) and infringed GDPR Articles 33(1) and 34(1). Because of the established infringements, the Authority imposed a data protection fine of 2 million forints on the controller. [NAIH-295/2024]

*2. Data breach in the course of processing by an ambulance service*

An ambulance service (Controller) learned from the press that a case form generated in the course of a rescue operation was disclosed to the public in an article published on an internet news portal. There were differences of content between the case form and the document published in the press, at the same time, the document published by the press included data, which were originally recorded on the case form. In view of this, it was established that a document on which the case file was based was made public, based on the knowledge of the

rescue event and the data in the case form, which implies that the person who forwarded the document to the press viewed the case form in the system of the Controller.

Most of the data were blocked out in the document published in the press. When the ambulance unit arrived, the patient was no longer at the scene, hence the patient was indicated as an unknown person on the case form and none of his personal data were recorded apart from his age. The circumstances of the case led to the conclusion that the personal data made public could only be leaked from the system of the Controller.

The Controller established the data breach, which, however, did not affect health-related personal data. The data subjects of the data breach were staff members of the Controller, whose personal data were unlawfully leaked from the system. The Controller made a record of the breach and reported it to the Authority within 72 hours of becoming aware of it; it appropriately assessed the risks and informed the ambulance staff concerned. In view of this, the Authority established that the Controller complied with its obligations set forth in GDPR Articles 33 and 34 in relation to the data breach.

The internal investigation by the Controller could not unambiguously establish how many persons viewed the case form and for what purpose once it was recorded. In view of this, the Authority established that the Controller failed to meet the requirements included in its own internal rules because its logging system was unsuitable for the subsequent comprehensive review of user operations and in the event of an infringement for the establishment of responsibility.

In view of the above, the Authority established that the Controller infringed its obligations set forth in GDPR Article 32(1)(b) and 2 . Having taken all the circumstances of the case into account, the Authority did not deem it justified to levy a fine. [NAIH-9469/2024]

3. *Data breach in the course of processing the data of private persons applying for adult training*

On 24 January 2024, a non-profit limited liability company (Controller) reported an intermittent data breach to the Authority, according to which it noticed a data breach on the website operated by it: the sub-sites of the website intended for the individual administrators temporarily became accessible to internet brows-

ers, hence the data of private individuals applying for adult training courses organised by the Controller were leaked, and unauthorised individuals may have had access to them. The data leakage was caused by a configuration error. The number of persons affected by the data breach was 10 to 50, the users of the website and those subscribing to the training courses; the leaked personal data were largely data on personal identity and contact data. The controller notified the data subjects by phone and e-mail of the data breach immediately after becoming aware of it.

As a result of this procedure, the Authority established that the Controller acted in compliance with the provisions of GDPR Articles 33-34 when managing the data breach; however, it could have been avoided had the client carried out the configuration of the web server, regular logging and event monitoring and testing in a separate test environment. In view of this, the Authority established that the Controller infringed the principle of data security incorporated in GDPR Article 32 and issued a warning. [NAIH-5446/2024]

*4. Data breach in the course of processing by a family doctor service*

Upon request, the Authority investigated the lawfulness of processing by a family doctor service. Beginning in July 2022, the family doctor service queried the medical data of the data subject accessible in EESZT on several occasions over several months. The data subject visited the family doctor service complained against only once in 2011 because he belongs to another family doctor service. During the authority procedure, the head of the family doctor service stated that he had no knowledge of any unauthorised viewings and he did not query the medical data of the data subject.

In the surgery of the family doctor, the direct assistant of the family doctor also had access to the family doctor software. The assistant acknowledged that she had access to the medical data of the data subject and viewed them. Apart from curiosity, she had no reason for this. She did not forward the queried data to any third person and did not query the data of any patient other than the data subject. She did not have a separate password for the family doctor software; her employer only gave her the password for work-related use.

The Authority established that neither the family doctor service, nor the assistant were authorised to access the medical and related personal data of the data subject, hence they infringed Article 6(1) of the General Data Protection Regulation. The Authority also established that the family doctor service infringed the ob-

ligation set forth in GDPR Article 33(1) as it failed to notify the data breach to the Authority without undue delay having learned of it and because of this the Authority issued a warning. The Authority also established that the assistant as an independent controller committed a data protection infringement with her deliberate behaviour and imposed a data protection fine of HUF 50,000 on her. [NAIH-4082-5/2024]

*II.3.2. Data breaches subject to the Privacy Act*

*Failure to take measures ensuring restricted processing of personal data on the part of a prosecutor's office*

The prosecutor's office issued copies of documents to a suspect and his authorised defence attorney. The document issued contained the personal data of a judge as witness and also injured party, who had requested the restricted processing of his personal data, including his date and place of birth, mother's name and address, without blocking them. The Authority launched an authority procedure for data protection because of deficient data security arising from the failure to implement a measure ensuring the implementation of restricted processing. According to the statement of the prosecutor's office, in the case of the restricted processing of personal data the restricted personal data are not shown in the protocol enclosed with the documents, they are recorded in a separate document, or the protocol signed and complete with the personal data is put in a closed envelope, which may only be opened by the authority taking action. The administrative system does not separately mark the fact of restricted processing. No internal rules concerning the issue of document copies were made at the prosecutor's office. When issuing document copies, the prosecutor's office acts according to the relevant provisions on the Act of Criminal Procedure in the case of restricted processing. The rules of document management applicable also to clerks of the prosecutor's office are governed by a supreme prosecutor's instruction 26/2018. (XII. 28.) LÜ on the document management rules of the prosecutorial organisation (hereinafter: LÜ instruction); furthermore, the tasks of the clerks are detailed in their job specification. Pursuant to Section 37(2) of the LÜ instruction referred to, documents shall be forwarded in such a way that the official copy of the prosecutorial measure be forwarded in accordance with the instruction issued by the administrator of the case. In the course of expedition, the office manager has to check whether every instruction related to the issue of the document was carried out and whether the annexes were enclosed. A disciplinary procedure was launched at the prosecutor's office on account of the data breach and the disciplinary responsibility of the clerk was established.

The Authority established that in the course of its procedure, the prosecutor's office infringed certain data security provisions of the Privacy Act by not ensuring the prevention of unauthorised access to personal data to be processed in a restricted manner when forwarding the data as it failed to implement the measure ensuring the restricted processing of the personal data of the injured party, as well as the application of the control mechanism ensuring this as an appropriate data security measure, hence both the suspect and the defence attorney had unauthorised access to the personal data of the injured party, which should have been processed in a restricted manner. In view of all this, the Authority decided to levy a data protection fine of HUF 5,000,000, that is, five million forints on the prosecutor's office. In imposing the fine, the Authority considered as a mitigating circumstance the measures taken by the prosecutor's office after the breach, but took into account as an aggravating circumstance failure to protect the data of the injured party precisely in a case because of a violent crime against a public official [SZTF-124/2024.].]

# III. Freedom of information

## *III.1. The Authority's monitoring procedures and meeting the RRF commitment*

In order to implement the reform under the Improvement of transparency and access to information of public interest (milestones 229 – 233) of Hungary's Recovery and Resilience Plan C9.R26, it is necessary to draft reports on semi-annual periods for the second half of 2022 and thereafter each year until the first half of 2026 (altogether eight reports need to be published under the commitment).

Under the European Commission proposal COM (2022) 686, in order to achieve milestone [C9.R26.] for the improvement of transparency and access to information of public interest, Act CI of 2023 on the system of the utilisation of the national data assets and certain services added a new chapter VI/B. to the Privacy Act, which gave a new function and powers to the Authority and in connection to this specified an extended reporting obligation for organs performing public tasks. Pursuant to the provisions of the law, organs performing public tasks, including municipalities and business organisations in public ownership in particular, have to provide data on the preceding year from 2024 by 31 January of each year on
a) the number of meeting and rejecting requests to access data of public interest and data accessible on public interest grounds and the characteristic reasons of rejection,
b) the average number of days needed to meet requests to access data of public interest and data accessible on public interest grounds, and
c) the accurate internet accessibility of the location where data of public interest and data accessible on public interest grounds are published (hereinafter: freedom of information reporting).

Pursuant to Section 30(3) of the Privacy Act, organs performing public tasks shall, as before, keep records on the requests refused and the reasons for refusing them. In addition, pursuant to Section 42 of Government Decree 335/2005 (XII. 29.) on the general requirements of document management by organs discharging public tasks, requests for data of public interest received by such organs will have to be filed so as to be searchable by subject matter. These records constitute the primary basis of the present reporting; however, if warranted, an organ may keep separate records in order to meet a reporting obligation.

The reporting constitutes one of the fundamental pillars of discharging its tasks of monitoring compliance with the requirements concerning the transparency and accessibility of data of public interest and data accessible on public interest grounds for NAIH. This is the so-called monitoring procedure. The new, extended freedom of information reporting obligation exists from 1 January 2024.

In addition to the above, based on Section 71/D of the Privacy Act, the Authority shall have to carry out the following tasks as part of freedom of information monitoring:

- it has to monitor the obligee organs twice a year based on the reporting. Monitoring by the Authority extends to the examination of the public disclosure of data of public interest and data accessible on public interest grounds,
- based on notification, the Authority also conducts separate monitoring,
- the Authority may request data from the monitored organs for monitoring; the monitored organs are required to comply with such requests within 8 days from receiving the request,
- the Authority may make recommendations to the monitored organs with a view to promoting compliance with the requirements for transparency of data of public interest and data accessible on public interest grounds and for their accessibility,
- the head of the organ affected by the recommendation has to draw up an action plan for the implementation of the necessary measures and transmit this plan to the Authority within 15 days from receipt of the recommendation,
- as part of its public report, the Authority has to draw up a report annually on the monitoring.

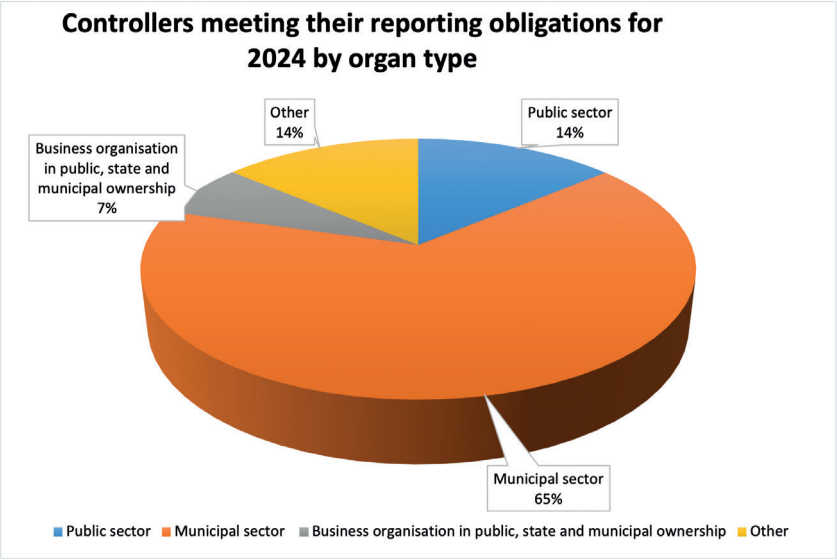
*III.1.1. Statistical data of freedom of information reporting*

By 31 January 2025, the Authority received reports for 2024 from **5,952** obligee organs covering the following organ types:

– state-owned business organisation, state public authority, state public institution, budgetary organ according to the Act on Public finances, legal entity in the register of the state treasury, public body (**public sector**);
– local government, body of representatives and its organs, budgetary organs founded and supervised by the local government, minority governments and their organs (**municipal sector**);

– non-profit business organisation in public ownership, state-owned business organisation performing public tasks specified in legal regulation, state-owned business organisation or municipal business organisation operating with a share in state ownership to be kept in national assets of outstanding significance for the national economy (**business organisation in public and state ownership**);
– institution maintained by the church, KEKVA (Asset Management Foundation of Public Interest), public foundation, priate law organisation discharging public task, legal entity established by law, other (**organs discharging other public tasks**).

The following figure contains the breakdown of reporting organs by organ type.

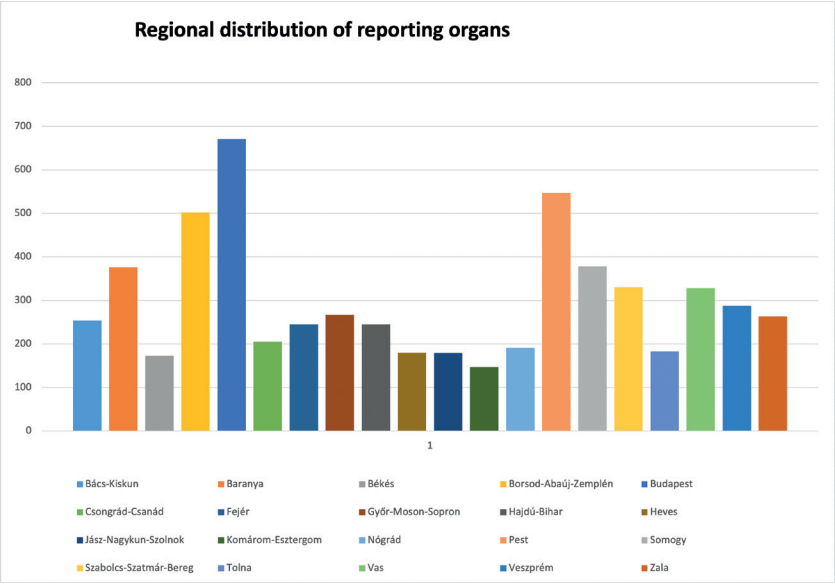



The number of those providing reports continues to be characterised by a rising tendency, as early in 2023, then in 2024 and in January 2025, reporting obligations by the due date specified by law (31 January 2025) were met by 1,350, 5,895 and 5,952 organs performing public tasks (for 2022, 2023 and 2024), respectively.

Local governments and minority governments together with their organs in the municipal sector had the largest cardinality.

With regard to 2022, 584 local governments and their organs and 25 minority governments submitted reports [altogether: 609] – at the time only on the data of rejected data requests. Extended reports on the year 2023 were submitted by 2,612 local governments and their organs, 870 budgetary organs founded and supervised by local governments and 301 minority governments and their organs to the Authority, totalling: 3,783 reporting municipal organs.
With regard to 2024, as many as 2,165 local governments and their organs, 1,220 municipal budgetary organs and 436 minority governments and their organs – altogether: 3,821 organs – met their reporting obligation.

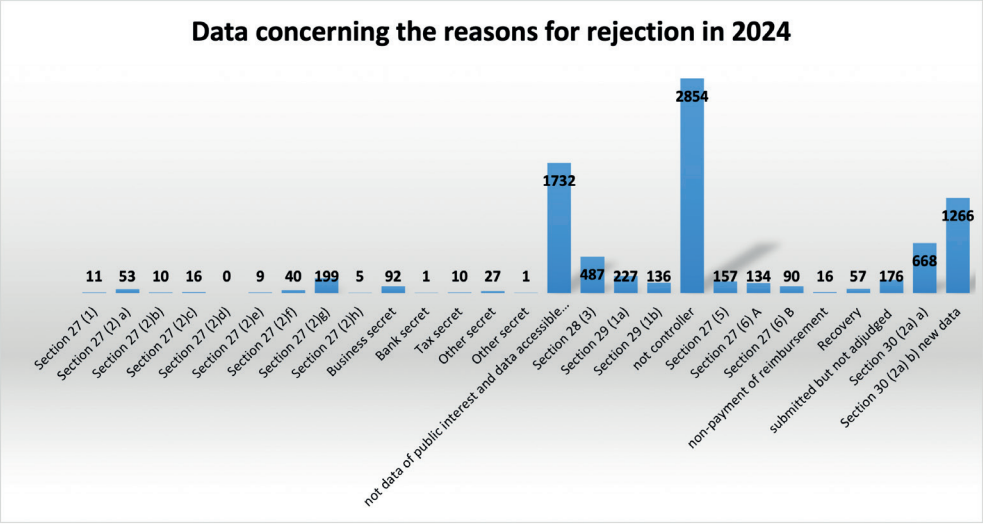
Based on the regional distribution of reporting organs, Budapest submitted the largest number of reports (871), followed by Pest County (547) with Komárom-Esztergom County bringing up the rear (147).




Similarly to the increase in the number of reporting organs, the ratio of requests for data of public interest met and rejected showed a positive change relative to the data of the preceding years:

- in 2023, 3,260 of the 9,739 data requests (33%) with regard to 2022 was closed with the restriction or exclusion of access to data of public interest,

- in 2024, the controller organ performing public tasks declined to grant access to data of public interest in 6,210 cases (21%) of the 14,840 data requests in the reports of 2023, involving 30,238 data types,
- in 2025, organs discharging public tasks had to report on their annual data disclosure practices in a semi-annual breakdown in their reports on 2024. Based on aggregated data, organs discharging public tasks granted access to data in 12,548 datasets out of 16,806 [75%], while access to 4,256 datasets [25%] was refused in the first half of 2024. According to the data on the second half of 2024, data were released in the case of 9,787 datasets out of requests for 14,004 [77%], but the controller rejected access to 4,215 datasets [23%]. **The aggregation of the semi-annual data shows that requests for access to the various datasets were granted in 76% of the cases and rejected on average in 24% of the cases**. A comparison of the data for 2023 and 2024 reveals a slight increase in the ratio of rejections.



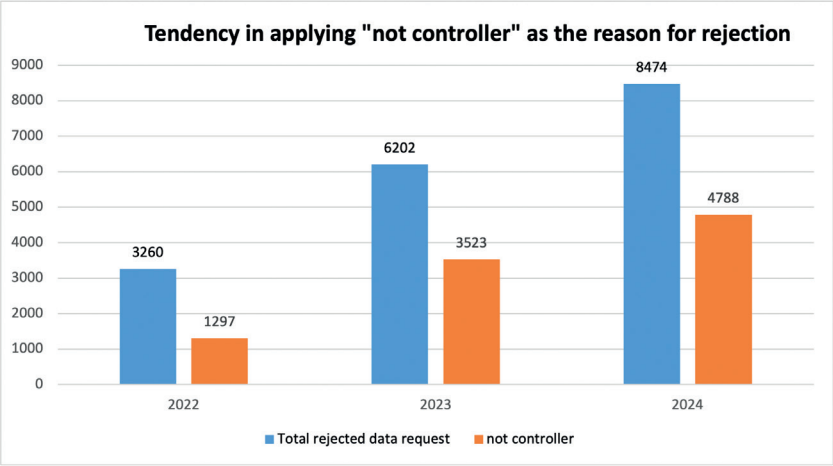
The reasons for rejections applied most frequently in preceding years (2021, 2022, 2023) [data not in the public interest, personal data not accessible on the grounds of public interest, not controller] continued to be at the head of the list in the 2024 reports too.

Essentially, the two new reasons for rejection introduced by Section 30(2a) (a) and (b) of the Privacy Act in force since 1 January 2024 can be interpreted as the same as the reason for rejection "*not controller*".

Pursuant to these provisions, the organ performing public duties shall not be obliged to comply with the data request, if meeting the request would necessitate

a) procuring or collecting data other than those the organ performing public duties effectively processes, including in particular data that are processed by an organ performing public duties under the direction or supervisions of the former, or
b) producing new data relative to the data it processes by comparing data of public interest or data accessible on public interest grounds effectively processed by the organ performing public duties.

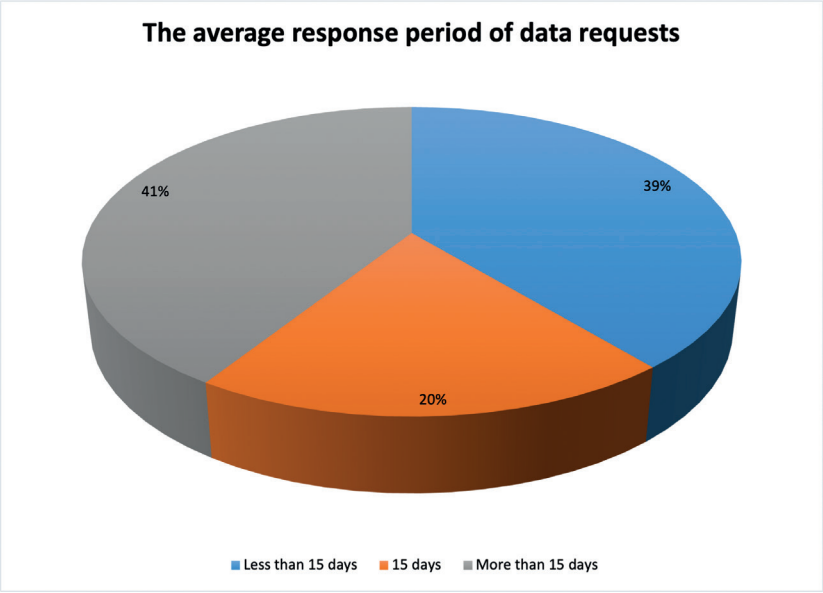
Based on the statistical data, however, this change did not involve an increase in the ratio of rejected data requests with reference to the new reasons for rejection. Whereas in 2023 the reason for rejection that the given organ did not process the data to be accessed made up 57% of all the reasons for rejection, in 2024 references to the two new reasons for rejection and to the "not controller" status together also constituted 57% of the reasons for rejection.



The report extends to determining the average number of days spent on meeting the data requests in a given year. In 2023 and in 2024, 63% and 83% of the reporting organs made so-called “zero” statements, respectively (they did not receive data requests). **In 2024, the average number of days spent on meeting data requests was 12.5 in the case of organs performing public tasks, which did receive data requests**.

In the case of organs, which received data request (first half of the year: 1,030, second half of the year: 1,035), the average response period was as follows:

- the average response period was 15 days in the case of 20% of the organs [213 organs],
- the average response period was less than 15 days in the case of 39% of the organs [394 organs],
- the average response period was more than 15 days in the case of 41% of the organs [425 organs].



*III.1.2. Monitoring procedures to verify the adequacy of the provision of access to data and to examine the practice of meeting individual data requests*

In 2024, the Authority launched monitoring procedures to verify the adequacy of the transparency and accessibility of data of public interest and data accessible on public interest grounds in 53 cases based on Section 71(D)(1) of the Privacy Act. In five cases, this was done based on complaints lodged or freedom of information supervision already in progress and in 48 cases ex officio.

In the case of ex officio procedures, the Authority relied on the data of the reports for 2023 in accordance with Section 71(D)(4) of the Privacy Act; as set forth in the monitoring schedule for 2024, the monitoring affected

– the reporting organs selected on the basis of their reports, where the selection criteria included, inter alia, the rejection of a large number of data requests or if the period open for meeting the data requests substantially exceeded the 15 days required by law;
– selected organs of the central public administration, and
– organs performing public tasks concerned in supervisory procedures launched on the basis of individual complaint, but which were unsuccessful.

The organs performing public tasks monitored in 2024 were the following: *Szerencsejáték Zrt., Dobó István Vármúzeum, Eger MJV Önkormányzata, Újszentiváni Polgármesteri Hivatal, Fejér Vármegyei Katasztrófavédelmi Igazgatóság, HUN-REN Társadalomtudományi Kutatóközpont, Budapest IV. kerület Újpest Önkormányzata, BAZ Vármegyei Központi Kórház, Ópályi Község Önkormányzata, Szabadszállási Roma Nemzetiség Önkormányzat, Tolna Vármegyei Kormányhivatal, Budapest Főváros Kormányhivatal, Pusztadobos Község Önkormányzata, Szomolya Község Önkormányzata, Marcali Város Önkormányzata, Penészlek Község Önkormányzata, MÁV-START Zrt., Győr MJV Önkormányzata, Nógrád Vármegyei Kormányhivatal, Nagynyárád Község Önkormányzata, Szabadszállás Város Önkormányzata, Győr MJV Polgármesteri Hivatala, BTVR Budafok-Tétényért Városfejlesztő Kft., Vilmányi Közös Önkormányzati Hivatal, Pálháza Város Önkormányzat, Hollóháza Község Önkormányzata, Miskolc MJV Polgármesteri Hivatala, Csepeli Önkormányzat, Csepel Polgármesteri Hivatala, KÉZMŰ Közhasznú Nonprofit Kft., ERFO Közhasznú Nonprofit Kft., Dunaújvárosi Vagyonkezelő Zrt., Székesfehérvár Városgondnokság Kft., HungaroControl Zrt., Debrecen MJV Polgármesteri Hivatala, Alacska Község Önkormányzat, Zala Vármegyei Kormányhivatal, Óbuda-Békásmegyer Önkormányzata, Jász-Nagykun-Szolnok Vármegyei*

*Kormányhivatal, Közép-Budai Tankerületi Központ, Hódmezővásárhelyi Tankerületi Központ, Pécsi Tankerületi Központ, Debreceni Tankerületi Központ, Nagykanizsai Tankerületi Központ, NNGYK, Közép-Pesti Tankerületi Központ, Szolnoki Tankerületi Központ, Kecskeméti Tankerületi Központ, Salgótarjáni Tankerületi Központ, Veszprém Város Önkormányzata, Veszprém Város Polgármesteri Hivatala, Litér Község Önkormányzata, Litér Közös Önkormányzati Hivatal*.

In the course of the monitoring procedures, the Authority examined not only the requests for data of public interest submitted to and adjudged by the monitored organ in 2023 and the responses given to them; it also reviewed the procedures of the monitored organs granting access to data of public interest. In addition, it also requested the submission of judgments made in public data litigations related to the rejection of access to the data, if there were any.

The majority of the organs discharging public tasks cooperated with the monitoring and responded to the Authority's questions within short periods, accepted the Authority's recommendations and produced action plans to remedy the observations made in the recommendations, which in many cases included factors that have been accomplished simultaneously with sending the action plan. At the same time, there was an organ performing public tasks, which showed a total lack of cooperation and not even the involvement of its supervisory organ into the procedure altered their attitude to the monitoring. The monitoring extended to the examination of the lawfulness of the extension of the period open for responding and of the call to clarify the data request, the appropriate application of the restriction on accessing the data referred to in the course of rejecting the data request and the existence of information on the right to legal remedy.

The Authority summarised the deficiencies exposed in the course of the monitoring procedures, its recommendations and the results of the monitoring in the individual reports published in full on its website.[19]

Presumably, the impact of the monitoring procedures will be perceptible in the coming year(s) as the new procedures implemented to eliminate the deficiencies exposed in the data release practices of the individual organs will have to be incorporated into their everyday practice and its effective outcome will be determined on the basis of the examination of the data release practices of the coming year/years and the analysis of the freedom of information reports.

19 https://naih.hu/monitoring-jelentesek-menu-heading/kozerdeku-adat-kiadasi-monitoring

*III.1.3. Monitoring procedures supervising the publication practices of organs performing public tasks*

In 2024, the Authority launched 74 monitoring procedures examining publication practices, in 43 cases based on notification and in 31 cases ex officio. In the ex officio procedures, the Authority started off from the results of its previous comprehensive project aimed at the improvement of the efficiency of the freedom of information; hence it supervised the publication practices of ministries, government offices and publicly held business organisations.

Section 37(1) of the Privacy Act requires organs performing public tasks to publish the data specified in the *general publication schemes* of Annex 1 thereto as specified in Annex 1. Hence, in its monitoring procedures supervising compliance with the publication obligations, the Authority checked not only whether an organ published every single item of the required data, but also whether the publication took place in the structure according to Annex 1 to the Privacy Act, or Annex 1 and 2 of IHM Decree 18/2005. (XII.27.) (hereinafter: IHM Decree) in the required place with the updates at the required frequency and in keeping the necessary retention periods.

The purpose of the general publication schemes specified in Annex 1 to the Privacy Act is that interested parties be able to quickly find the organisational, operational and financial management data of organs performing public tasks, which the legislator defined as the proactive minimum of the freedom of information collected in one place on the website of the organ in a specific way and with specific content. It is a common – but not acceptable – practice to publish the data of the general publication scheme in a fragmented mode in different parts of the organ's website. Another unacceptable practice is when interested citizens have to find out what is the search word using which they can find the data of the general publication schemes in a database containing data other than the data of the list. Nevertheless, the Authority encountered this solution on several occasions.

In 2024, the Authority examined the publication practices of 9 ministries; it published seven reports on the results of the monitoring procedures, while two procedures were still pending early in February. At the start of the monitoring procedures, not a single ministry had general publication schemes, which would have been drawn up in the structure according to Annex 1 of the Privacy Act, or Annexes 1-2 of the IHM Decree.

Ministries publish data of public interest in a joint document library, which can be searched by ministry organisational and staffing data, activity and operation related data and financial management data. The date of publication can also be set as a filter; search words can also be used. A typical deficiency at the time of launching the monitoring procedure was that the Document Library did not contain a scheme according to Annex 1 of the Privacy Act, one can only search and use filters in it. Filtering for "Organisational and staffing data", "Activity and operational data" and "Financial Management data" at the same time failed to produce all the data lines according to Annex 1 of the Privacy Act (or folders with corresponding names). The documents accessible in the Document Library do not fully contain the data listed in Annex 1 to the Privacy Act or Annex 1 to the IHM Decree; several ministries hardly published any data of public interest other than the statements of assets and the remuneration for senior political leaders in the Document Library. The Authority called upon the ministries to notify the Authority of the accurate place of publishing the required data by completing the enclosed Annex 1 to the Privacy Act; every ministry complied with this call. After this, the Authority sent a detailed analysis of the missing data and the erroneous publication to the ministries and requested action plans indicating the persons responsible for corrections and a period for completion not longer than 30 days. The Authority summarised its recommendations, the results of the monitoring and the remaining deficiencies in the reports published in full on its website.

All in all, it can be stated that, with the exception of a single ministry, the monitored ministries still failed to publish all the data of public interest required in Annex 1 to the Privacy Act either in the Document Library or in a table format. As a result of the procedure, two ministries uploaded the list according to Annex 1 to the Privacy Act in a table format [NAIH-2405/2025, NAIH-2851/2025]; one of the ministries did so with minor deficiencies. Another ministry uploaded virtually without fail the required data of public interest to the Document Library [NAIH-10195/2024], in this case there was no need to draw up an action plan. Two ministries did publish more data as a result of the procedure, but several datasets were still missing [NAIH-2839/2025, NAIH-2851/2025]. Three ministries made minimal additions or did not upload the missing data at all [NAIH-2836/2025, NAIH-1686/2025, NAIH-2842/2025].

Besides the ministries, the Authority found that several county government offices did not have general publication schemes drawn up in the structure according to Annex 1 to the Privacy Act or the IHM Decree, instead they uploaded data of public interest to the menu "Documents, forms" on the central site of government offices. Because of this, the Authority conducted monitoring procedures against

five county government offices in 2024. Four procedures were closed with reports; one procedure is still pending. In the four closed procedures, three government offices published the general publication schemes in the table structure according to Annex 1 of the Privacy Act; one government office already had a scheme – albeit deficient – upon launching the procedure. Two government offices uploaded a larger number of missing data, even though not in full [NAIH-2786/2025, NAIH-3003/2025]; in the case of one government office a major data range continues to be missing [NAIH-1640/2025]. The government office with the deficient scheme made up for the missing data almost in full already at the beginning of the procedure, hence there was no need for an action plan [NAIH-1642/2025].

The Authority monitored the publication practices of a number of municipalities, in most cases based on notification. These procedures showed a varied picture: there were municipalities, which had general publication schemes, but with many data missing; there was one, which had not updated the scheme for two years, and there was another one, which did not even have an operational website, so they did not publish any data of public interest at all. All in all, it can be established that as a result of the monitoring procedures, every municipality uploaded their general publication scheme; however, they failed to publish the required data in full even after the expiry of the action plan due date.

Publication in accordance with legal regulations constitutes a physical and financial burden for small municipalities; they try to use the municipal ASP website, or they purchase similar programs from companies. With regard to the decision-making and the decisions of the body of representatives, the data content of the publication unit is often confused and mixed up by many, and the publication of the data is often deficient. The invitation to the meetings of the body of representatives, the submissions and the minutes of the meetings are published in a variety of ways, in some places at one location containing everything, while elsewhere everything is shown separately. Even if there are data of this type, they are typically showed not under the menu “Data of public interest”, but under other menu points of the website. Information concerning the order of administering municipal authority cases is frequently deficient, or can be found in ways other than incorporated in the scheme. In many cases, the publication of financial management data is also deficient. Notifiers repeatedly object to the absence of justification of the results of tenders. In the case of projects funded with EU support, there is often failure to publish contracts.

Numerous organs find the interpretation of certain datasets problematic, or these datasets are typically absent from the general publication schemes. In the case of grants awarded on the basis of non-individual decisions (no discretion, automatic if the application complies with the legal conditions), the justification should at least indicate the legal regulation and its section containing the conditions of decision-making which enables or requires the grant.

Another general deficiency is that only the public procurement plan is uploaded to the scheme from the data on public procurement; a summary of bid evaluation and contracts is missing. In the case of this dataset, the publication obligation can be met by providing the accurate link to the summaries published in EKR (Electronic Public Procurement System) (it is, however, not sufficient to provide access to the central EKR website).

In many cases, organs performing public tasks publish the public findings of investigations conducted by them and not the findings of investigations run to check their basic activities. In many cases, statistical data are also missing (e.g. OSAP datasheets). With regard to development projects implemented with support from the European Union, the aid contract, as well as the other contracts implementing the investment project must also be uploaded.

Finally, it should be underlined that only a very few organs show the dates of updating the data, in spite of the fact that only with the knowledge of this date can one decide the period reflected in the data and whether the data are valid.
Based on the experiences of the first year of monitoring, it can be established overall that as a result of the procedures, the publication practices of the majority of the monitored organs improved. The Authority published the reports on its website.[20]

20 https://naih.hu/monitoring-jelentesek-menu-heading/kozzeteteli-gyakorlatot-erinto-monitorig

## *III.2. Additional freedom of information activities of NAIH in 2024*

### *III.2.1. Amendments of the Privacy Act affecting freedom of information*

On 17 December 2024, Parliament adopted Act LXXXV of 2024 on the Amendment of Certain Acts for Deregulation in the Interest of Legal Competitiveness, which also amended the Privacy Act as of 1 January 2025.

With the entry into force of the Act, the range of organisations subject to the obligation to publish data on the Central Informational Public Data Records (kif.gov.hu) platform (hereinafter: Platform) expanded substantially adding about 5,600 obligees based on Section 37/C of the Privacy Act. In the future, all legal entities registered by the State Treasury according to Act CXCV of 2011 on General Government (General Government Act)[21] will be required to publish the data of public interest specified in the Act on the Platform. Beyond budgetary organs, they include public bodies, local governments, minority governments, associations, regional development councils and other legal entities applying the rules governing the financial management of budgetary organs based on legal regulation, categorized by law into the central subsystem of general government. For the first time, obligees are required to publish their data generated after 1 January 2025 on the Platform by 28 February 2025. It is a new provision that every obligee has to publish the data generated by the 30th day preceding the due date of the next reporting (28th day of every even month) on the Platform.

In addition, the Privacy Act was also amended as of January 2025, stating that if an organ performing public tasks managing data requests calls upon the requestor to clarify the request because it is not unambiguous, it may do so by setting a due date at max. 15 days, which period is not included in the period for meeting the data request. The definition of data of public interest in Section 3(5) of the Privacy Act was also clarified, so that the organ, organisation or person performing public tasks and taking over such tasks specifically qualify as one discharging public duties, hence they are under the obligation to release data. Following the amendment of Section 27(6) of the Privacy Act, within the time limit referred to in paragraph (5) [10 years], requests for access to data used for decision-support may be refused, if access to the data would jeopardise the lawful functioning of the organ performing public duties or the performance of its func-

21 https://www.allamkincstar.gov.hu/Koltsegvetes/Torzskonyvi_nyilvantartas/ktorzs

tions and powers without undue external influence, in particular the free expression of its views in the course of certain court procedures.

The amendment also affects Section 29(2a) of the Privacy Act and its Annex 1, the general publication scheme[22].

We indicated in the report on 2023 that data hosts more and more frequently cited among the reasons for refusal the fact that they do not process the requested data in the requested format, they are not under an obligation to generate such data, or that they are not controllers. According to the freedom of information reports for the year 2024, these two reasons for rejection – the former for 1,266 and the latter for 2,854 datasets – were cited as legal basis by the organs.

As several submissions in the preceding year addressed the mode of meeting data requests, the HIKAP/KIKAP portal operation and the accessibility and downloading of data, the Authority issued a recommendation concerning the review of the operation of the KIKAP portal detailed in the subsection of Freedom of information recommendations of the Authority.

### *III.2.2. Authority procedures for transparency*

2024 was the second consecutive year when the Authority conducted authority procedures for transparency; this year, 115 procedures were launched (they were launched ex officio even in the case of notifications). In 82 of the 88 decisions, infringements were established and nine decisions contained orders. The Authority imposed procedural fines to an amount of HUF 430,000; fines according to substantive law were not imposed. Budgetary organs turned to the courts against the decisions of the Authority in four cases. The Authority won one of these procedures; the other three are still pending.

The Central Informational Public Data Records Platform and the authority procedures for transparency proved to be efficient means of ensuring the transparency for the use of public funds. In 2023, 649 organs uploaded 5,608 reports to the Platform; by the end of 2024, the number of these organs rose to 1,768 and the number of their reports increased to 10,856. With two exceptions, the budgetary organs reviewed made up for the publication of their missing financial man-

22 https://naih.hu/component/phocadownload/category/6-tajekoztatok-koezlemenyek?download=1062:kozlemeny-az-onkormanyzatok-es-tovabbi-torzskonyvi-jogi-szemelyek-uj-kozzeteteli-kotelezettsegerol-es-az-infotv-2025-januar-1-en-hatalyba-lepo-egyeb-modositasarol

agement data at the latest in the course of transparency procedures, so there was neither need (nor possibility) to impose a fine according to substantive law.

As to the objective scope of the obligation, several issues of law interpretation arose in the Authority's practice in 2024. Centralised public procurement proved to be a particularly problematic area. As these involve high value procurements up to several 10 billion forints in value, their transparency requires particular attention. Centralised public procurement consists of two stages; as a result of the first stage, the central procurement organ specifies the essential conditions of the subsequent institutional procurement, while in the second stage, the institution concludes the individual contracts and submits its direct orders. In 2024, the Authority reviewed the publication of contracts concluded in the first stage of centralised public procurement by the central procurement organ, as well as that of the contracts concluded as a result of the second stage. In these procedures, it was disputed that the framework agreements concluded in the first stage, or even the contracts concluded as a result of the second stage were subject to the objective scope of the publication obligation. If this was accepted as the proper interpretation of the law, there would be absolutely no information on the Platform on centralised public procurement. During the Authority procedure for transparency, the central procurement organ accepted the position of the Authority and published the missing 107 contracts found by the Authority, as well as the other 26 contracts, which it found [NAIH-4077-11/2024].

One ministry did not share the Authority's position according to which contracts come into being as a result of the confirmed direct orders in the second stage of the framework agreement procedure. The Authority launched authority procedures for transparency against several ministries because they did not provide data on contracts concluded on the basis of the direct orders sent via the internet-based system of the Directorate General for Public Procurement and Supplies pursuant to the framework agreement on "International travel organisation". Section 105(2) of Act CXLIII of 2015 on Public Procurement (hereinafter: Public Procurement Act) declares that public procurement may be realised by means of a direct order, then in its next sentence it states that the contracting authority concludes the contract for the realisation of the given public procurement. This means that as a result of confirmed orders contracts come into being. Section 26(4) of Government Decree 168/2004. (V. 25.) on the centralised public procurement system and the tasks and powers of the central procurement organisation expressly declares that contracts for pecuniary interest come into being as a result of direct orders. Four ministries complied with the order, or published the missing data already during the procedure. One ministry turned to the courts

as according to their interpretation of the law, contracts do not come into being on the basis of direct order. According to the position of the Authority, the ministry was in default, because it failed to provide any data concerning a substantial number of contracts of significant value (at least totalling HUF 893,164,961 net). Hence it ordered the publication of its decision. The ministry requested immediate legal protection against the publication of the Authority's decision, which the court rejected [NAIH-4456/2024 – litigation pending].

Several budgetary organs interpreted the due date for reporting according to the requirement for updating in Section III.4 of Annex 1 to the Privacy Act. Pursuant to Section III.4 of Annex 1 to the Privacy Act, organs performing public tasks are required to publish data on certain contracts on their website in their general publication schemes within 60 days following the date of the contract. With regard to these contracts, however, based on Section 37(4a) of the Privacy Act, budgetary organs do not have the general publication obligation on their own websites, instead they have to comply with their obligations according to Section 37(C)(1), which requires publication on the Platform on a two-monthly basis. According to the position of the Authority, the due date of 60 days required under the general publication obligation by contract calculated from the date of the contract does not correspond to the due date specified in Section 37(C)(1) of the Privacy Act as the latter is differently worded. Furthermore, Section 75/D of the Privacy Act requires the publication not only of the data generated between 29.11.2022 and 28.12.2022 by 28.02.2023 (for which the 60 days passed since their generation by 28.02.2023), but also the data generated between 28.12.2022 and 28.02.2023, in which case the 60 days from their generation has not expired by the due date of publication. According to the position of the Authority, as the data provided by the budgetary organs have been accessible to the public on the Platform since 28.02.2023 – i.e. the first publication on the Platform took place uniformly on 28.02.2023, so data provided earlier were first disclosed on the Platform at that time, hence the due date for publication has to be uniformly calculated from the date of the first publication on 28.02.2023 for each organ (that means that the next publication due date was 28.04.2023). The Privacy Act stipulates publication at bi-monthly intervals, which means the publication of the data according to the definition set forth in the Privacy Act. This interpretation of the law is supported by the objective and the expectation of the legislator, namely "the transparency of the use of public funds". [NAIH-6984/2024 – litigation pending; the Courts of Appeal turned to the Constitutional Court with a view to the review of the regulation.]

In another case, a budgetary organ challenged the decision of the Authority because in their view the Authority ordered them to publish non-existent data. In columns 15 and 16 of the datasheet to be published on the Platform, the reporting organ has to indicate the EKR identifier of the public procurement procedure and the exact accessibility of the detailed data of the procedure on the website ekr.gov.hu. According to Section 31(5) of the Public Procurement Act, the use of EKR (Electronic Means of Communication) is not always mandatory in public procurement procedures, for instance, when procurement is administered through the KEF Portal (in the dynamic procurement system operated by KEF or based on a framework agreement concluded by KEF); however, the data specified in the Public Procurement Act, or in its implementation decree has to be published in EKR even in these cases. An EKR procedure identifier is generated also in this case, which has to be published on the Portal [NAIH-1636-6/2024, litigation won].

The Authority launched an ex officio procedure against a ministry because, when checking the publication of budgetary support in an investigative procedure, it found that the beneficiaries included as such in the decision on support were not the beneficiaries indicated on the Platform, but the administering organ. The ministry may entrust an administering organ with the discharge of tasks related to public support for sports. In such cases, according to the Authority's position, the beneficiaries of support are the sports organisations named in the decision on support; hence they have to be shown on the Platform as beneficiaries. This position is supported by the fact that even according to OTR data, the sports organisations were the beneficiaries, the administering organ did not claim the support under study, the necessary funding was available in the administrative account of the ministry according to the contract on support, and the administering organ acted on behalf of and representing the ministry. The enforcement of the freedom of information in line with Article VI(3) and Article 39 of the Fundamental Law is fully implemented when budgetary organs make the data of budgetary support provided by them transparent on the Platform by naming the actual beneficiaries. [NAIH-3786-10/2024, – litigation pending]

Calculation of the value of the contracts continued to be problematic for the organs subject to the publication obligation. The Authority underlined several times that the text of Section 37/C(4) of the Privacy Act defines the value of contract as the "agreed upon" consideration and not the paid consideration; this means that if the value of the consideration in the contract was agreed to be a value in excess of 5 million forints, the organ will have a publication obligation with regard to this contract upon its conclusion. In other words, this obligation is generated

not at the time when the paid consideration exceeds the limit value of 5 million forints. Moreover, the options and the reserve funds set forth in the contract are not necessarily exhausted but as the Privacy Act contains the phrase “agreed upon consideration”, the value of the option and of the reserve fund is also part of the value of the contract.

Another issue of legal interpretation related to the value of contracts was whether only those contracts under which an organ incurs expenditures or those also under which it receives revenues have to be published. A national park requested the statement of the Authority on whether they have to publish the data concerning the leasehold contracts of land areas it manages on the Platform, because under these contracts it does not incur expenditures but receives revenues. According to the position of the Authority, the obligation applies also to revenues because Section 37/C(2)(b) of the Privacy Act subjects the data of the sale and exploitation of assets to this obligation and it is clear that the organs selling or exploiting assets obtain revenues from contracts of this type. [NAIH-12269-2/2024]

The Authority requested the statement of the Ministry of Justice concerning the joint interpretation of the publication obligation of public education institutions according to Section 37/C(1) of the Privacy Act and the derogation in Section 33(4) of the Privacy Act. According to Section 33(4) of the Privacy Act, public education institutions and vocational training institutions fulfil their obligation by electronic publication under this Act by providing data to the information system specified by sectoral laws. It was another issue of legal interpretation whether public education institutions operated by municipalities (in which case it is not the school districts that conclude contracts and do the reporting on the Platform) should discharge their obligation according to 37/C(1) of the Privacy Act in the sectoral information system or on the Platform. According to the position of the Ministry of Justice, Section 37/C of the Privacy Act stipulates a sui generis publication obligation, which is generally separate from the (general) publication obligation addressed under Subtitle 23 of the Privacy Act, hence Section 33(4) of the Privacy Act does not affect the publication obligation on the Platform. [NAIH-14387/2024]

As a recurrent problem it should be mentioned that the organs subject to the publication obligation still frequently provide the exact link to the detailed data of the procedure on the ekr.gov.hu website in a manner requiring identification in the case of contracts concluded as a result of public procurement. Transparency of the published data is greatly hampered when many organs publish not only new data, but also carry forward already published data on their datasheets.

## *III.3. Cases related to personal data accessible on grounds of public interest and local governments*

### *III.3.1. Accessibility of data of political consultants*

An organisation submitted requests for data of public interest to several ministries in which they asked for the name of persons holding jobs of political consultant and senior political consultant on their staff (including the ministerial cabinet, the cabinet of the state secretariat and the cabinet of the political director), the name of the organisational unit, the commencement of the public service (period of incumbency) and their remuneration. However, the ministries failed to comply with the request for data of public interest even after its clarification, but differently from the request, they showed the total number of consultants and the aggregate amount of their gross monthly remuneration in their answers of merit. According to their justification, the data of political consultants do not qualify as data accessible on grounds of public interest. Only one ministry complied with the data request lawfully, saying that they do not have political consultants and senior political consultants.

In its statement, the Authority presented its position in detail concerning the fact that the response calling for clarification was made without a reason and it was unjustified, as well as the consistent practice of the courts supporting its position, including a number of judgments made on this subject matter.

The Authority explained that the name of the persons in political consultant and senior political consultant roles, the name of the organisational unit, the commencement of public service (duration of the period on the job) and the data on remuneration are data closely related to the performance of public tasks and hence are data accessible on public interest grounds. As to which persons in what jobs take action under the functions and powers of an organ discharging public tasks can only be decided on the basis of the legal regulations pertaining to the specific organ, the public tasks stipulated therein, the rules governing the operation of the organ, the job descriptions and the subject matter of the contracts of assignment, i.e. only specifically with respect to the given organ. In view of the fact that political consultants serve to support the activities of the Prime Minister, the decision-making of the Government and tasks directly related to the activities of the minister and the secretary of state, they qualify as persons performing public tasks set forth in legal regulation, hence they are persons taking action under the functions and powers of the organ.

Making the identity of political consultants public is in the legitimate interest of citizens; it is important also for society to be able to ascertain whether the decisions of a minister are taken on the advice of a professionally recognised expert, whether and how this person is able to use his special knowledge and work experience to assist in the work of these organs and whether he serves the interests of society because decisions made at the ministries have a direct or indirect impact on the life of every citizen.

According to the consistent practice of the Authority and of the courts, the data concerning the working conditions of and the work done by persons acting within the functions and powers of organs performing public tasks, such as the name of their organisational unit, the commencement of their legal relationship (period of being on the job), and the data on their remuneration qualify as other personal data related to the performance of public tasks pursuant to Section 26(2) of the Privacy Act, hence accessible on the grounds of public interest. Furthermore, the Authority presented the evaluation report and recommendations of the Group of States against Corruption (GRECO) with regard to Hungary:
GRECO monitors in what way Member States comply with the anti-corruption documents of the Council of Europe. Under Section 37 of the GRECO evaluation report on Hungary adopted on 17 June 2022 the GET (the GRECO evaluation team) "*also observed a lack of transparency around the composition of ministerial cabinets and the functions and remuneration of their members. Their appointments are not made public, except for the PM's cabinet, nor is there any obligation or practice to publish the names and duties of political advisers on the government's or the ministries' websites. The GET recalls that GRECO has highlighted on numerous occasions the importance of transparency regarding the role of those persons providing advice to top political leaders. Therefore, GRECO recommends that the name and duties of all political and personal advisers to the Prime Minister, ministers and state secretaries be published on the government's and ministries' internet sites and that this information be kept up to date*".

The Authority established that the data requested by the notifier must be released by the ministries. Pursuant to Section 56(1) of the Privacy Act, the Authority called upon the ministries to grant the notifier's requests for data of public interest and to send him the name of the political consultants and senior political consultants in a political service relationship on the staff of the ministry (including the ministerial cabinet, the cabinet of the state secretary and the cabinet of the political director), the name of the organisational unit, the commencement of their service (period on the job) and remuneration. In view of the fact that the general,

specific and individual publication schemes required by law are not accessible on the websites of the ministries, the Authority requested the ministries pursuant to Section 56(1) of the Privacy Act to take measures to comply with their electronic publication obligations in accordance with the legal regulations in force, and as part of this, have the data to be published in the general, specific and individual publication schemes uploaded. Finally, pursuant to Section 58(3) of the Privacy Act, the Authority informed the notifier that as the Authority's calls according to Section 56 of the Privacy Act did not achieve a result in this case – the ministries repeated that they disagreed with the positions of the person requesting the data and the Authority and maintained their own positions constituting partial (substantive) refusal of the request, the Authority deemed that in this case it had no authority powers and that there was no realistic prospect for changing the position of the ministries, so informed the notifier that he may go to court pursuant to Section 31 of the Privacy Act. [NAIH-687/2024

*III.3.2. The accessibility of the name of the nominating organisation in the case of a member of the electoral commission*

With regard to a member delegated to a local electoral commission, a citizen requested the name of the delegating organisation/person, who delegated the person concerned. The municipal executive asked whether the name of the organisation or the delegating nominee can be released.

The position of the Authority is that in the case of persons obtaining membership in an electoral commission by way of nomination, the data of the nominating organisation or person as personal data accessible on grounds of public interest can be forwarded to the person requesting them. At the same time, the attention of the person requesting the data must be called to the fact that by accessing the data, he becomes the controller and the rules of the General Data Protection Regulation are also applicable to the processing of personal data accessible on public interest grounds, and that under Section 26(2) of the Privacy Act, he may propagate the accessed personal data only in compliance with the principle of purpose limitation and that its publication on a website is also governed by the provisions of Annex 1 and the separate act concerning the legal standing of a person performing public tasks. The local electoral office as controller is subject to the controller obligations according to the General Data Protection Regulation, which includes providing information to the data subject and ensuring that the data subject can exercise his rights.

When performing their activities in the course of the electoral process (tasks specified by legal regulation), the members of the electoral commission and the polling station commission act as persons performing public tasks, hence their data related to the performance of this public task qualify as personal data accessible on grounds of public interest. The process of nomination (or delegation, to use a common expression), through which they obtain membership in the commission is directly related to the performance of their public tasks, and therefore the name of the organisation or person nominating (delegating) the member can be made accessible as data accessible on grounds of public interest together with the personal data (name) of the member. [NAIH-9363-2/2024]

*III.3.3. Statement of assets*

Year by year, the Authority receives requests for statements concerning the accessibility of the statements of assets of municipal representatives. Pursuant to Section 39 of Act CLXXXIX of 2014 on the Local Governments of Hungary (hereinafter: Municipalities Act), the statement of assets of municipal representatives can be made accessible under a request for data of public interest or data accessible on public interest grounds in accordance with Section 28(1) of the Privacy Act; the representative and their employer may not restrict accessibility by contractual provision. [NAIH-12792-2/2024; – accessible on the website[23].]

Without his consent, the representative's statement of assets may be published only if the municipality orders the mandatory publication of statements of assets in an individual publication scheme based on Section 37(3) of the Privacy Act in a municipal decree.

The publication of the statements of assets of representatives on the website is in line with the goals according to Section 1 of the Privacy Act, in view of which the legislator rendered statements of assets accessible on public interest grounds: the transparency and public control of the exercise of public power, administering public affairs and, in this context, the use of public funds. Section 26(2) of the Privacy Act sets the restriction on the dissemination of the data, i.e. they cannot be disseminated for purposes other than those listed, for instance, to manage personal conflicts. [NAIH-13865-2/2024][24]

23 https://www.naih.hu/dontesek-infoszab-allasfoglalasok?download=957:onkormanyzati-kepviselo-vagyonnyilatkozat-tetelenek-jovedelmi-adata-megismerhetosegenek-a-kepviselo-munkaltatoja-altali-korlatozhatosaga

24 https://naih.hu/informacioszabadsag-ajanlasok?download=1065:a-nemzeti-adatvedelmi-es-informacioszabadsag-hatosag-ajanlasa-az-onkormanyzati-adatkezelo-egyedi-kozzeteteli-lista-letrehozasaval-kapcsolatos-feladatairol

*III.3.4. Municipal consultants*

The Authority received a submission for consultation concerning the personal data of municipal consultants accessible on grounds of public interest. The person requesting the data asked for the names of persons holding jobs as municipal consultants, their employment contracts, the list and amount of other benefits not governed by the employment contract and the documents verifying their qualifications. Of the provisions of the Privacy Act and Act CXCIX of 2011 on Civil Servants (hereinafter: Civil Servants Act), the Authority underlined Section 26(2) of the Privacy Act, according to which data accessible on public interest grounds shall include the personal data listed in the various acts on legal standing, as well as such person's other personal data relevant to performing public duties. The Authority found it important also to highlight that the fact that data on municipal consultants related to the performance of public tasks is part of the basic civil service register according to the Act on Civil Servants (or of any other register) does not mean that it would not be accessible through a request for data of public interest. Over and above the fact that Sections 26-31 of the Privacy Act do not contain such restriction on access, this also follows from the enforcement of the data of principle as it is not the register and not even the individual documents that are accessible on public interest grounds, but the "data" that comply with the provisions of Section 3(6) of the Privacy Act. Section 1 of the Privacy Act specifies the objective to be served by access to data of public interest and data accessible on public interest grounds, which is the transparency of public affairs, which means in addition to the transparency of the management of public funds and public assets, the transparency of the discharge of public duties itself. According to the position of the Authority, the consultant's activities influencing decision-making in merit is part of the performance of public tasks just as the activities of civil servants, thus under request for data of public interest, in addition to their names and data on their incomes, the data of the performance of the tasks they carry out (job) and – as consultancy presupposes special expertise for them – the data on qualifications supporting or eventually calling into question their suitability to perform the tasks should also be accessible[25]. [NAIH-13540-2/2024]

25 https://www.naih.hu/dontesek-infoszab-allasfoglalasok?download=963:onkormanyzati-tanacsadok-tevekenysegere-es-juttatasaira-vonatkozo-adatok-megismerhetosege

*III.3.5. Making video and sound recordings of the session of the body of representatives*

Both the Constitutional Court in several of its decisions, and the Authority in several of its statements emphasised that anyone, even members of the audience, may record public sessions of the body of representatives without separate permission from the other persons present about the statements of the representatives and may use such records for any purpose that is not unlawful.

The Authority summarised the requirements for making the video and sound recordings in its statement NAIH-12396-2/2024 as follows:

If the persons participating in the session make the recording as part of their personal activity for home use (as keepsake, for sharing with friends, relatives and acquaintances, such as in a private Facebook group, etc.), the processing of the data is not subject to the objective scope of the General Data Protection Regulation.
In contrast, if the recordings are made by a journalist, a politician, a representative of a social organisation, etc. present at the session not for private use, but for other purposes, such as publication, they must inform the participants of the session in advance of the processing of personal data under Article 13 of the General Data Protection Regulation. The mode of providing this information should be developed and appropriately regulated on the spot: for instance, the controller should notify the municipal executive or the chairperson of the session of the recordings in advance prior to the session.
A case other than the above is when the municipality itself is the controller, for instance, when a public session of the body of representatives is live streamed.
In any case, the participants of the session must be informed in advance of the live streaming or making the recordings by a statement calling attention to this to be uploaded to the municipality's website, or in the text of the invitation to the session. In addition, it is recommended to place a conspicuous announcement in front of the hall where the session is held prior to entry, disclosing the contact data of the data protection officer and providing information on the data subject rights according to Articles 15-21 of the General Data Protection Regulation and the place where additional detailed information according to GDPR Article 13 is accessible on the processing of the data.

The Authority considers it good practice to provide rows of chairs in the meeting hall for the audience which are outside the angle of view of the camera or which are not shown on the recordings or in live stream. Even in the absence of this, it

is necessary to ensure the enforcement of data subject's rights for the members of the audience, including the possibility of erasure in view of the objection of a data subject, or if it is expressly requested. [NAIH-12179-2/2024; NAIH-13877-2/2024]

## *III.4. The 2023 amendment to the Privacy Act and its impact on the release of data under Section 30(2a)*

Section 110 of Act CI of 2023 on the System for the Exploitation of National Data Assets and on Certain Services introduced a new rule to the provisions of Section 30 of the Privacy Act enabling the restriction of access to data of public interest and data accessible on public interest grounds. Under paragraph (2a) in force since 1 January 2024, the organ performing public duties shall not be obliged to comply with the data request if it would necessitate
*a) procuring or collecting data other than those the organ performing public duties effectively processes, including in particular data that are processed by an organ performing public duties under the direction or supervision of the former, or*
*b) producing by consulting the data of public interest or data accessible on public interest grounds effectively processed by the organ performing public duties, new data as compared to those it processes*.

According to the justification, the bill aligned with the relevant practice of the courts and the Constitutional Court stipulates that organs performing public duties cannot be required to *collect data other than those they process, or to produce qualitatively new data with regard to the data they do process*.

Act CXXXI of 2009 on the promulgation of Council of Europe Convention on access to official documents (hereinafter: Convention) introduced the provisions of the Convention into Hungarian law as of 1 December 2020. According to Article 5(2) of the Convention "if the public authority does not hold the requested official document, or if it is not authorised to process that request, it shall wherever possible refer the application or the applicant to the competent public authority." The Authority explained its position in the relevant Recommendation[26] and it expects controllers to follow the recommendation in practice: if the organ discharging public duties does not process the requested data, in addition to the notification on the refusal according to Section 30(2a) of the Privacy Act, the

26 https://www.naih.hu/informacioszabadsag-ajanlasok?download=505:a-nemzeti-adatvedelmi-es-informacioszabadsag-hatosag-ajanlasa-az-igenyelt-kozerdeku-adatot-tenylegesen-kezelo-szervezetre-vonatkozo-tajekoztatasi-kotelezettsegrol

controller shall inform the person requesting the data of the identity of the actual controller of the requested data of public interest or data accessible on public interest grounds provided that the controller has this knowledge. Because of this, the Authority called upon controllers to inform the person requesting the data of the identity of the actual controller not only in its statements on investigations [NAIH-5560/2024], but put forward recommendations concerning the data release practices of several organs performing public duties in the course of the monitoring checks.

Problems related to the production of new data had appeared earlier in the practice of the Authority when performing data requests of public interest. In the past, in several cases, controllers rejected providing access to data of public interest in the absence of reasons for rejection set forth in a legal regulation, citing Constitutional Court Decision 13/2019. (IV. 8.) AB (hereinafter: AB Decision). The justification to the AB Decision declares:
"[*59] 5.2. Searching for data, which are in any way processed (for instance, stored), as separate from the case when the data request is aimed not at data or series of data related to the public tasks, which can be specifically searched simply or with some extra work, but at requiring the controller to procure or collect new data other than those processed, or to produce new qualitatively different data by comparing data, which it otherwise processes (statistics, statements), or materials explaining the data, or draw conclusions from the data. […] Similarly, the controller is under no obligation to produce new data series out of otherwise accessible or published data filtered according to specific criteria. The person requesting the data may not claim that somebody else carry out the sorting of accessible data.*
*[60] This means that* ***the controller is under an obligation to release only the existing data of public interest/data accessible on grounds of public interest recorded in any way and actually processed by it****. An obligation to produce data does not follow from the Fundamental Law. If the character of the data requested to be released – qualified as data of public interest (cf. Section 3(5) of the Privacy Act), or accessible on grounds of public interest (cf. Section 3(10) of the Privacy Act) cannot be established, this constitutes an impediment to compliance with a claim of fundamental right aimed at accessing data of public interest [Constitutional Court Decision 3252/2016. (XII. 6.) AB]*."

In the justification to the AB Decision, the Constitutional Court specified the criteria[27], which according to the position of the Authority, controllers need to take into account when applying Section 30(2a)(b) of the Privacy Act.

The mayor of a municipality rejected a request for data of public interest aimed at the contracts of a municipal business organisation concluded in 2023 citing the production of new data, because of which the complainant turned to the Authority. The case threw light at another procedural order not unique among organs performing public tasks, according to which the person exercising the powers related to requests for data of public interest entrust another leader of the organisation with answering. In this case, the statutes of the municipality authorised the mayor to exercise the powers related to reporting with regard to the release of the data of the municipal company, who entrusted the municipal executive to give an answer. Because of this, it was not the municipal company that assessed and answered the data request complained against.

In the course of the investigation, the municipal executive informed the Authority that "no separate records are kept of orders and contracts, their original copies are simply filed and any subsequent documents are manually enclosed with the relevant contract". On that basis, the Authority established that the data request aimed at accessing actually recorded existing data, and in view of this, it should be performed. It was also established that the data, which the person wished to access – how many contracts were concluded by the company in 2023, with whom, what was the subject matter and value of the contract – did not require a comparison of existing processed data or complex research, development of new sorting criteria or methods of calculation that had not existed before, or the assessment of statistical or legal analysis. So, according to the position of the Authority, in view of established judicial practice, the data to be accessed do not qualify as new data; because of this, in addition to establishing the infringement, the Authority ordered the company to release the requested data of public interest. [NAIH-3885/2024]

In another case, the person requesting data wished to access data concerning dates that could be reserved in the date booking system of the National Transportation Authority (which administrator issued it, which user reserved it, data concerning the deletion of reserved dates) in a breakdown by site. In the course of the investigation, the controller explained that there is no legal requirement for recording the data according to the request; these data are records run-

27 AB Decision 13/2019. (IV. 8.), Justification, Sections [45] – [61]

ning in the background of the application, facilitating the technical operation of the system. The controller also added that a separate development project would be needed to meet the data request by programming the recording of the first date of announcement in a new database field and allowing for the traceability of modifications (who altered an announcement, when and in what way). The Authority accepted the reasons of the controller and terminated the investigation without establishing an infringement. [NAIH-12959/2024]

In the year of the entry into force of the provisions related to the production of new data, these provisions were applied as follows based on the reports of the controllers:

| **Reason for rejection** | **Number of datasets rejected, first and second half of 2024** | **Total** |
|---|---|---|
| *Section 30(2a)(a) collection of data* | 318 + 350 | 668 |
| *Section 30(2a)(b) production of new data* | 758 + 508 | 1266 |
| | | 1934 |

*The source of the data is reporting according to Section 71/D(3) of the Privacy Act.*

## *III.5. The accessibility of environmental data*

A highly frequent reference for restricting access in relation to requests to access environmental data, and a reason for rejection is the nature of the data used as a basis for decision-support under Section 27(5)-(6) of the Privacy Act.

An NGO complained that a Ministry failed to make the technical design documentation to be used as the basis for the planning documents for regulating the Balaton shoreline (hereinafter: Technical design documentation) available to it. The ministry claimed that the requested document serves as the basis of a future ministerial decree and a government decree stipulating the special local development planning and building requirements pertaining to buildings on the Balaton waterfront area, the criteria of designating the territorial scope of the public purpose area utilisation plan, the requirements concerning the content of the plan and the requirements concerning the shoreline regulatory plan content

is currently being developed. According to the position of the Ministry, making the regulated shoreline public prematurely would lead to detrimental processes; building plots would be developed before the new regulatory shoreline would prohibit it. Similarly, areas, which the old regulation (currently in force) qualified as dry land would be filled in (where filling in is lawful), while according to the new regulation (planned, appearing in the Shoreline Plan), these areas would constitute part of the lake bed zone (where filling in is forbidden). In these cases, the goal of the regulation (keeping the 30-metre band of land along the shoreline untouched and the prohibition of filling in the lake bed) would be clearly thwarted, if the technical design documentation were to be made public prematurely. The Authority requested information whether the Shoreline Plan was subject to the scope of Government Decree 2/2005. (I. 11.) on the environmental examination of individual plans and programmes (hereinafter: Skvr.) and, if so, whether the environmental assessment of the Shoreline Plan was carried out and in what way was the required information provided to the public. The Ministry informed the Authority that conducting the environmental assessment is mandatory in the case of the Shoreline Plan, the production of the environmental assessment according to Section 8 of Skvr. is in progress, it is expected that the accessibility of the environmental assessment will be ensured simultaneously with the professional and civil consultation on the Shoreline Plan. The Authority accepted the Ministry's arguments on how the accessibility of the technical design documentation could thwart the efficient implementation of the Government Decree on the requirements concerning the land use of the Balaton waterfront areas (BATÉK), in view of the fact that at the time of the data request BATÉK has not yet been adopted. [NAIH-9041/2024]

In another case, also related to the reason for restricting access to data on which a decision was based, the legal representative of the notifier complained that a request for data of public interest in an environmental status assessment was rejected by a ministry, stating that the data in the data request qualify as data supporting decision-making. According to the position of the notifier, the ministry should enable anyone to have access to the assessment of the conditions as environmental information based on the relevant request. Upon contacting the ministry as part of the Authority's investigation, the ministry revised its position concerning the data request and sent the requested environmental data to the notifier. [NAIH-8724/2024]

A new phenomenon in meeting requests for data of public interest concerning cases related to the activities of battery plants, which are the responsibility of a government office, included the adjudication of the qualification of the request for

data of public interest, on the one hand, and of the accessibility of the relevant emission data concerning the workplace environment, on the other hand.

In one of the cases, the notifier posed questions in connection with a planned battery plant; however, the Government Office did not regard his submission as a data request. According to the position of the Authority, the notifier's letter should have been handled as a request for data of public interest and answered accordingly as the notifier clearly indicated at the beginning of the letter that he was submitting a request for data of public interest: "I am turning to you for the purpose of requesting data of public interest". An organ performing public tasks may and is even obliged to handle a submission as a request for data of public interest, not marked as a request for data of public interest, but a submission marked as a request for data of public interest cannot be handled as not a request for data of public interest. Therefore, if anyone marks his submission as a request for data of public interest, the mandatory elements of form and content of rejecting the request as set forth in Section 30(3) of the Privacy Act may not be waived. If the assessment of the content of the data request leads to the outcome that it does not concern data of public interest, or that the requested data are not held by the organ, then the position concerning this and its justification must be expounded in a rejection complying with Section 30(3) of the Privacy Act. The Government Office's answer to the notifier included that the decision annexed to the answer "contained the answer for every question concerning the Government Office". This, however, does not reveal for which questions the decision contains an answer and which section of it, or whether there are any questions for which the decision does not contain an answer. Hence, the Government Office would have acted in compliance with Section 30(3) of the Privacy Act, if:
1. the decision contained the answer to a question, the Government Office accurately indicated the section of the decision that covers the answer to a question, or if it had answered the question;
2. the notifier had a question to which the decision did not include an answer, but the Government Office had the requested data (and there was no legitimate reason for restricting accessibility), then it should have answered the question,
3. the notifier requested data, which were not held by the Government Office, then it should have rejected the data request in that regard, and should have informed the notifier that it was not under an obligation to produce the data,
4. the notifier did not request data of public interest, then it should have rejected the data request with reference to this and give reasons why the requested data did not qualify as data of public interest. [NAIH-402/2024]

In another case, the notifier objected to the fact that when the Government Office granted his request for data of public interest, it blocked out data of public interest without a legal basis in some of the documents of its decisions ordering the elimination of deficiencies and imposing fines for safety and health at work, acting within its powers as safety and health authority. According to the position of the notifier, the Government Office unlawfully impeded access to data of public interest because it was not possible to learn the extent of exposure of the battery plant employees without the blocked data, what carcinogens they were exposed to and what carcinogens caused heightened mass exposure, which materials were examined in the course of the authority monitoring, to what extent the presence of pollutant/carcinogenic materials exceeded the prescribed limit values in certain rooms of the plant and employees in which jobs were exposed to high risk.

According to the position of the Government Office, the monitoring of the work environment means an examination of the internal air condition of the workplace and provides data on the exposure of employees to dangerous materials, measurement by personal sampling shows the eventual extra exposure affecting the individual working in the given workplace and it does not provide information on any hazardous materials eventually emitted to the external environment. Hence, in its judgement, these data do not qualify as environmental data.

According to the position of the Government Office, monitoring the work environment is not suitable to establish the extent of pollution to the environment, harmful impact on the environment, to measure the extent of pollution to air, water and soil, or compliance with environmental requirements. The Government Office considered that the technical processes and technologies concerning the selection of waste received and its preparation for processing, collection and storage, and the materials used as proprietary information covered by business secrets. The Government Office acknowledges the particular importance of the accessibility of environmental data and the fact that environmental information in the domain of the freedom of information constitutes high-profile data of public interest. In the course of its balancing test, the Government Office arrived at the conclusion that the blocked data were not relevant emission data from the viewpoint of the protection of the environment, the data request extended to data other than data accessible on public interest grounds, including protected know-how, the accessibility of which would cause disproportionate disadvantage to the holder of the secret, than meeting the data request of the notifier in part, hence the Government Office performed the data request by making the data concerning protected know-how invisible.

In the course of its investigation, the Authority established that based on the Fundamental Law, Article 2(3)(a) and Article 4(4((d) of Act LXXXI of 2001 on the Proclamation of the Aarhus Convention of 25 June 1998 adopted in Aarhus (hereinafter: Aarhus Convention), Section (3)(5) and (6), Section 26(1) and Section 32 of the Privacy Act, the provisions of Section 12(1) and (2) of Act LIII of 1995 on the General Rules of the Protection of the Environment (hereinafter: Environment Act) and Section 2(a) and (f) of Government Decree 311/2005. (XII.25.) on the order of public access to environmental information (hereinafter: Government Decree), the notifier had a right enshrined in law to access environmental data, because under the legal provisions, the emission data relevant for the protection of the environment are accessible to the public because the conceptual framework of the Aarhus Convention extends to all levels of the human environment, including the workplace air and environment as well as the conditions and circumstances of the workplace. The Authority also found that it is not an infringement of the right to business secrets when the business secret is released in order to protect public interest to the extent justified by the purpose, nor when the acquisition, use or disclosure of a business secret is required or permitted by a directly applicable Union act or law, and information relating to release into the environment cannot be withheld on the grounds that it is a business secret.

The Authority also called attention to the fact that the civil and criminal legal consequences related to the violation of business secret have no relevance in this case because under Section 220 of Act C of 2012 on the Criminal Code according to the legal definition of the crime of the misuse of data of public interest may constitute a criminal act if they are concealed from or made inaccessible to the person requesting them. The Government Office performed the data request with the requested data content for the notifier. [NAIH-809/2024]

The appreciation of the importance of the accessibility of environmental data was also indicated by the fact that a consultation question related to environmental data was sent to the Authority by an officer of an organ performing public tasks, which also processes environmental data.

The notifier requested the Authority's opinion on the disclosure and publication of data processed in the course of the procedure, and on the interpretation of the provisions of the Privacy Act, taking into account that it is a member of a state or local government organ performing public tasks and functions, which has conducted an official procedure on soil contamination. In its statement, the Authority expounded that an organ discharging public tasks acting within its powers may

in the case of a data request make a decision on disclosure while complying with the request, in the course of performing the mandatory publication obligation, or through the publication of decisions made in a public administrative procedure or the expert opinions, calculations and analyses concerning environmental data as set forth in legal regulation. The professional leader acting within his decision-making powers, in compliance with the chain of command, may decide to release the environmental data officially making them public, or to refuse to do so under an obligation to provide justification based on the provisions of the Privacy Act or the Code of General Administrative Procedure.

A subordinate employee of an organ discharging public duties is bound by the legal regulations applicable to his job with regard to making data public, the provisions of the Privacy Act or the Code of General Administrative Procedure, as well as the confidentiality rules arising from his obligations on the job; so, to answer the specific question, the notifier as a member of the organ may not lawfully disclose data related to the activities of the organ as an individual, partly because of the infringement of procedural and employment rules and their legal consequences, and partly because, in the context of the activities of the organ, he is not in an independent private individual enforcing his rights, but he is a person acting within the functions of the organ discharging public duties. Following the release or publication of the data, they can be freely disseminated (except for personal data accessible on public interest grounds, which is restricted on the grounds of purpose limitation); at the same time the official is still subject to the employment rules. With regard to data concerning environmental information, which are data of public interest, and data generated by others, the organ performing public tasks is the controller in the course of their use. The organ performing public tasks is entitled and obliged to disclose data of public interest generated in the course of the work of the organ performing the public task or produced by others in authority procedures related to polluting activities, based on the Privacy Act and relevant legal provisions. In the context of lawfully disclosing personal data accessible on public interest grounds, the Authority underlined that the rules applicable to access data of public interest must be applied to accessing them; nevertheless, the personal data nature of these data is retained; the most important guarantee of data protection i.e. the principle of purpose limitation applies also to these data; the purpose of processing these data may be the transparency and public control of the exercise of public authority, the administration of public affairs and the use of public funds[28]. [NAIH-606/2024]

28 https://naih.hu/dontesek-infoszab-allasfoglalasok?download=932:kozfeladatot-ellato-szerv-tisztviselojenek-jogai-kornyezetvedelmi-hatosagi-eljarasban-kezelt-adatok-kozzetetele-kapcsan)

## *III.6. Recommendations issued by the Authority in the context of the freedom of information*

In 2024, the Authority issued three recommendations in the context of the freedom of information, which are also published on its website.[29]

### *III.6.1. Recommendation on the application of Integrated Portal for the Disclosure of Data of Public Interest of the Government (KIKAP Portal)*

The report on 2023 already touched upon the advantages and the related complaints concerning the operation of portals used to perform data requests.
The Government of Hungary set up KIKAP in order to ensure the right to access data of public interest. However, no normative rules were enacted concerning the technical implementation of the Portal; the content and operation of the KIKAP portal has been without regulation ever since its launching. According to controllers using KIKAP and the description available on the online portal, the system has a number of advantages:

- it minimises the possibility of data loss,
- the uploaded materials are displayed in a more transparent format,
- the documents made available do not encumber the mailbox of the person requesting the data,
- the system guarantees the full protection of the personal data of the person requesting the data.

The Authority pointed out the problems listed below, which restrict the person requesting data in exercising his fundamental right to the freedom of information:
a) the documents uploaded to KIKAP cannot be searched and cannot be copied, their accessibility is non-transparent;
b) the person requesting the data cannot see the size, the number of pages and other relevant characteristics of the uploaded documents;
c) the released data can be viewed by a single user at any one time; the documents can only be scrolled and downloaded page by page only;
d) the accessibility of the data is far too restricted in time. The data of public interest uploaded to the platform is made inaccessible after 15 days, and they are erased from the platform within 90 days. So, if somebody for any reason whatsoever is unable to download the data within 15 days, he would have to submit a repeated data request to the controller, which may refuse to release the data pursuant to Section 29 (1)(a) of the Privacy Act;

29 https://naih.hu/informacioszabadsag-ajanlasok

e) controllers frequently use watermarks in the uploaded files, whose content is regularly the same as the e-mail address of the person requesting the data. This solution not only enables the identification of the person requesting the data, but it also restricts the broad dissemination of the data of public interest made available to the person requesting them;
f) data made accessible on the KIKAP platform upon a request for data of public interest are accessible exclusively to the person requesting them; in the case of an eventual other data request for the same set of data, the controller may not use the simplification provided for under the Privacy Act, according to which the data request may be granted by sending the link pointing to the data, provided that they were made public earlier. It follows that the data holder must repeatedly collect and upload the data to the platform which had earlier been released in this way.

The Authority recorded the following issues in its recommendation:
1) The Authority accepts that the use of the KIKAP portal in performing requests of data of public interest is adequate for releasing the data electronically; it considers it a good and up-to-date solution, but one that needs further improvement.
2) When performing data requests, the operators of the system and the controllers have to ensure multiple logins into the platform in possession of the access link and the person requesting the data should be able to download, save and print the data uploaded there several times. This, however, necessitates that the data uploaded and made accessible in granting the request for data of public interest be accessible for a period longer than the current 15 days, in other words, there should be no technical or time limit to accessing the data, to the actual performance of the data request. The Authority has no wish to determine or prescribe the number of occasions (logins, downloads) and the technical time period of access, however, the current time restriction in accessing the data is not aligned with compliance with the principle of transparency. In addition, it is also necessary to meet data requests in a format adequate to the technical requirements and possibilities of the 21st century, or if that is not possible, in a resolution that enables machine reading and processing.
3) The use of “watermarks” (for instance: displaying the e-mail address of the person requesting the data) in the files uploaded to the KIKAP platform is not acceptable as it may impede access to the data, their machine readability and the exercise of the right to disseminate the data. The use of watermarks or similar solutions should be discontinued.
4) General information on the operation of the portal is not available on the KIKAP platform, hence the Authority recommends that information be provided

to the organs performing public tasks using KIKAP in the course of performing the data request and inform the person requesting the data on the occasion of the first contact on the operation and use of the KIKAP portal, if the organ discharging public duties, performs the data request through the intermediation of the portal.
5) The implementation of a technical solution and provision of information is needed, which makes it clear to the persons requesting data that they could access and fully download all the data that were made accessible. In the case of large files containing many pages, the system should enable the downloading of data at once and not only by pages.
6) What could guarantee the adoption of the proposals set forth in the recommendation is a legal act by the Prime Minister's Cabinet Office accessible to anyone, which would determine the rules of processing and task performance related to the release of data of public interest on the KIKAP and similar other online portals in adequate detail and assignment of responsibilities.

*III.6.2. Recommendation concerning the Electronic Documentation System supporting the Building Authority's licensing procedure (ÉTDR)*

The Authority made a recommendation to transfer the text of Section 10(6) of Government Decree 312/2012 (XI.8.) on building and building supervision authority procedures and supervision and the building authority service, which was annulled as of 16 August 2024 into the chapter of the Building Code entitled XVI. REGISTERS, SPECIALISED SYSTEMS AND ELECTRONIC PLATFORMS and its repeated entry into force as follows.

The Minister of Construction and Transport did not accept the recommendation. In his answer, he explained that ÉTDR was not created to enable access to data of public interest. The informative function of ÉTDR has a secondary role, producing documents for a public platform constituted an extra burden for architects and producing the information meant a separate task for the building authority. In his view, the restriction of access to ÉTDR does not mean that its clientele would have become smaller. He maintained his opinion that the right to respect the privacy and home of others and the protection of the right to property is more important than the right to access data of public interest and data accessible on public interest grounds and the related freedom of expression. He explained that Act C of 2023 on Hungarian Architecture (the Building Code) specifies at the level of principle concerning measures and decisions of public interest that information to the public and the possibility of control by the community must be ensured in the manner stipulated by legal regulation prior to taking them and upon imple-

menting them; also as determined by legal regulation, action must be taken to provide adequate information to the interested party and they must be enabled to express their opinion and make recommendations in a manner which would not give them disproportionate difficulty. According to the intention of the legislator, this provision affects the data of public interest related to spaces of settlements and adopting decisions on them and the system supporting electronic spatial planning with a view to the implementation of the principle of digitalisation and cannot be applied generally to the data of the individual authority cases in ÉTDR.

### *III.6.3. Recommendation concerning the tasks of the municipal controller related to the creation of individual publication schemes*

In the period following local government elections and the establishment of the body of representatives in 2024, there was an increase in the number of submissions to NAIH, in which organs performing public tasks – making use of the authorisation set forth in Section 37(3) of the Privacy Act – wished to render their operation more transparent by creating individual publication schemes beyond mandatory ones. In every case, the Authority values and appreciates endeavours by organs performing public tasks when they publish the data of public interest or data accessible on public interest grounds that they process proactively in an electronic format ensuring wide access to them. The recommendation whose full text is accessible in the Authority's website provides assistance for its lawful and professional implementation[30].

30 https://naih.hu/informacioszabadsag-ajanlasok?download=1065:a-nemzeti-adatvedelmi-es-informacio¬szabadsag-hatosag-ajanlasa-az-onkormanyzati-adatkezelo-egyedi-kozzeteteli-lista-letrehozasaval-kapcsolatos-feladatairol

# IV. Cooperation with the data protection authorities of the European Union and international affairs

## *IV.1. Setting up an AI lab at NAIH*

The Authority decided at the end of 2024 to implement early in 2025 a new AI lab in addition to its existing Forensic Lab to enable a more effective authority supervision of AI models using its own resources over the long term as this requires special means and professional knowledge, as well as research in order to better understand the technology and the examination of the lawful practical utilisation of AI solutions. The Authority attaches priority to setting up the AI lab and endeavours to prepare for the technical challenges of the present and the future with the continuous training of its staff.

## *IV.2. Specific supervision of the Hungarian banking sector*

As AI systems have been spreading at significant speed as means of processing data, and the banking sector processes the personal data of millions of data subjects, the Authority wishes to gain an overview of what personal data are processed by the AI systems in the Hungarian banking sector for what purposes and in what way their compliance with data protection law is achieved. In this context, the Authority first contacted the Magyar Nemzeti Bank in 2024 for consultation and information sharing, and then selected several banks to which it sent a survey questionnaire as part of the specific supervision. Once this supervision is completed, the Authority will publish a general report on how and for what purpose the AI systems operate at the individual banks under study; this may help a number of data subjects to better understand the operation, proper use and risks of the AI systems. In the light of the information identified, the Authority will take any other steps that may be necessary to facilitate the enforcement of the right to the protection of personal data. With a view to pre-emptive operation and to facilitate the provision of appropriate information to data subjects, the Authority is planning specific investigations related to AI systems in other sectors also in 2025.

## *IV.3. Data governance*

As of 1 January 2024, the amendment to the Privacy Act designated the Authority to perform the tasks according to the Data Governance Act (DGA)[31], which has been in force since 23 June 2022 and has been directly applicable since 24 September 2023. Pursuant to Section 38(3)(j) of the Privacy Act, the Authority shall perform the tasks of the competent authority for the registration and supervision of data intermediation service providers and those of the competent authority for the registration and supervision of data altruism organisations specified in the Data Governance Act (Section 34/B-E of the Privacy Act governs the new authority procedural rules).

To supervise the requirements enshrined in the data Governance Act, the Authority upon notification launches an authority procedure according to the Code of General Administrative Procedure, or may launch an ex officio authority procedure at any time. In 2024, the Authority registered a Hungarian data intermediation service provider, the second in Europe after Finland. The guidelines and the new registers related to the Data Governance Act and the new procedures of the Authority are available on the Authority's website in a roll-down menu under "Data Governance". The Authority will continuously expand this information as the EU and Hungarian implementation decrees still in the legislative pipeline are adopted.

## *IV.4. Activity of the European Data Protection Board*

### *IV.4.1. Expert level structure*

The renewed expert subgroups of EDPB are the following: Borders, Travel & Law Enforcement; Compliance, e-Government, Health; Cooperation; Enforcement; Financial Matters; International Transfers; IT Users; Key Provisions; Social Media; Technology.

A new expert subgroup to be launched in 2025 is Cross-Regulatory Interplay and Cooperation. Two unique formations are the Coordinators, which is the meeting of the expert subgroup coordinators and the Strategic Advisory, which is a high-

31 Regulation (EU) 2022/868 on European Data Governance and amending Regulation (EU) 2018/1724

level expert body assisting the work of EDPB on individual issues. Through its experts, the Authority is represented in every expert subgroup.

*IV.4.2. The Coordinated Enforcement Framework (CEF) of the Supervisory Authorities*

Under the "Coordinated Enforcement Framework", the European Data Protection Board specifies a subject matter demanding priority attention each year. In 2024, it focused on compliance with Guidelines 01/2022 on data subject rights – right of access – on the implementation of the right of access by controllers in order to facilitate the efficient exercise of data subject rights and to encourage controllers.

Under the coordinated enforcement framework, the Authority wished to survey primarily the practices of domestic enterprises engaged in protecting assets, public utility providers and telecommunication service providers related to ensuring the right of access according to the GDPR, and contacted 14 controllers with its detailed questionnaire. The reason for selecting service providers also providing remote surveillance service in the asset protection sector was that because prior to 26 April 2019 Act CXXXIII of 2005 on the Rules of Activities Involving Personal and Property Protection and Private Investigation did not allow for data subjects to access copies of video recordings on them; copies of the videos could be issued only when required by an authority or a court. It was largely the property protection sector, which hardly received any access requests – only one out of the five controllers received such a request. The reason for this includes that in many cases these companies acted as processors, hence requests for the exercise of data subject rights were not submitted directly to them, hence they did not mention them in their answers, or the public may still have believed that a previous legislation before 2019 was in force, so they did not exercise their right to obtain copies. In the case of telecommunication service and public utility providers, the Authority assumed that data subjects exercised their rights in large numbers in this category of controllers.

The questionnaire survey showed major differences in the public utilities sector, presumably because one of the service providers received requests (more than 10,000) largely linked to the administration of cases by the customer service. It was noticeable that controllers, which did not receive data subject requests, did not develop internal procedures for dealing with access requests; however, some controllers indicated an intention to review their processing practices. One of the respondent controllers stated that should well-grounded doubts arise concerning the identity of the data subject, they asked for copies of ID of the data

subject requesting access. However, Guidelines 01/2022 (Sections 74-79) considers this practice as a risk to the security of personal data. In general, this method cannot be regarded as an appropriate one for authentication, except if it is necessary to comply with Member State requirements. The Authority found in the case of several controllers that the provisions of Section 111 of Guidelines 01/2022 are not complied with because they only inform data subjects about changes in the personal data processed or merely the changes in the processing itself since the last request. This is only acceptable, if the data subject gives his express consent. It was interesting that because of the burden of proof certain controllers answer the data subject's request even when they consider them ungrounded or excessive.

## *IV.5. Overview of cooperative procedures conducted pursuant to GDPR*

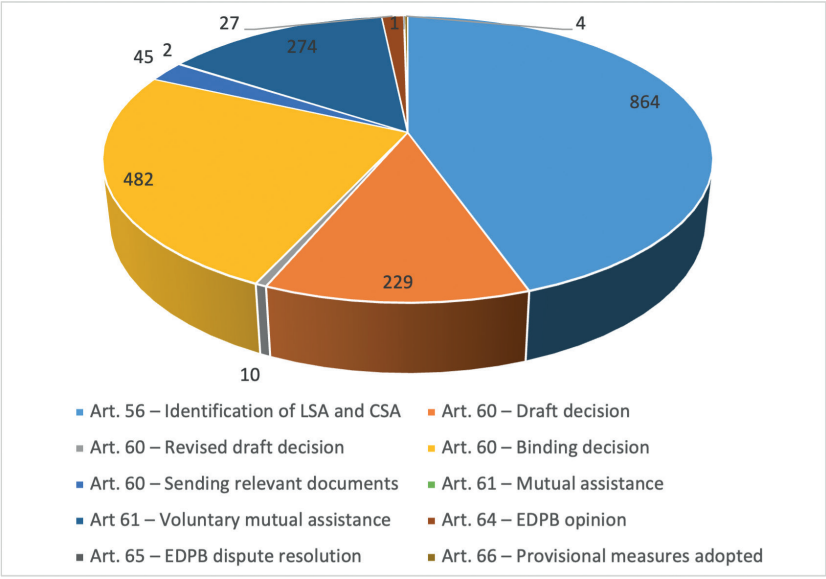



*Figure 1: Procedures received by NAIH*

Since the application of GDPR beginning in 2018, the Authority has taken an active part in the cooperative procedures according to Article 60 conducted with the Member States of the EEA. Based on the statistics kept since GDPR be-

came applicable in May 2018, it can be established that the trend of shifting the main focus of procedures between Member State authorities from the identification of the lead supervisory authority towards cooperation and communication is continuing.

In addition to providing opinions on draft decisions and the frequently recurring issues in voluntary mutual assistance procedures (processing issues related to cameras, insurance companies, messaging software), it should be underlined that checking identity by controllers in accordance with the GDPR continues to be a challenge for controllers in the territory of the European Union. A popular site offering accommodation categorised Hungary as one of the countries that do not offer an appropriate alternative to sending a copy of an ID card, but the Hungarian authority disagreed with this decision. An alternative solution supported by the Authority could be the presentation of the original document in the course of a secure online video call, or using the magyarorszag.hu service. The convenience of the controller and making minimal savings on costs are no reason for exemption from the obligations under the GDPR. Uploading an image of the ID card is not suitable for achieving the purpose and violates the principle of data minimisation according to the practice of the Hungarian authority.

The one-stop access[32] serves the investigation of cases launched on the basis of complaint-related trans-border processing or ex officio procedures. Communication among the authorities involved in the cooperative procedures is conducted via an interface specifically transformed for these procedures in the Internal Market Information System (hereinafter: IMI system). Details of these procedures have been presented in previous reports (for instance in the one for 2023).

In 2024, the Authority received 864 cases from the authorities of other Member States through the IMI system. Of these, the Authority found itself concerned in more than 280 cases; it acted as the lead supervisory authority in seven procedures; however, in 2024, it did not launch a single procedure according Article 56.

In 2024, one dispute settlement procedure was launched against the draft decision of the French Authority according to Article 65 (which is still in progress). No dispute settlement procedure has yet been launched against any draft decision of the Authority.

32 Article 60 of the GDPR

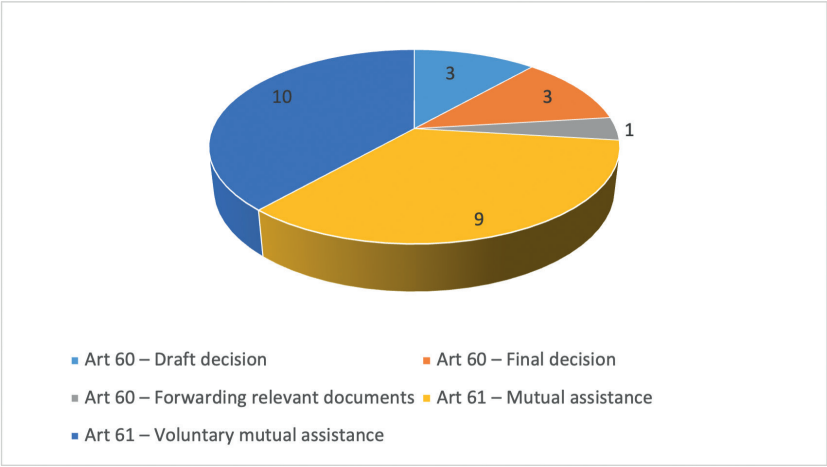



*Figure 2: Procedures launched by NAIH*

## *IV.6. NAIH as the lead supervisory authority*

The complaints in question were received from Polish, Dutch and French complainants; they were fundamentally related to granting erasure requests submitted to a Hungarian transportation company, affecting processing of roughly the same period (2018, 2019). The controller performed the erasure requests (at least in part) in all three cases only after the deadline and it either failed to notify the data subject of extending the deadline, or refer to non-lawful reasons (citing only the large number of similar requests, but as this does not make the specific requests either complex or numerous, this could not be a lawful reason for extending the deadline). There have been cases, where the erasure request was delayed because of the erroneous filing of the request and that was why they failed to extend the deadline. And there was the additional problem that, in view of the erroneous filing, the controller requested additional information from the data subject, which may have given the impression that it made compliance with the erasure request conditional. In the case of the French complainant, the controller performed the erasure with a delay without extending the deadline. In the case of the Dutch complainant, the erasure of the account was not carried out even within the unlawfully extended deadline, in addition, the account erasure which was done with additional delay was not full, and thus additional erasure operations were needed. In the case of the Polish complainant, the erasure of

the account was implemented within a month, despite the unlawfully extended deadline, but the erasure was not full, hence an additional erasure operation carried out with an additional delay became necessary also in this case.

The controller notified the data subjects of the implementation of the erasure operations either with a delay or not at all. In addition, the notifications either did not provide any information, did not provide it in a transparent matter or provided it expressly erroneously on the processing continued after the erasure. The controller stated in all three cases before the Authority that it continued to process the data of the data subjects even after erasure for purposes of providing evidence in authority procedures (which is incidentally a legal obligation and contrary to the controller's position not a legitimate interest), and for recording activities related to the enforcement of the data protection rights of the data subject. In relation to the latter, with reference to Section 105 of judgement C-439/19 of the Court of Justice of the European Union and GDPR Recital (64), the Authority underlines that controllers are not under an obligation to process personal data only to comply with the GDPR. If so interpreted, GDPR Article 5(2) as a restriction on erasure would essentially render the data subject's right to self-determination impossible because erasure would never be carried out, or if so, only with a substantial delay.

Based on all this, the Authority – in addition to imposing a fine – established the infringement of GDPR Article 5(1)(a), Article 12(3), Article 6(1) and Article 17(1)(a) and (b), and ordered the controller to erase the personal data processed for the purpose of recording activities related to the enforcement of the data protection rights of the data subject.

In another case, a Romanian complainant unsuccessfully attempted several times to unsubscribe from the controller's newsletter by clicking on the unsubscribe button at the end of the e-mail and by completing the form for this purpose on the website, despite the fact that the data protection officer of the controller reassured him that his e-mail address was deleted from the newsletter database as requested and he was unsubscribed from the newsletters. The ex officio authority procedure found that the Controller, using a system ridden with technical problems as was acknowledged by it, as a result of which it did not erase the Complainant's e-mail address from the Controller's newsletter database, the Controller failed to take the necessary technical measures to ensure data subject requests, infringing thereby Article 25(1) of the General Data Protection Regulation.

## *IV.7. Law enforcement and judicial cooperation – Hungary's evaluation for data protection under the Schengen Convention in 2024*

In accordance with the Schengen monitoring and evaluation mechanism for the period 2023-2029, Hungary's evaluation took place in the summer of 2024. In the course of the onsite evaluation for data protection conducted between 2-7 June 2024, the representatives of the Commission and the data protection experts designated by the Member States visited the Authority as the competent national body responsible for overseeing the appropriate implementation of the EU and national data protection regulations related to the Schengen Information System and the Visa Procedures. The staff of the Authority presented the relevant national regulations, the organisation, functions and powers of the Authority, its supervisory activities, as well as the results of the data protection audits carried out at the Hungarian organs having access to the Schengen Information System and the Visa Information System. They also presented the process of exercising data subjects' rights, the statistical data related to submissions to the Authority, the information documents accessible on the Authority's website, as well as international cooperation with the data protection authorities of the Member States.

The next stop of the evaluation programme was the N.SIS Office at the Deputy State Secretariat in charge of keeping the records at the Ministry of the Interior, where the legal regulations pertaining to the Office and the structure and activities of the organisation were presented, followed by presentations by colleagues present representing the companies responsible for operation and development. Then the delegation visited the server room accommodating the NS.CP server and the national interface. The next day, the evaluation continued at the 5th District Police Station, and then at the SIRENE Office. The head of the SIRENE Office presented the operation of the organisation, its tasks, the legal background for their activities and the statistical data of the requests received by them. The delegation viewed the premises of the SIRENE Office, as well as the IT operation of the SIS system. At the National Directorate General for Alien Policing, their tasks related to processing carried out in relation to the Schengen Information System, their cooperation with partner authorities and the SIRENE Office, the modes of exercising data subjects' rights, the process of managing requests received by the Directorate General and the relevant statistical data, as well as the legal environment, architecture, operation and development of the National Visa Information System were presented. At the Ministry of Foreign Affairs and Trade, after the introduction of the Consular Service and presentations by the data protection officer, the organisational unit running the Consular Information System and the developers of the visa system, the group carrying

out the onsite inspection visited the central server room of the Ministry of Foreign Affairs and Trade. Finally, the delegation visited the Airport Police Directorate where the organisation's activities related to data protection, the border checking procedures and devices were presented. To close the programme, the members of the expert group and the representatives of all the organs concerned met for a joint consultation.

# V. Cases of litigation for the Authority

In 2024, the Authority had altogether 35 closed cases of litigation at the Municipal Court of Budapest or the Curia.

Of this, the Authority won 22 cases in full, the court rejected even the petition in one lawsuit, the court terminated one lawsuit, and the Authority partially won three lawsuits and lost litigation in six cases only.

In 2024, the Authority imposed fines of HUF 355,185,000, of which HUF 350,130,000 was data protection fine, HUF 4,955,000 was procedural fine and HUF 100,000 was enforcement fine. Of the fines imposed, including the late payment penalty, HUF 276,382,411.00 was paid voluntarily by the obligors, while an enforcement action by NAV was taken in connection with fines of HUF 14,830,000.00, i.e. about 78% of the fines imposed were paid voluntarily by the obligors. This shows a 16% increase compared to the amount of fines paid voluntarily in the previous year and it clearly indicates the inevitability of the payment of fines and the improvement in the willingness of those liable to pay them. Fewer and fewer debtors are risking enforcement proceedings by the NAV.

Based on the Authority's experiences with litigation, it can still be concluded that the emphasis of litigation is on administrative lawsuits following data protection procedures launched upon request, but 20% of the cases closed in 2024 were related to decisions taken in ex officio authority procedures. In the sixth year of the application of the General Data Protection Regulation, it can be said that the Authority has to deal with increasingly complex data protection law issues, both factually and legally. The number of administrative cases brought against the Authority was 37 in 2023 and 22 in 2024, i.e. almost 40% fewer cases were initiated. The decrease in the number of litigations suggests that data protection awareness of individuals in the area of their rights has increased and that, in parallel, controllers are also striving to comply with the law, in particular since the adoption of the EDPB Guidelines on the calculation of administrative fines, which allow the Authority to impose much higher data protection fines.

Below we highlight some of the more interesting and significant court cases.

## *V.1. Claims enforced against Meta Platforms Ireland Limited for the infringement of the right to privacy*

*The facts of the case*

The respondent is a provider of the social media service “Facebook”, with its registered office in Ireland and its centre of business is also in Ireland. On Facebook, users can, among other things, create profiles and pages which allow them to share information about themselves with others in the form of posts, photos, etc. It is also possible to share such information posted by other users on their own page, as well as to comment on information and content posted on other people’s pages.

Clause 4.2 of the Facebook Terms of Use (hereinafter: Terms of Use) provided the possibility for the respondent to suspend or permanently block a user’s access to their account in case of a clear, serious or repeated violation of the Terms of Use or other policies of the respondent, including in particular the so-called Community Principles. If the provisions of Clause 3.2. 1-3.a of the Terms of Use are violated, if Facebook removes any content shared by the user due to a violation of the Community Principles, it will inform the user and explain the options available to request a repeated review, unless the user is in serious or repeated breach of the Terms of Use, or if by doing so Facebook would expose itself or other to legal liability, harm the user community, impede or hinder the operation or integrity of Facebook’s service, system or product, or if this possibility is prevented by technological limitations, or if it is prohibited from doing so by legal reasons. Pursuant to Clause 3.1 of the Terms of Use, the content once deleted will cease to be visible to other users, immediate deletion is not possible due to technical limitations, and it will be effectively deleted within a maximum of 90 days from the date of deletion.

Similar rights were granted not only to the respondent, but also to the operator of the page concerned. The persons who managed the specific Facebook page (three roles are relevant to the dispute: the administrator, the editor and the moderator) were all entitled to reply to comments and posts on the page, to delete them from the page or to “ban” or “block” another Facebook user from the page. The administrator and the editor also have the right to create and delete posts on behalf of the page, and to edit the page. In addition to that, administrators also have the ability to manage roles and settings for the page. When a Facebook user created a page, they automatically became its administrator.

When a user's profile is "blocked", the blocked user will not be able to see the content posted by the blocking user, will not be able to access it, and will not be able to find the page and view the posts posted there. When a user is "blocked", the blocked user can view the content of the page, but cannot comment on posts. Users banned or blocked by another user will not be notified of the action.

Facebook's Privacy Policy (15/A/3) indicated the contact details of the controller responsible for the data and the data protection officer, and specified the data that the respondent processes in support of the services it offers. In this context, the respondent collects information and content provided by the user when using Facebook, collects data on the people, accounts, Facebook pages and groups to which the user is connected, the way in which the user interacts with them, and the intensity of the interaction. It collects information about how he uses the service, such as what types of content he views; it logs when he uses the service, which posts and content he views. According to the Privacy Policy, the respondent may use these data to provide and support the respondent's products and services, as defined in the Terms of Use, to the user. The Privacy Policy also includes the manner in which such data may be used and shared, the legal basis for processing, a notice for the possibility to exercise the rights granted by the GDPR.

Only the so-called "help centre" provided information about the roles (five different roles) associated with each page, and that if a user blocks the profile of another user, the blocked person will not be notified that the profile has been blocked. The "Activity Log" is a Facebook feature that allows users to review and manage their activity, it includes the posts they have made, activities on the pages, comments by others, messages, other activities.

The petitioner, as a Facebook user, noticed in the months of August and September 2021 that the comments he had previously made to articles and posts shared on the public figure's Facebook page were no longer available either on the designated page or in his own activity log, and that he could no longer comment on articles and posts shared on the public figure's Facebook page. In the course of the lawsuit, he noticed that in 436 cases his comments made between 1 October 2020 and 21 October 2022 were deleted (became inaccessible), while in 110 cases the information about the recipient of the comment was also deleted.

*The petition*

In his petition, the petitioner sought a declaration, pursuant to Section 2:51(1)(a) of the Civil Code, that the respondent, as controller, had violated his personal rights to freedom of expression and human dignity, and to the protection of personal data and human dignity.

Because of the above infringements, the petitioner requested on the basis of Section 2:51(1)(b) of the Civil Code that the court prohibit the respondent from committing similar infringements in the future, so that no decision (blocking) can be applied against users who identify themselves as public figures in the Facebook system as representatives of the Facebook page in question (editor, moderator, administrator), as they are entitled to make decisions, in relation to their past and future comments and reactions, which would result in the restriction or prohibition of their right to express their opinion or the deletion of their comments. Pursuant to Section 2:51(1)(d) of the Civil Code, he asked that the respondent be ordered to do away with the prejudicial situation by restoring access to the public figure's Facebook page and his deleted posts within 15 days and by restoring all his subsequently deleted posts (110+436).

According to the petitioner's argument, the respondent is not only a passive hosting provider, but also a controller in its own right (but at least acting in common with the "administrators" of the pages blocking him) (GDPR Article 4(7); GDPR Article 26). He himself is a "data subject" within the meaning of GDPR Article 4(1), and his comments are so-called "sensitive personal data" within the meaning of GDPR Article 9(1). The deletion of his personal data (the comments) stored in the system operated by the respondent is a processing operation within the meaning of GDPR Article 4(2). Even if it was not the respondent who deleted the comments, the hosting and the system developed and operated by it allowed third parties (administrators, editors and moderators) to delete the comments, and therefore it is also a controller. Solely the respondent can be held liable for the deletion of his comments not only from the Facebook pages accessible to all, but also from his activity log. The respondent's processing is unlawful in the absence of the conditions laid down in GDPR Article 6(1). Under the (reverse) burden of proof rule applicable under GDPR Articles 5, 24 and 82, it is for the respondent to prove that it cannot be held liable for this. By accepting the Terms of Use (which cannot be considered as a waiver), he accepted only the legal consequences of lawful blocking and deletion, not the restriction in the case at hand. The content of the Terms of Use that is contrary to the GDPR shall be disregarded. The respondent should not have provided the possibility to third

parties (administrators, editors and moderators) for deletion and ban in connection with a public figure's page, but if it had done so, it would have been obliged to operate the system in conformity with the GDPR pursuant to Articles 24(1) and 25(1) to (2).

The respondent's processing in breach of the norm and the shortcomings of the supply of information led to the fact that he was unable to exercise his rights as a data subject properly. The Privacy Policy only identifies the respondent, without any reference to the processing of data by the administrators of individual sites, the relationship between the respondent and these administrators, the division of responsibilities and rights. The possibilities for the exercise of data subject's rights are not transparent, such processing is not fair.

In his view, by its above conduct, the respondent violated the following principles of the GDPR concerning the processing of personal data: (1) the principles of "lawfulness, fairness and transparency", because it did not provide adequate prior information on the processing (GDPR Article 5(1)(a)); (2) the principle of "purpose limitation", because his comments were not only inaccessible to the public, but also to him, and he was unable to comment on the page (GDPR Article 5(1)(b)). (3) the principle of "integrity and confidentiality", because he has not taken appropriate technical and organisational measures to protect his personal data against loss or destruction, which means that his data cannot be modified and are no longer accessible to him (GDPR Article 5(1)(f)).

In order to enable the petitioner to win in the action, NAIH, which intervened in the case, requested a decision in accordance with the petitioner's claim – solely in respect of the action for infringement of the petitioner's right to the protection of personal data. It argued that the respondent was a joint controller (GDPR Article 26) with the other Facebook user who applied the deletion and the ban, because it participated in the determination of the means and purposes of the processing through the operation and functionality of the software used for that purpose (by designing the conditions of processing). In the absence of proof of the lawfulness of the processing by the respondent pursuant to Section 23(2) of Act CXII of 2011 on the Right of Informational Self-Determination and Freedom of Information (hereinafter the Privacy Act), joint controllers are jointly and severally liable pursuant to GDPR Article 82(2) and (4).

For a correct interpretation of the GDPR, it referred to the European Data Protection Board's (EDPB) Guideline 7/2020. It pointed out that the capacity of controller does not require that the controller has access to the data being pro-

cessed, and that joint processing can take the form of joint decisions, as a result of coordinated decisions, if the decisions are complementary and inseparable. It pointed out that the respondent's status as controller has been established by the Court of Justice of the European Union (CJEU) in several judgments (CJEU C-319/20; C-645/19). In its judgment in Case C-210/16 Wirtschaftsakademie Schleswig-Holstein (paragraph 26 et seq.), the CJEU held that the administrator of a social network site and the respondent were joint controllers. The CJEU also confirmed in its judgment C-40/17 (Fashion ID) that the decision of an organisation to use for its own purposes a tool or other system developed by another organisation which allows the processing of personal data is likely to constitute a joint decision on how those organisations process personal data.

The Court of First Instance dismissed the action.

The judgment of the Court of Second Instance found in connection with the deletion of the petitioner's comments from the activity log that, contrary to the judgment of the Court of First Instance, the respondent had infringed certain provisions on data processing, including fundamental principles. However, as the petitioner's action as a whole was aimed at enforcing sanctions under the law for personality protection (and not specific data protection under the Privacy Act), but despite the data processing infringements the Court did not find that the respondent had infringed the personality rights, which were the subject of the action, and a retrial at first instance was not justified either by the examination of the adequacy of information by the respondent or by the fact that the respondent would have been required under Section 23(2) of the Privacy Act to prove the lawfulness of the processing of the data during the proceedings at first instance, but no such evidence was provided on this point.

Following the petitioner's action for review, the Curia held that in this case the Curia had to assess whether the courts acting in this case had infringed the substantive provisions of law identified by the petitioner in the application for review – including Article 2:43(e) of the Civil Code protecting the right to the protection of personal data – and whether they had interpreted that provision in accordance with the constitutional content of the Fundamental Law and given it sufficient effect.

The petitioner also claimed that his right to the protection of personal data had been infringed [Section 2:43 (e), Civil Code], and based on the infringement of these personal rights, he requested the application of the legal consequences set out in Section 2:51(1)(a), (b) and (d) of the Civil Code. There is no doubt

that the court of second instance did not provide detailed grounds for rejecting the application of the objective legal consequences. However, since it was clear from the final judgment that the court of second instance was of the opinion that the conduct which the petitioner listed as the alleged basis of the infringement did not lead to the infringement of the petitioner's personality rights, it follows reasonably, without any further justification, that it did not consider that neither the objective sanctions for the infringement of the personality rights, which were not attributable to the applicant, nor the subjective ones, could be applied.

The petitioner did not request the payment of HUF 1,000,000 by the respondent solely on the legal basis of Section 2:52(1) to (3) of the Civil Code, but also claimed this amount on the basis of GDPR Article 82(1) and (2), as compensation for non-material damage. In paragraph [64] of the final judgment, the Court of Appeal, citing the provisions of GDPR Article 82(1) to (3), held that the petitioner's personality rights had not been infringed which in the Court of Appeal's view excluded the petitioner's claim on that ground as well. Following from all this, in the final judgment, the Court of Second Instance gave reasons for rejecting the petitioner's claims on various grounds, and the other deficiencies in the statement of reasons for the final judgment on the other issues raised in the petition for review (the split of the processing operations into 'phases', the assessment of the respondent's capacity as joint controller) alone did not justify a reopening of the proceedings or a new decision, since they did not affect the assessment of the merits of the case, for the following reasons.

During the proceedings, the petitioner claimed that the deletion of his comments and those of their addressees left him in a vulnerable and humiliated position, feeling stigmatised; the loss of evidence, the obstruction of the exercise of his rights as a data subject filled him with tension and fear. Even if these circumstances are accepted, they are not sufficient to establish an infringement of the personality rights mentioned in the petition, as referred to in Section 2:42(e) of the Civil Code, and the processing of the data by the respondent does not, in the opinion of the Curia, constitute an attack against the petitioner's privacy and his personality rights in the case in question. The respondent did not infringe the petitioner's right to the protection of personal data, and therefore the merits of the case were not affected by the reasoning of the judgment of the court of second instance – which otherwise does not state a legal basis – that the right to the protection of personal data is due only in the event of "unauthorised acquisition of personal data, disclosure to an unauthorised person or disclosure to the public". The unfoundedness of those grounds alone did not affect the assessment of the

merits of the case, and for that reason the final judgment could not be repealed on the basis of Section 423(3) of the Civil Code.

Nor does the petitioner's review argument justify the repealing of the final judgment that the final judgment infringes the concepts of processing and controller in GDPR Article 4(2) and (7), the tasks of controller in Article 24(1), the concept of joint controller in Article 26 and Article 82(1). In the present case, the parties have not challenged by way of review the points in the final judgment that the respondent infringed the obligation to inform under GDPR Articles 12(1) and 13(2)(a), the controller's tasks under Article 24(1), the data protection obligation by design and by default under Article 25(1), the principles of lawfulness, fairness, transparency and integrity under Article 5(1)(a), and those of confidentiality under Article 5(f) by deleting the petitioner's comments and their addressees from his activity log. Therefore, the Curia had to decide whether the petitioner had proven any disadvantage suffered in connection with the respondent's infringing conduct that would justify the application of the legal remedy under GDPR Article 82(1).

It follows from the wording of Article 82, as it transpires from the justification of the CJEU judgment in Case C-300/21, that the existence of "damage" or "damage suffered" is one of the conditions for the right to compensation referred to in that provision, as is the existence of a breach of the GDPR and the existence of a causal link between that damage and the breach. Therefore, it cannot be considered that any "breach" of the provisions of the GDPR per se opens the right to compensation in favour of the data subject, such an interpretation would be contrary to the wording of Article 82(1) of the said Regulation. A data subject who suffers negative consequences as a result of a breach of the GDPR is not exempted from proving that those consequences constitute non-material damage within the meaning of Article 82 of that Regulation. According to the interpretation of the law by CJEU upheld in several of its judgments (C-340/21, C-456/22, C-667/21), the concept of damage under recital 146 of the GDPR must be interpreted broadly, and in such a way as to fully reflect the objectives of the Regulation. The provisions of the GDPR cannot, however, be interpreted in such a way that any breach of a provision of the Regulation in itself gives rise to a right to compensation, and cannot be derived from the concept of "damage" or "damage suffered."

It is clear from the above-mentioned judgments of the CJEU that the person affected by a breach of the GDPR, to whom it has adverse legal consequences, has the burden of proving that those consequences have caused non-material

damage within the meaning of GDPR Article 82. Hence, the practice of the Curia is also in line with GDPR Article 82 and the judgments of the CJEU, according to which a possible violation of the data subject's rights does not in itself automatically result in an infringement of the privacy of the data subject, and the violation of data protection rules is not in itself sufficient to impose legal consequences, (Curia Pfv.IV.21.084/2020/4., Pfv.IV.21.251/2021/8.). In the case of an action based on GDPR Article 82(1), it is not sufficient to prove a breach of the data processing rules either, and the additional condition for compensation is to provide proof of the adverse consequences affecting the petitioner and causal link.

In view of all the above, the Curia found that the court of second instance did not violate the legal provisions indicated in the petition for review and it did not deviate from the published decision of the Curia on a point of law, therefore the final judgment has been maintained in force on the basis of Section 424(1) of the Civil Code. Court of Appeal [Kúria Pfv.IV.20.003/2024/13.].

## *V.2. The Budapesti Elektromos Művek Zrt. case at the Court of Justice of the European Union and its afterlife in Hungary (C-132/21.)*

The Municipal Court of Budapest sent the following questions to the Court of Justice of the European Union (CJEU):

Should 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 court appeal provided for in Article 79 constitutes an instrument for the exercise of private rights? If so, does it follow from this that the supervisory authority competent for administrative appeal has primary competence to establish the fact of the infringement? If the data subject, who considers that the processing of personal data relating to them has infringed the General Data Protection Regulation, exercises both the right to lodge a complaint under Article 77(1) of the General Data Protection Regulation and the right to judicial remedy under Article 79(1) of the General Data Protection Regulation, which interpretation is consistent with Article 47 of the Charter of Fundamental Rights:

a.) that the supervisory authority and the court have an obligation to examine the existence of an infringement independently from one another, 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 independent legal status of the supervisory authority granted by GDPR Articles 51(1) and 52(1) be interpreted as meaning that the supervisory authority, in its procedure and in its decision on a complaint under Article 77 is independent of the final judgment of the competent court under Article 79 and may therefore reach a different decision on the same alleged infringement.

The Authority also intervened on its own behalf before the Court of Justice of the European Union in this case.

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 of Fundamental Rights of the European Union must be interpreted as permitting the remedies provided for on the one hand in GDPR Articles 77(1) and 78(1), and on the other hand in Article 79(1) to be exercised concurrently with and independently of each other. It is for the Member States to lay down detailed rules in accordance with the principle of procedural autonomy with regard to 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 as referred to in Article 47 of the Charter.

After the respondent's decision, the Municipal Court of Appeal examined the relationship between the final judgment of the Civil Division of the Municipal Court of Budapest and the respondent's decision on the basis of the administrative procedural order and the judgment of the CJEU.

According to the Municipal Court of Budapest, paragraphs [54]-[56] of the CJEU judgment are relevant for the resolution of the case insofar as it states in relation to GDPR Articles 78 and 79 that conflicting court decisions would weaken the protection of natural persons with regard to the processing of their personal data, which would lead to legal uncertainty due to lack of consistency. The Municipal Court of Budapest decided to annul the Authority's decision and ordered it to conduct a new procedure, and instead of the Authority's interpretation of the law,

it followed the final judgment of the Municipal Court of Appeal in the parallel civil proceedings on the substantive data protection issue.

The Curia, however, upon the Authority's request for review, ruled that where, as a result of parallel appeals, the final judgment of the civil court in a given case precedes the final judgment of the administrative court in time, but the interpretation or application of EU law under the civil judgment is erroneous, as in the present case, as the Curia held, the administrative court that subsequently rules may depart from the final judgment of the civil court. In the present case, the administrative court, i.e. the court of first instance, could have departed from the judgment of the civil court. [Kúria Kfv.V.37.595/2023/6].

The Municipal Court of Budapest examined the legality of the respondent's administrative act in the retrial on the basis of the guidelines for retrial of the Curia order and found that the CJEU judgment answered the parallelism between the civil judicial remedy, jurisdiction and the administrative remedy (respondent's powers, administrative remedy, jurisdiction) by stating that the issue falls within the jurisdiction of the Member State. The court of first instance therefore rightly stated that – although the CJEU judgment held that it is for the Member States to lay down detailed rules governing the relationship between parallel legal remedies in accordance with the principle of procedural autonomy – there is no such detailed regulation in the Hungarian legal system. However, having established the existence of Member State competence and the absence of detailed regulation in Hungary, the judgment erred in its conclusion drawn from paragraphs [54] to [56] of the CJEU judgment (which, as regards the relationship between GDPR Articles 78 and 79, stipulated that conflicting judicial decisions would weaken the protection of natural persons with regard to the processing of their personal data and would create legal uncertainty due to the lack of consistency).

Consequently, if the final judgment of the civil court in a specific case precedes the final judgment of the administrative court in time due to parallel appeals, but the interpretation or application of EU law under the civil judgment is erroneous, the administrative court that subsequently decides may depart from the final judgment of the civil court.

In the light of the above, the court dismissed the petition on the basis of Section 88(1)(a) of the Code of Administrative Court Procedure [Fővárosi Törvényszék 105.K.700.069/2024/7.].

## *V.3. Obtaining identity data and social security number for natural persons from a public administrative body for the purpose of providing financial assistance during the COVID-19 pandemic*

In February 2020, Controller3 decided to provide financial support in the form of vouchers to residents belonging to groups at risk of the Covid-19 pandemic, who met certain conditions (e.g. reaching retirement age, eligibility for certain social benefits). In order to obtain the personal data necessary to establish the eligibility criteria – in particular natural person identification data and the social security number – it contacted Controller1 and Controller2, who complied with its requests. Controller3 aggregated the data received in a database and created a unique identifier and barcode for each set of data. The payment of the aid was governed by municipal regulations, which contained the conditions of eligibility for the aid. Data subjects were notified about their eligibility for the aid in a customised form.

By its decision, the Authority found that Controller1 breached the principle of lawfulness under GDPR Article 5(1)(a) by complying with the request of Controller3 without examining its lawfulness and GDPR Article 6(1) by providing Controller3 with the data relating to the data subjects affected by the data request in March 2020 without a proper legal basis.

Controller2 infringed GDPR Article 5(1)(a) by complying with the request of Controller3 without examining its lawfulness.

Pursuant to GDPR Article 58(2)(d), the Authority ordered the petitioner (Controller3) to delete the personal data of data subjects who were eligible to receive the aid on the basis of the information provided by Controller1 and Controller2 but who did not submit a request to Controller3.

In its petition, the petitioner also claimed, inter alia, that the respondent should not have had the right to order the deletion on the basis of Article GDPR 58(2)(d), and in this context it also requested the initiation of a preliminary ruling procedure.

The court suspended the proceedings and referred the following questions to the Court of Justice of the European Union (CJEU) for a preliminary ruling:

1) Is Article 58(2) 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 (EC) No 95/46/EC (hereinafter: GDPR) to be interpreted – with special regard to points (c), (d) and (g) thereof – as meaning that the supervisory authority of a Member State, acting in its corrective capacity, may order the controller or processor to erase personal data processed unlawfully, even without an explicit request from the data subject pursuant to GDPR Article 17(1)?

2) If the answer to the first question is that the supervisory authority may order the controller or processor to erase unlawfully processed personal data without a request from the data subject, is this irrespective of whether the personal data were collected from the data subject or not?

By judgment C-46/23 of the CJEU (hereinafter: CJEU judgment), the CJEU ruled that GDPR Article 58(2)(d) and (g) should be interpreted as follows:
In the exercise of its corrective powers under those provisions, the supervisory authority of a Member State is entitled to order the controller or processor to erase personal data processed unlawfully, even where the data subject has not made a request to that effect in order to exercise their rights under Article 17(1) of this Regulation. GDPR Article 58(2) should be interpreted as follows: the power of the supervisory authority of a Member State to order the erasure of unlawfully processed personal data may cover both data collected from the data subject and data obtained from other sources.

On the basis of the CJEU judgment, the Municipal Court of Justice dismissed the petition as unfounded on the basis of Section 88(1)a) of the Code of Administrative Court Procedure.

## *V.4. Establishment of client status*

The non-litigant applicant filed a request for a data protection authority procedure (hereinafter: “authority procedure”) against the non-litigant Transplant Committee (hereinafter: the “petitionee”) in connection with the data processing of the transplant waiting list, requesting, inter alia, data on the delivery to the petitionee and the clinic providing care.

Following the above, the Authority issued an order to notify the petitioning university of the fact and subject matter of the Authority’s proceedings and of the involvement of the Hungarian National Blood Transfusion Service (hereinafter: OVSZ) as a client. Noting that the case directly concerned the petitioner’s rights

and legitimate interests, it granted the petitioner client status in the procedure and invited it to provide information on questions 1 to 9 of the order, within a time-limit, in order to clarify the facts. In the justification of the order, it referred to Section 10(1) of Act CL of 2016 on the Code of General Administrative Procedure (hereinafter: Code of Administrative Procedure) and to the fact that, from the documents submitted by the OVSZ, it can be established that the respondent's members (the members of the committee) carry out their work on the basis of a contract of engagement concluded with the petitioner as the principal, that the petitioner gives instructions to the members on this basis and that the petitioner prepares the petitionee's report. The petitioner also has control over the petitionee's assets on the basis of a contract concluded with the OVSZ and the OVSZ provides non-reimbursable support to the petitioner for the petitionee's operations. In that context, the OVSZ referred to the agreement concluded between the petitioner and the OVSZ on the delegation of tasks.

In its petition, the petitioner sought primarily the annulment of the order and secondarily that it be set aside, complaining in essence that the justification of the order does not even make it possible to establish the facts on the basis of which the status of a client could be ascertained, because the justification does not establish any link between the subject-matter of the case and the petitioner, it does not indicate the data in respect of which the petitioner is subject to the authority procedure, the petitioner refers to access to data managed by a Waiting List Committee as appropriate. The respondent deduced the petitioner's status as a client from the documents annexed by the OVSZ, but does not specify how the documents support the petitioner's status as a client.

For the first time since the entry into force of the GDPR, the Municipal Court of Budapest had to decide whether, on the basis of the information contained in the justification of the order, the respondent had lawfully decided that the case subject to authority procedure directly affected the petitioner's rights and legitimate interests and that it was therefore necessary to grant it client status in the procedure.

The substance of the administrative dispute was whether the determination of the legal status of client could be challenged on the basis of legal rules per se. Sections 10(1) and (2) of the Code of General Administrative Procedure provide for subjective and objective client capacity. The respondent granted the petitioner client status on the basis of Section 10(1) of the Code of General Administrative Procedure, since there is no law or government decree which, in the procedure before the data protection authority, would in itself confer client status on

the petitioner. According to Section 10(1) of the Code of General Administrative Procedure, the directness of a right or legitimate interest is to be interpreted in relation to the case and the description of the case is determined by a combination of a number of factors. Also according to the Great Commentary on client capacity of the Code of General Administrative Procedure "the involvement of the client with respect to the right or legitimate interest of the client must always exist in relation to the administrative decision. This means that it must be assessed in relation to the legal relationship which is the subject of the procedure. The directness of the right or legitimate interest in the case means that, if the respondent identifies it, it is lawful to involve the given legal entity in the procedure.

The authority procedure was initiated by the petitioner against the petitionee for access under the GDPR, and the case is therefore essentially delimited by the content of the petition. The petition also refers to the petitioner's organisational unit, which foreshadows the indirectness of the petitioner's involvement in the case. According to the legislation, the petitioner is undoubtedly separated from the respondent organisationally and economically, but in general, in procedures before public authorities, including the authority procedure conducted by the respondent, the facts necessary for the substantive determination of the case typically change (mostly expand) at different stages of the procedure. For this reason, the client status in a case can neither be established nor excluded on the basis of the legal norms applicable to the case as such. Direct legal involvement cannot be ruled out by reference only to statutory duties, because this would imply, in addition to the prior delimitation of the substantive law relevant to the case, the assumption that the legal norms and their application (facts) correspond exactly in every case.

The determination of the client status is a procedural question. However, the arguments put forward by the petitioner were expressly based on substantive law, from which the summary assertion was derived that direct involvement could not be at issue because the petitioner's and the petitionee's tasks, organisation and data processing were not interrelated. The essence of the case cannot, however, be whether or not the petitioner is, for example, a joint controller, since such and similar issues are a matter for the merits of the case before the authority. By contrast, in authority procedures, the direct involvement of the petitioner must be decided on the basis of the general concept of a client, on the basis of facts and information which the respondent has but on which a decision cannot yet be based. The restrictive interpretation of the petitioner (in relation to substantive law), which is inherent in the procedural nature of client status, cannot be accepted either because upholding the petitioner's claim would mean that, in the

authority procedure still pending, the petitioner's status as client could not subsequently be based on facts not yet known to the respondent.

The respondent rightly established the petitioner's client status in the procedure not on the basis of the substantive law but on the basis of the content of the documents at its disposal, without deciding on the merits of the case. Thus, the justification of the order contains sufficient, documentary and reasoned grounds in relation to the performance of the duties, the assets and the contractual relationship between the members of the petitionee and the petitioner, which the court does not repeat. The facts known to the respondent at the time the order was made in the authority procedure sufficiently demonstrate that the petitioner's rights and legitimate interests are directly affected by the case. Therefore, the respondent lawfully involved the petitioner in the procedure. The pleas in litigation relating to legal status and the separation of legal relationships were not decisive in the present dispute.

On the basis of the above, the order of the respondent is lawful in the scope of the petition, therefore the court dismissed the petition on the basis of Section 88(1)(a) of the Code of Administrative Court Procedure [Fővárosi Törvényszék 105.K.700.152/2024/10.].

### *V.5. Decisions of the Curia in review proceedings concerning the data protection authority procedures on request in connection with surveillance using the "Pegasus" spyware*

In 2021, the Authority conducted an investigation concerning the application of the "Pegasus" spyware in Hungary, in view of the fact that according to the news published by the media, personal data may have been unlawfully processed using the spyware. The Authority published the parts of the findings of its ex officio investigation in 2022, which could be made available to the public. After this, several petitions were received for conducting authority procedures for data protection requesting investigation of the unlawfulness of processing personal data in relation to the surveillance of the petitioner by the Pegasus spyware and ensuring the petitioner's data subject rights according to Section 14 of the Privacy Act in accordance with Section 71(1a) of the Privacy Act.

In these cases the Authority conducted the procedures 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 through the involvement of the Authority and it informed the data subjects – in accordance with Section 71(1a) of the Privacy Act – that it performed every necessary review concerning their petitions.

The documents generated in the course of the Authority's procedures also contained classified data, which can only be disclosed if the conditions laid down by specific law are met. Pursuant to Section 11(1) of Act CLV of 2009 on the Protection of Classified Data (Protection of Classified Data Act), the data subject is entitled to access his/her nationally classified personal data subject to a letter of access issued by the classifier.

Pursuant to Section 27(2) of Act CL of 2016 on the Code of General Administrative Procedure (hereinafter: the Code of General Administrative Procedure), the authority shall ensure that secrets protected by law and other data protected by law (hereinafter together: protected data) are not disclosed to the public, that no unauthorised person becomes aware of them, and that the protection of such protected data as defined by law is ensured in the procedures of the Authority. It may be inferred from the data protection obligation provided for in Section 27(2) of the Code of General Administrative Procedure that decisions – when they are drafted – shall not contain any data or any data allowing for the inference thereof which cannot be known to the person to whom the decision is communicated.

In view of the above, the Authority communicated its decisions to the petitioners and their legal representatives by means of an extract from the decision (hereinafter: decision), which does not contain classified data. The petitioners have brought an action against the Authority's decisions.

Overall, the Municipal Court of Budapest found that the Authority's decisions were unlawful on the merits of the cases, as the Authority, in breach of its duty to protect fundamental rights, did not include any descriptive information in the decisions, which could not provide the petitioners with legal protection arising from the Protection of Classified Data Act. The Municipal Court of Budapest annulled the Authority's decisions and ordered the Authority to conduct new procedures.

The Authority submitted a petition for review to the Curia against the judgments of the Municipal Court of Budapest. The Curia found in its review proceedings that the Authority is not charged with providing data in its procedures required for the initiation of procedures according to Section 11 of the Protection of Classified Data Act to ensure the exercise of rights in this form. The law does not stipulate

such an obligation; this was deducted by the court that handled the case solely from the Authority's function of protecting fundamental rights. The lawfulness of classification may be examined in a procedure for the supervision of secrets, classified data may be learnt in a procedure to learn them or in possession of a permit to learn the classified data in a procedure designed to issue a use permit. The Curia stressed that neither classified data, nor document, item of the facts of the case or legislation may constitute part of the public decision of the Authority from which classified data may be inferred because the national security interest that serves as a basis for the restriction affected by the classification procedure would clearly be infringed by that. This also includes whether or not data was processed with respect to the petitioner, and if yes, who the controller was. The Authority has no discretion whether to disclose the restricted data or not, it is authorised to decide how and in what way it will grant the rights of the data subject, in what way and when it meets the notification obligations; however, granting the rights of the data subject must not mean a breach of the restriction. The Curia – as the court of review – set aside the judgments of the Municipal Court of Budapest and ordered the court of first instance to conduct new proceedings and adopt new decisions.

The content in principle of the Curia's decision is the following:

"The obligation of the data protection authority stemming from legislation is not merely to withhold classified data but to ensure under Section 71(1a) of the Privacy Act that the interests that serve as a basis for the legitimate restriction of the rights due to the data subject should not be infringed. This, however, is a much broader definition than the restriction on the disclosure of classified data. Consequently, neither classified data, nor document, item of the facts of the case or legislation may constitute part of the public decision of the respondent from which classified data may be inferred, because the national security interest that serves as a basis for the restriction affected by the classification procedure would clearly be infringed by that. [Kúria Kfv.III.37.188/2024/13.]."

# VI. The Authority's legislation-related activities

The Authority's role to be played in the preparation of legislation and its right to express its position on data protection issues affected by draft legislation under preparation is ensured by Section 38(4)a) of the Privacy Act. The Authority shall also have the right under this Act to propose the drafting of an amendment to legislation concerning the processing of personal data and the disclosure of data of public interest and data accessible on public interest grounds.

Unfortunately, there were cases in 2024, as in previous years, where a ministry preparing a draft law sent a proposal for an opinion only after it had been submitted to Parliament for discussion, or did not at all submit it to the Authority, despite its data protection content. Although this is not usually the case for the drafters of legislation and the drafting process, it would be desirable in the future to avoid a practice which limits the rights granted to the Authority by the Privacy Act.

## *VI.1. The statistical data of cases related to legislation*

**The number of opinions communicated by the Authority by level of legislation**

| Level of legislation/year | 2021 | 2022 | 2023 | 2024 |
|---|---|---|---|---|
| Act | 77 | 68 | 89 | 70 |
| Government decree | 74 | 56 | 56 | 55 |
| Ministerial decree | 15 | 16 | 53 | 36 |
| Government decision | 14 | 4 | 18 | 4 |
| Other (Parliament decision, instruction, etc.) | 16 | 19 | 17 | 11 |
| Total | 196 | 163 | 233 | 176 |

**Statistics of substantial observations made in the opinions on legal regulations**

| Nature of observations | Number of observations | | | |
|---|---|---|---|---|
| | 2021 | 2022 | 2023 | 2024 |
| Related to data protection | 488 | 311 | 341 | 406 |
| Related to freedom of information | 89 | 40 | 97 | 109 |
| Other | 9 | 26 | 36 | 21 |
| Total | 586 | 377 | 474 | 536 |

## *VI.2. Priority cases*

### *VI.2.1. Act on the digital state and certain rules for the provision of digital services*

Act CIII of 2023 on the Digital State and Certain Rules for the Provision of Digital Services (Digital Citizenship Act), adopted by Parliament in December 2023, entered into force in 2024, and the Twelfth Amendment to the Fundamental Law of Hungary, which amends Article XXVI in relation to the Digital Citizenship, entered into force on 1 July 2024. Pursuant to the amendment, the state will provide everyone with a digital identifier for the digital management of affairs, and the Government may decide by decree on the manner in which the data required for this purpose are to be handled and the scope of the data to be handled.

The Government's objective is still that by 2026 citizens will be able to conduct almost all matters of public administration online, primarily through portable ICT devices. Accordingly, preparations are ongoing in the legislative field, both at the level of laws and decrees. In the course of 2024, the Authority had the opportunity to give its opinion on several drafts related to the subject. In general, these concern, on the one hand, the extension of the possibilities for digital administration (e.g. access to eKréta with a digital ID) and, on the other hand, the review of existing digital services to ensure that they can also be operated within the framework of Digital Citizenship (instead of the E-Administration Act). Due to its special data protection aspect, it is worth mentioning here that the legal provisions on the "Szitakötő Program" (Dragonfly programme), for example, have been incorporated into the Digital Citizenship Act without any changes, probably as a result of which neither a review of this programme, nor an evaluation of its results have been carried out so far.

In addition, the Government designated IdomSoft Informatikai Zrt. as the digital citizenship service provider in Government Decree 320/2024 (XI. 6.) on the designation of certain organisations related to the implementation of the digital state, which is also the provider of framework services and also performs application operation and development tasks. The Government Decree also designated the providers of the administrative services, the registration bodies of the Client Settings Register and NISZ Zrt. as the body responsible for the custody of the data repository. Also related are Government Decree 321/2024 (XI. 6.) on certain rules for digital citizenship, which consolidates the rules on digital services and electronic administration, and Government Decree 322/2024 (XI. 6.)

on detailed technical requirements for digital services, digital citizenship services and support services, which lays down provisions, inter alia, for the electronic payment system and the central address register, and sets out requirements for electronic signatures.

*VI.2.2. Implementation of the Artificial Intelligence Regulation*

The regulation of artificial intelligence at the level of the European Union, the adoption and entry into force of the Artificial Intelligence Regulation (Regulation (EU) 2024/1689 of the European Parliament and of the Council) required the Hungarian legislator to carry out additional tasks. The Artificial Intelligence Regulation provides for the designation of national authorities by the Member States at several points. Article 70 provides for the designation of a notifying authority and a market surveillance authority, which are competent national authorities that must exercise their powers independently, impartially and without bias. Article 77 provides for the designation of an authority (authorities) protecting fundamental rights to supervise or enforce the respect of obligations under Union law relating to the use of high-risk AI systems, aimed at protecting fundamental rights and therefore should have the appropriate powers to do so.

The designation has not yet been implemented at the legislative level, but a government decision was adopted in September setting out the Government's expectations on the issue. Pursuant to Government Decision 1301/2024 (IX. 30.), the notifying and market surveillance authority will be an entity under the supervision of the NGM (Ministry for National Economy). The government decision sets out the relevant codification tasks, which have not yet been carried out. A draft law on the designation of authorities for the protection of fundamental rights has been submitted to the Authority for its opinion, designating the Ministry of Justice as the authority under Article 77 and as the competent authority for market surveillance. [NAIH-13860/2024.] However, this draft did not become law and the relevant text was removed from the draft during the discussions before Parliament.

The government decision also provided for the drafting of legislation establishing the Hungarian Artificial Intelligence Board to which the Authority would also delegate a member. Pursuant to Article 74(8) of the AI Regulation, in the case of high-risk AI systems used for used for law enforcement purposes and border management, the data protection supervisory authority under the Law Enforcement Directive (in this case the Authority) shall be designated as the market surveillance authority, or such other authority as may be designated un-

der the conditions set out in the Law Enforcement Directive. This was also mentioned by the European Data Protection Board in its Statement 3/2024.

# VII. Annexes

## *VII.1. The financial management of the Authority in 2024*

We have passed the 13th year of the operation and financial management of the Hungarian National Authority for Data Protection and Freedom of Information as of 31 December 2024. Below, we provide a brief presentation of the data related to its financial management.

### *VII.1.1. Revenue and expenditure estimates and the data of its performance in 2024*

The following table presents the figures for NAIH's 2024 budget (in HUF '000):

| Description | Original estimate | Amended estimate | Performance | 2024 remainder from basic activity |
|---|---|---|---|---|
| Operational other support from chapter | | 6 387 | 6 387 | |
| Revenue from the sale of goods and supplies | | 16 | 16 | |
| Invoiced VAT | | 74 | 74 | |
| Exchange rate gain | | 73 | 73 | |
| Other operational revenues | | 2 896 | 2 896 | |
| Cost recovery | | 28 283 | 28 283 | |
| Sale of tangible assets | | 8 400 | 8 400 | |
| Recovery of loan for non-operational purposes | | 4 181 | 4 181 | |
| Use of funds remaining from the 2023 budget | | 98 823 | 98 823 | |
| Grant from central budget from Managing Authority | 1 626 300 | 2 201 984 | 2 201 984 | |
| ***Revenue estimates total:*** | ***1 626 300*** | ***2 351 117*** | ***2 351 117*** | **-** |
| Estimates for payments to personnel | 1 165 400 | 1 441 128 | 1 441 128 | - |
| Employers' contribution and welfare contribution tax | 156 500 | 200 062 | 200 062 | - |
| Estimate for material expenses | 304 400 | 488 458 | 354 618 | 133 840 |
| Other operational expenses | | 134 | 134 | - |
| Investment | | 220 498 | 218 016 | 2 482 |
| Renovations | | 837 | 837 | - |
| ***Expenditure estimate total:*** | ***1 626 300*** | ***2 351 117*** | ***2 214 795*** | ***136 322*** |

*VII.1.2. Changes in the headcount of the Authority*

As of 31 December 2024, the Authority's headcount according to labour law was 135.

Human resource management is based on positions according to the Act on Organs of Special Legal Standing (AOLS), namely the Authority has four administrative job categories (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. Although the Authority has endeavoured to provide competitive salaries for its staff since the introduction of the AOLS, high inflation and a difficult economic environment have led to high labour fluctuation in our organisation. In the course of the year, 19 people left the Authority and 33 new colleagues entered. In 2024, 12 people were on long-term leave, and 4 returned from long-term leave.

*VII.1.3. Changes in fine revenues*

In 2024, a near-record amount of HUF 335 383 000 was again received in the Authority's fines account. It should, however, be noted that receipts from fines constitute the revenues of the central budget, not that of the Authority.

## *VII.2. List of legal regulations and abbreviations mentioned in the report*

- Aarhus Convention: Act LXXXI of 2001 on the proclamation of the Aarhus Convention of 25 June 1998
- Act C of 2003 on electronic communications
- Act CCXL of 2013 on the Execution of Sentences, Measures, Certain Coercive Measures and Detention for Misdemeanours
- Act CLIV of 1997 on Healthcare
- Act CLXI of 2011 on the Organisation and Administration of the Courts
- Act CVIII of 2001 on certain aspects of Electronic Commercial Services and Information Society Services
- Act CXCIX of 2011 on Civil Servants
- Act CXCV of 2011 on Public Finances
- Act CXL of 1997 on museum institutions, public library services and public culture
- Act CXXX of 2016 on the Code of Civil Procedure

- Act I of 2017 on the Code of Administrative Court Procedures
- Act LIII of 1994 on Court Distraint
- Act LIII of 1995 on the General Rules of the Protection of the Environment
- Act LXVI of 1995 on Public Documents, Public Archives and the Protection of the Materials of Private Archives
- Act LXXVIII of 2017 on the Activities of Lawyers
- Act LXXXVIII of 2013 on the Wanted Persons Registration System and on the Search and Identification of Persons and Things
- Act XLVII of 1997 on the Processing and Protection of Health and Related Personal Data
- Act XXXI of 1997 on the Protection of Children and the Administration of Guardianship
- Agri Aid Act, Act XVII of 2007 on Certain Issues of the Procedure related to Agri and Rural Development and Fishing Grants and other Measures
- AI Act, Artificial Intelligence regulation: Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828
- Állami Számvevőszék (ÁSZ) – State Audit Office of Hungary
- BATÉK: Government Decree on the land use requirements for the water-front areas of Lake Balaton
- BTLE: Borders, Travel and Law Enforcement Expert Group: The Borders, Travel and Law Enforcement expert subgroup
- CEF: Coordinated Enforcement Framework
- CIS: Customs Information System
- Civil Code, Act V of 2013 on the Civil Code
- CJEU: Court of Justice of the European Union
- Classified Data Act, Act CLV of 2009 on the Protection of Classified Data
- Code of Criminal Procedure, Act XC of 2017 on the Code of Criminal Procedure
- Code of General Administrative Procedure, Act CL of 2016 on the Code of General Administrative Procedure
- CSC: Coordinated Supervision Committee (carrying out the joint supervision of the large information systems of the European Union)
- Data Act, translated in a former draft as data-sharing legislation: Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828

- 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
- Decree 14/2002 (VIII.1.) IM on the Rules of Court Administration
- DGA: 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
- Digital Citizenship Act: Act CIII of 2023 on the Digital State and Certain Rules for the Provision of Digital Services
- EAFRD: European Agricultural Fund for Rural Development
- EAGF: European Agricultural Guarantee Fund
- ECRIS: European Criminal Records Information System
- ECRIS-TCN: centralised system for the identification of Member States having information concerning judgments against third country nationals and stateless persons
- EDIB: European Data Innovation Board
- EDPB: European Data Protection Board
- EDPS: European Data Protection Supervisor
- EES: European Entry/Exit System
- EESZT: Healthcare Service Space
- EKR: Electronic Public Procurement System
- EMFAF: European Maritime, Fisheries and Aquaculture Fund
- EPPO: European Public Prosecutor's Office
- ÉTDR: the Electronic Documentation System supporting the building permit procedure of the Construction Authority
- ETIAS: European Travel Information and Authorization System
- Eurodac system: European Dactylographic Comparison system
- Fundamental Law, Hungary's Fundamental Law (25 April 2011)
- 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
- General Data Protection Regulation: see GDPR
- Government Decree 2/2005 (I. 11.) on the environmental assessment of certain plans and programmes
- Government Decree 335/2012 (XII.4.) on the detailed rules for the provision of postal services and the postal service for official documents, as well as on the general terms and conditions of postal service providers and on items excluded from or conditionally delivered by postal services
- GRECO: Group of States against Corruption

- HNBTS: Hungarian National Blood Transfusion Service (OVSZ)
- IHM decree: Decree 18/2005 (XII.27.) IHM on the publication models for the publication of data in publication schemes
- IMI system: Internal Market Information System
- KEF: Directorate-General for Public Procurement and Provisions
- KIKAP: Integrated Portal for the Disclosure of Data of Public Interest of the Government
- LLM: Large language models
- LÜ instruction: Instruction 26/2018 (XII. 28.) LÜ on the Rules of the Prosecutor's Office on File Management
- MBVK: Hungarian Association of Judicial Officers
- Municipalities Act, Act CLXXXIX of 2011 on Hungary's Municipalities
- National Security Services Act, Act CXXV of 1995 on National Security Services
- NBF: Special Service for National Security National Security Authority (NSA HUN)
- NBSZ: SSNS: Special Service for National Security
- NOJ: National Office for the Judiciary
- Nuclear Energy Act: Act CXVI of 1996 on nuclear energy
- Police Act, Act XXXIV of 1994 on the Police
- Postal Services Act, Act CLIX of 2012 on Postal Services
- Privacy Act, Act CXII of 2011 on the Right of Informational Self-Determination and the Freedom of Information
- Prize Act: Act XII of 1990 on the Kossuth Prize and the Széchenyi Prize
- Public Procurement Act, Act CXLIII of 2015 on Public Procurement
- SIS: Schengen Information System
- Sports Act, Act I of 2004 on Sports
- Tromsø Convention, Council of Europe Convention on access to official documents (CETS No.205., promulgated in Hungary by Act CXXXI of 2009)
- 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
- VIS: Visa Information System

Other legal regulations:

- Act C of 2023 on Hungarian Architecture
- Act CCIV of 2011 on National Higher Education

- Act CI of 2023 on the System for the Exploitation of National Data Assets and on Certain Services
- Act CLI of 2011 on the Constitutional Court
- Act CLXVI of 2012 on the identification, designation and protection of vital systems and facilities and Government decree 65/2013. (III. 8.) on its implementation
- Act CLXXXI of 2007 on the Transparency on public grants from public funds
- Act CLXXXVIII of 2015 on the Facial Analysis Register and the Facial Analysis System
- Act CXXII of 2009 on the More Economical Operation of Business Organisations in Public Ownership
- Act CXXIII of 2015 on Primary Health Care
- Act CXXXI of 2009 on the promulgation of the Council of Europe Convention on Access to Documents containing Data of Public Interest
- Act CXXXIII of 2005 on the rules of activities involving personal and property protection and private investigation
- Act LII of 2023 on the New Careers of Teachers
- Act LIV of 2018 on the Protection of Trade Secrets
- Act LVI of 2024 amending certain acts on financial and property management
- Act LXXVII of 2024 amending the Acts concerning the internal affairs sectors
- Act LXXXI of 2001 on the promulgation of the Council of Europe Convention on Access to Documents containing Data of Public Interest
- Act LXXXV of 2024 amending certain laws for deregulation purposes in the interests of legal competitiveness
- Act XXXIII of 1992 on the Legal Status of Public Servants
- Commission Implementing Decision EU 2023/1795 of 10 July 2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework
- Government decision 1036/2024. (II. 22.) on the transfer of appropriations from and between chapters of the Central Residual Fund and on the revocation of a government decision
- Government Decision 1301/2024 (IX. 30.) on the measures necessary for the implementation of the Regulation of the European Parliament and of the Council on artificial intelligence

- Government Decree 168/2004. (V. 25.) on the centralised public procurement system and the responsibilities and powers of the central procurement organisation
- Government Decree 287/2006 (XII.23.) on the detailed rules of healthcare services that may be provided on the basis of waiting lists
- Government Decree 311/2005 (XII. 25.) on the order of public access to environmental information
- Government Decree 320/2024 (XI. 6.) on the designation of certain organisations related to the implementation of the digital state
- Government Decree 321/2024 (XI.6.) on certain rules of digital citizenship
- Government Decree 322/2024 (XI.6.) on the detailed technical requirements for digital services, digital citizenship services and supporting services
- Government Decree 335/2005 (XII. 29.) on the general requirements for document management by public bodies
- Government Decree 356/2022. (IX.19.) on exercising rights in relation to the disclosure of certain data of public interest in times of emergency
- Government Decree 499/2022. (XII. 8.) on the detailed rules of the Central Information Public Data Register
- Government Decree 499/2022. (XII. 8.) on the detailed rules of the Central Information Public Data Register
- Government decree 65/2013. (III. 8.) on the implementation of Act CLXVI of 2012 on the identification, designation and protection of vital systems and facilities
- Government Decree 90/2010. (III.26.) on the operation of the Hungarian National Security Authority and the handling of classified data
- Government Decree No 149/1997 (IX. 10.) on guardianship authorities and child protection and guardianship proceedings
- Penal Code, Act C of 2012 on the Penal Code
- Regulation (EU) 2021/1134 of the European Parliament and of the Council of 7 July 2021 amending Regulations (EC) 767/2008, (EC) 810/2009, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1860, (EU) 2018/1861, (EU) 2019/817 and (EU) 2019/1896 of the European Parliament and of the Council and repealing Council Decisions 2004/512/EC and 2008/633/JHA with a view to reforming the Visa Information System

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
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)