National Authority
for Data Protection
and Freedom of Information

ANNUAL REPORT OF THE HUNGARIAN NATIONAL AUTHORITY FOR DATA PROTECTION AND FREEDOM OF INFORMATION (NAIH) 2025

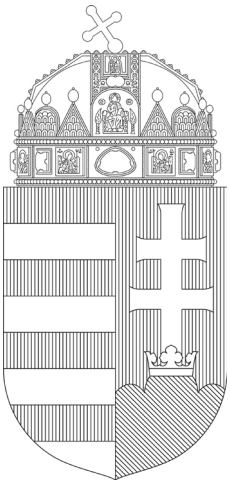
Report

(Excerpts)

– the Hungarian National Authority for Data Protection and Freedom of Information –

on its activities in 2025

Nemzeti Adatvédelmi és Információszabadság Hatóság
Budapest, 2026.



Introduction

Greetings Dear Reader

We have reached an important milestone this year in the field of data protection and freedom of information, as the National Assembly elected the first Data Protection Commissioner in 1995, meaning that in 2025 we celebrated the 30th anniversary of the institutional system protecting information rights in Hungary. To mark this anniversary in a fitting manner, the NAIH organised an international conference in Budapest on 17–18 September[1], at which the past, present and future of information rights were presented and discussed. It was a great honour for us that the conference was opened by Dr Tamás Sulyok, President of the Republic, and that the speakers included Dr Péter Polt, President of the Constitutional Court, Dr István Stumpf, former Constitutional Court judge, as well as several judges and renowned Hungarian and international data protection experts.

During the conference, a posthumous silver commemorative medal was awarded to Pál Könyves-Tóth for his work in preparing the first draft of the Hungarian Information Law, as well as for his active participation in shaping the rules governing data protection and freedom of information in Hungary. In his memory, we named the NAIH's IT training room after him; Pál Könyves-Tóth's family honoured us with their presence at the inauguration ceremony in December.

In NAIH's 2025 activities, particular attention was paid to the data protection challenges posed by the use of artificial intelligence. The application of artificial intelligence, its rapid spread, and the volume and sensitivity of the personal data processed necessitate exceptional caution from both a societal and a data protection perspective. The development of this technology is undoubtedly beneficial to society, but the risks involved are also significant.

As part of its supervisory activities in 2025, the data protection authority sought to obtain an overview of the purposes for which IT systems using artificial intelligence in the Hungarian banking sector process personal data, the types of personal data processed, and how legal compliance is ensured. The Authority published the results of this investigation and the best practices identified in this

1 The second meeting of the cooperation group of data protection authorities from the Central and Eastern European region – established at the initiative of the Austrian Data Protection Authority – took place this year in Budapest as part of the international conference.

regard in a report available in both Hungarian and English on its website[2] at the end of 2025. A further comprehensive investigation into sectoral data processing activities affecting many millions of people is expected in 2026.

In response to all these new challenges, the Authority has established the Digital Data Strategy Department, which will contribute to the work of the European Data Innovation Board and focus its activities on data processing involving artificial intelligence. The AI Lab, which was also established recently, has come under the management of the new department; as its first project, it plans to implement the anonymisation of the Authority's decisions with the involvement of experts from the European Data Protection Board. This project will not only make the Authority's current practices more transparent, but the planned report on this will, instead of merely outlining abstract theoretical rules, present tried-and-tested best practices regarding the responsible use of artificial intelligence, which may be useful in a wide range of other activities.

The NAIH will therefore continue to pay close attention to the use of artificial intelligence in Hungary. Its participation in the Artificial Intelligence Council also greatly assists this work.

The European Union's institutions have also embarked on a comprehensive legislative reform aimed at simplifying and clarifying digital regulation. In the Digital Omnibus Package, EU legislators are seeking to harmonise the provisions of the GDPR, the ePrivacy Directive and the EUDPR, and to incorporate existing case law into them. The proposed provisions would consolidate various other rules on access to data (Data Governance Regulation, Data Regulation, open data, etc.) and aim to introduce a uniform data breach reporting system. Another omnibus package relating to AI would, in addition, extend the deadline for compliance with the implementing provisions linked to the AI Regulation, which are yet to be adopted by the Commission, and would relax the strictness of certain requirements. Consultations on these legislative proposals with Member States have recently begun and will require a great deal of work from both the authorities and Member State legislators. The EDPB and the EDPS issued a joint opinion in early 2026 on the AI omnibus and the digital omnibus.

Issues relating to children's rights have also played a prominent role in the NAIH's activities from the outset: in 2025, the updated version of the study entitled 'Kulcs a net világához!' [3] [Key to the Online World!] , a study on the safe and rights-con-

2 https://www.naih.hu/hirek/802-jelentes-magyarorszagi-bankok-mi-hasznalatarol.
3 https://naih.hu/files/kulcs_a_net_vilagahoz_2025.pdf

scious use of the internet by children, was published, and Dr Júlia Sziklay, the Authority's Vice-President for International Affairs, released her book 'Children's (Online) Data Protection – A Guide for Adults' in e-book format.

Budapest, 20 February 2026.

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

I. Statistical data on the Authority's operations, the Authority's public relations

I.1. Statistical characteristics of our cases

In 2025, 16,162 new cases were registered in the Authority's internal case management system. Together with cases carried over from previous years (2,261), there were 18,423 cases pending before the Authority this year; we registered 725 new cases solely in connection with the Tisza Party data breach incident.
A comparison of the data sets shows that the number of investigation cases rose by nearly 37 per cent (from 3,561 to 4,855) compared to the previous year, whilst the number of official inspections increased by 52 per cent (from 587 to 893). Furthermore, the number of cases relating to consultations and GDPR cooperation (IMI) also showed a marked increase.

The Authority's document management and administrative procedures in 2025 were again governed by internal regulations established in previous years and continuously refined. These set out the detailed rules for the receipt, registration, signing, filing, forwarding, deadline tracking, archiving and disposal of documents, and therefore fulfil not only an administrative but also a safeguarding function.

When designing the processes in 2025, a consistent objective was to identify and eliminate steps that constituted an unnecessary, repetitive or disproportionate administrative burden. The Authority continued to strive for the application of well-documented, simplified and verifiable workflows, in which tasks with the same purpose or subject matter are handled according to uniform principles.

Building on the digitalisation measures implemented between 2021 and 2024, the further strengthening of electronic administration and paperless document management came to the fore in 2025. The Authority's operations have increasingly relied on the electronic channels provided by legislation for administrative procedures, in particular regulated electronic administration services.

It cannot be overlooked that interoperability remained a key focus in the development of internal specialist systems in 2025. The aim is to ensure that information can be transferred between individual systems quickly, securely and in a traceable manner, without the need for manual intervention. Through integrated op-

eration, the lifecycle of cases can be tracked on a single interface from receipt to closure, which substantially supports management decision-making, the preparation of reports for statistical and monitoring purposes, and facilitates the implementation of quality assurance measures.

The infrastructure put in place is capable of supporting changes to the Authority's remit in a flexible and scalable manner, and contributes to making the organisation's operations even more cost-effective, whilst ensuring that human resources management remains predictable in the longer term.

It is important to emphasise that whilst the Authority consistently encourages the use of digital channels, it does not neglect those clients who are unable to use electronic devices, or can do so only to a limited extent. We continued to accept paper-based submissions in 2025, although in practice we also recorded these electronically where possible.

The Authority's customer relations practice in 2025 continued to be based primarily on written communication – both electronic and postal – supplemented where necessary by face-to-face hearings and consultations. When designing the electronic interfaces, forms and information leaflets available to clients, the Authority continued to strive to ensure that the information provided was presented in a clear and easily understandable form, with particular regard to the course of proceedings, procedural deadlines and avenues of appeal.

Information security and data protection continued to play a key role in the operation of administrative systems.

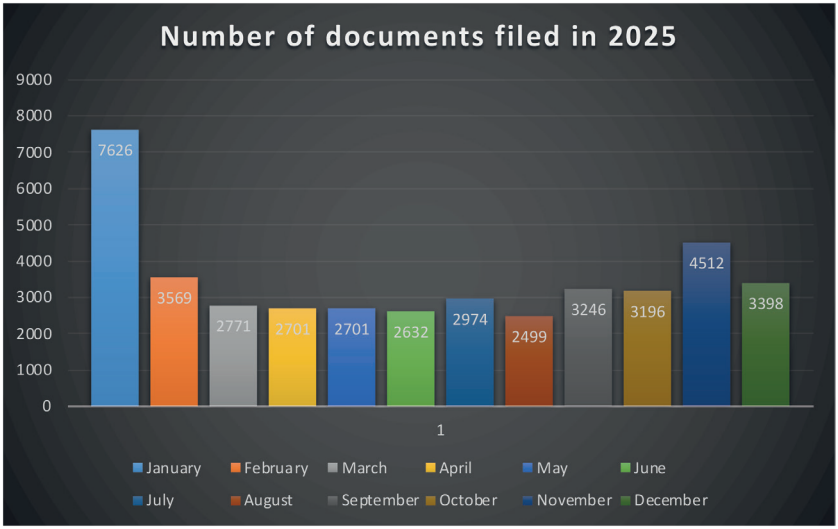
In line with its regulatory role, the Authority paid particular attention to ensuring that data processed in specialist systems are protected by appropriate safeguards, and that day-to-day administrative practices comply with internal standards and the required level of security.

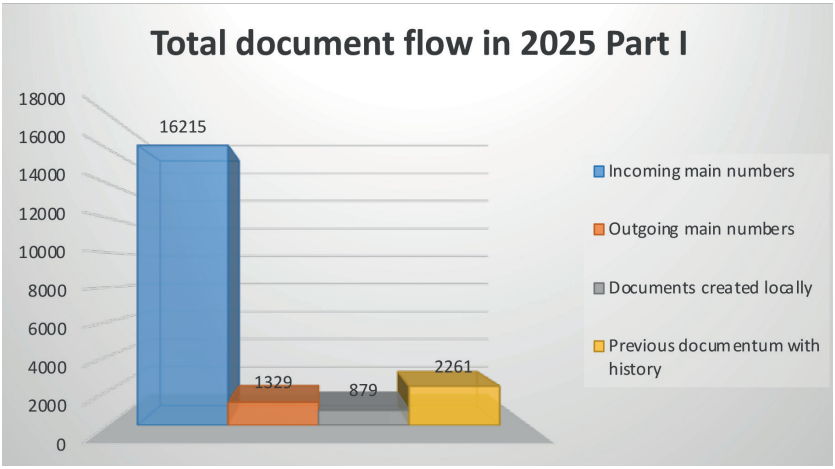
The administrative improvements implemented in 2025 built directly on the digitalisation and organisational development steps taken in the previous period. The Authority's aim was for the administrative structure to adapt flexibly to new types of procedures, the growing caseload and changing client needs, even as its tasks and remit expanded.

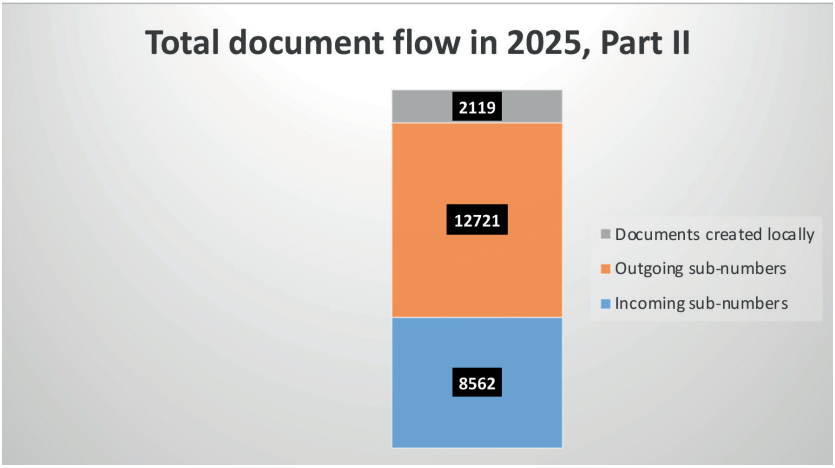
Overall, the experiences of 2025 showed that the strengthening of electronic administration, the simplification of processes and the integrated operation of

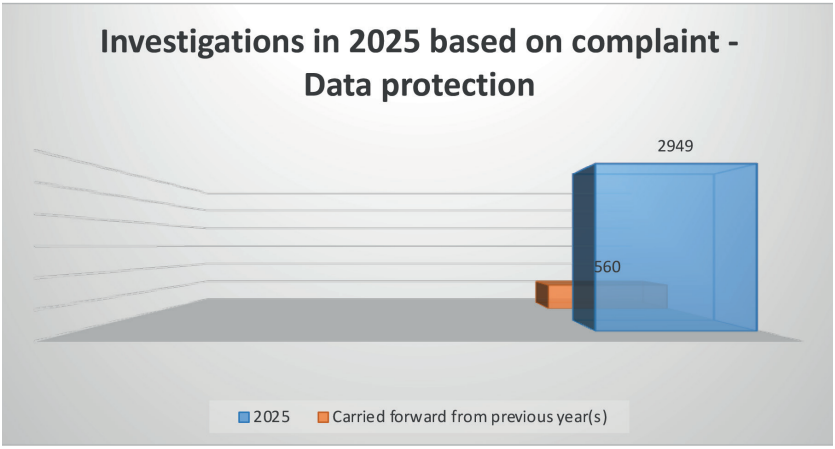
specialist systems collectively contributed to an increase in the efficiency of administrative activities. A positive trend was observed in the development of processing times in those areas where the traceability of cases and the clarity of the chain of responsibility were strengthened.

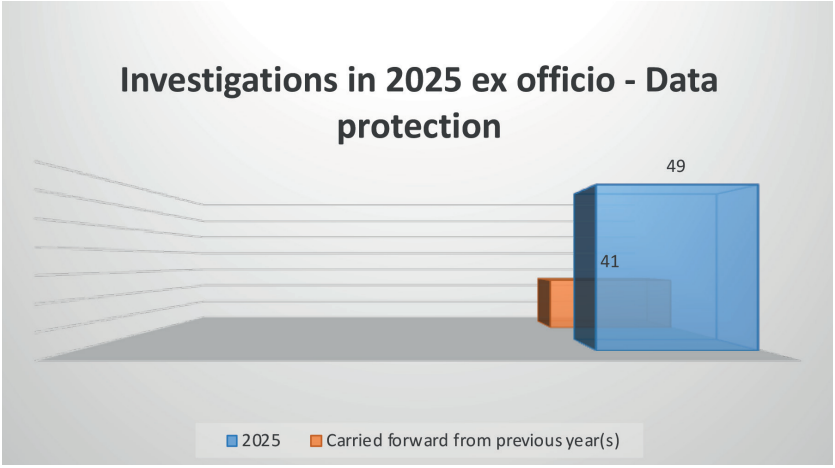
Based on the experience of 2025, the Authority has identified development priorities for the coming period aimed at further simplifying administrative processes, expanding tools supporting electronic administration, and deepening cooperation between specialist systems.

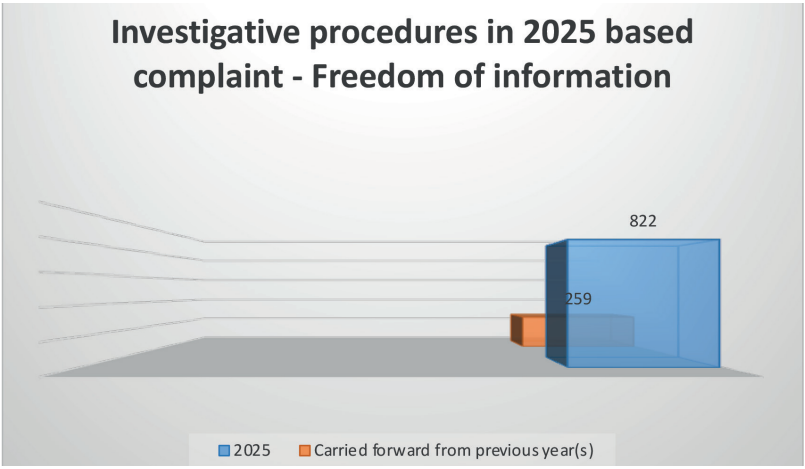


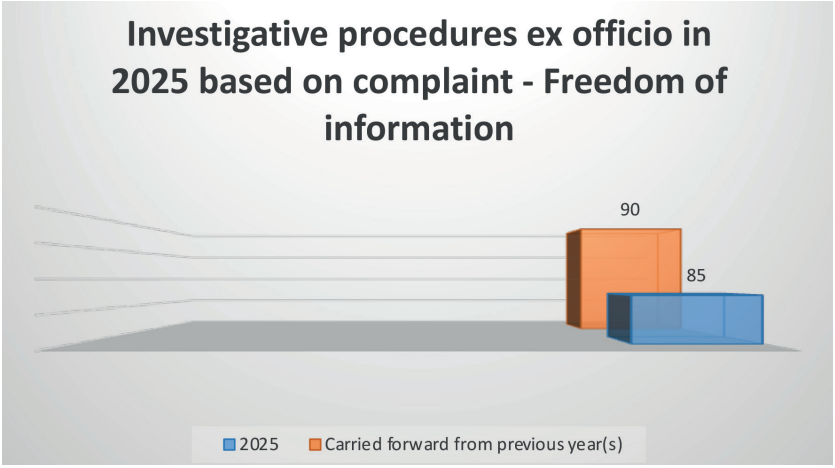


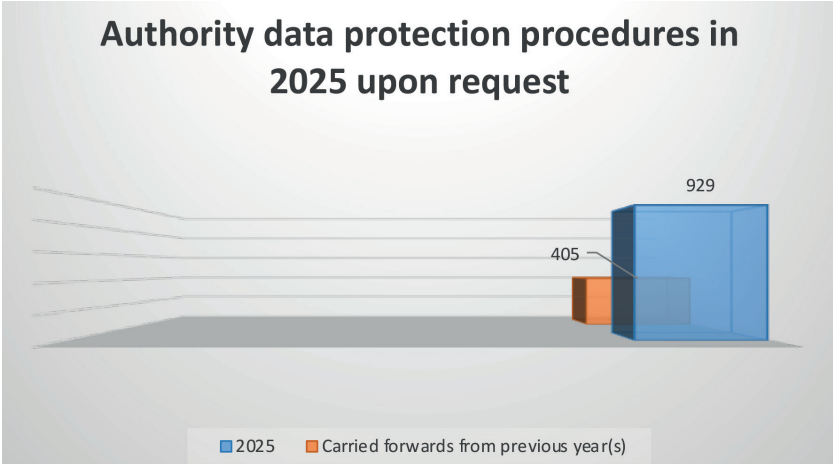

Total document flow in 2025, Part II
2119
12721
8562
Documents created locally
Outgoing sub-numbers
Incoming sub-numbers

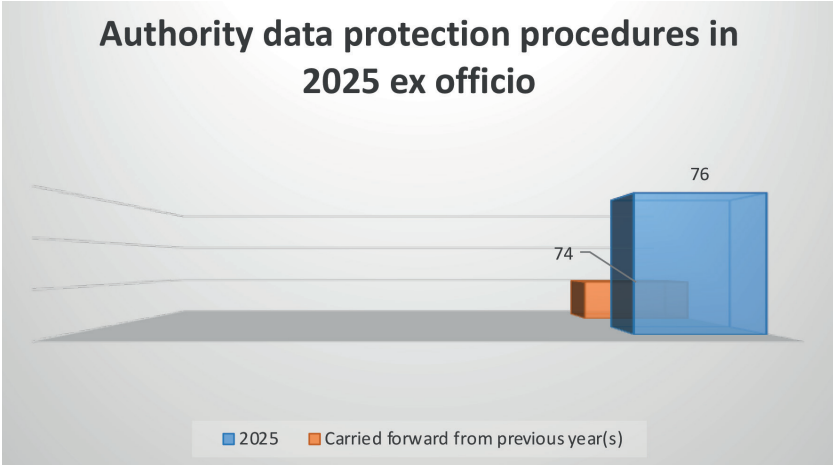

Investigations in 2025 based on complaint - Data protection
2949
560
2025
Carried forward from previous year(s)

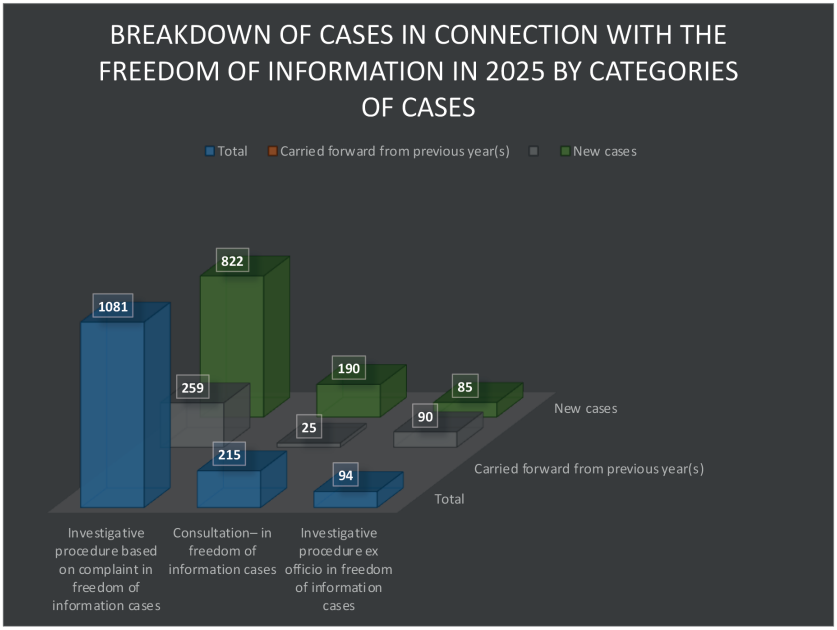

Investigations in 2025 ex officio - Data protection
49
41
2025
Carried forward from previous year(s)

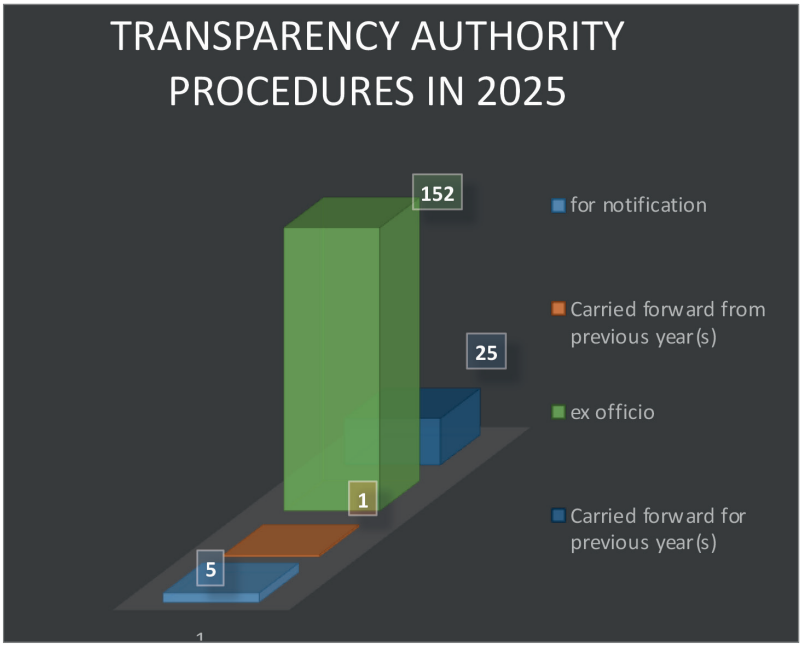

Investigative procedures in 2025 based complaint - Freedom of information
822
259
2025
Carried forward from previous year(s)

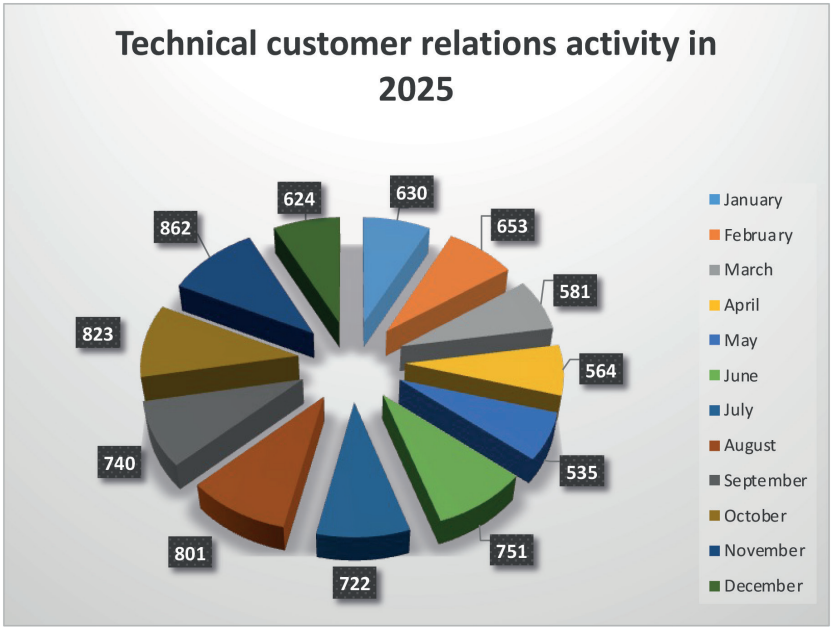

Investigative procedures ex officio in 2025 based on complaint - Freedom of information
90
85
2025
Carried forward from previous year(s)


Authority data protection procedures in 2025 upon request
929
405
2025
Carried forwards from previous year(s)


Authority data protection procedures in 2025 ex officio
76
74
2025
Carried forward from previous year(s)


BREAKDOWN OF CASES IN CONNECTION WITH THE FREEDOM OF INFORMATION IN 2025 BY CATEGORIES OF CASES
Total
Carried forward from previous year(s)
New cases
1081
822
259
190
85
25
90
215
94
New cases
Carried forward from previous year(s)
Total
Investigative procedure based on complaint in freedom of information cases
Consultation– in freedom of information cases
Investigative procedure ex officio in freedom of information cases


TRANSPARENCY AUTHORITY PROCEDURES IN 2025
152
25
1
5
for notification
Carried forward from previous year(s)
ex officio
Carried forward for previous year(s)


Technical customer relations activity in 2025
630
653
581
564
535
751
722
801
740
823
862
624
January
February
March
April
May
June
July
August
September
October
November
December

I.2. Annual Conference of Data Protection Officers

The Authority held the Annual Conference of Data Protection Officers on 25 November 2025. The event was not only attended by the nearly 80 data protection officers present at the Authority's premises; thanks to the cooperation of MTVA, it could also be followed live online via the Authority's website, without the need for registration. The Authority has also published on its website approximately four hours' worth of recordings of the conference presentations.

At the start of the conference, **President Dr. habil. Attila Péterfalvi** commemorated the 30th anniversary of the establishment of the institutional framework for information rights in Hungary, outlined its development from 1995 to the present day, and compared the key statistical figures relating to the institution of the Data Protection Commissioner and the Authority's activities. In his opening presentation, he outlined the recommendation published by the Authority in connection with the elections, emphasising the enforcement of data protection principles, highlighting the risks associated with campaign activities involving children's data, and then emphasising the data protection requirements relating to specific campaign tools. In his presentation, he emphasised that the Authority, as before, pays close attention to monitoring the lawfulness of data processing for political purposes.

In her address, **Dr Júlia Sziklay**, Vice-President for International Affairs, outlined the objectives and results to date of the Authority's AWARE project, launched in 2025, which aims to raise GDPR awareness among micro-enterprises.
The project focuses primarily on the transparency of data processing, explaining the rules of CCTV surveillance, handling requests relating to the exercise of data subjects' rights, the processing of personal data of minors and women, as well as the mapping and identification of data processing activities and data protection issues relating to employment. According to surveys to date, shortcomings on the part of controllers have arisen particularly in relation to the handling of requests concerning the exercise of data subjects' rights and the processing of employees' personal data.

Dr Dániel Eszteri, Head of the Data Breach Reporting and Forensic Analysis Department, gave a presentation on the results of the joint operation under Article 62 of the GDPR concerning data transmission by smart TVs; although the Authority ultimately closed its investigation due to a lack of evidence of a breach, the investigation report, containing numerous substantive findings, is available on the Authority's website in both Hungarian and English.

Dr András Bence Tóth, a data protection expert from the Data Protection Department, gave a presentation on the Authority's survey conducted under the 2025 Coordinated Enforcement Framework ('CEF'). The investigation began by contacting 13 domestic banks, which, whilst varying in size, were similar in terms of the services they provided and the data they processed.
He highlighted from the report that all controllers surveyed reported a significant workload in relation to the processing and storage of various types of customers' personal data, as well as the handling of requests from data subjects. When it comes to processing the same types of personal data, individual banks define the legal basis and purposes of data processing in a wide variety of ways. At the same time, the banks surveyed also follow a number of good practices in the processing of personal data, such as the erasure of personal data through anonymisation, and the so-called 'principle of least privilege' applied by one of the controllers can also be included here.

Dr Eszter Lajtos, a data protection expert at the Data Protection Strategy and Supervision Department, presented the Authority's report on the data processing practices of online media content providers and political parties regarding the right to erasure, which has also been published on the Authority's website.
The Authority surveyed 10 online media content providers and 14 political parties using a questionnaire comprising nearly 60 questions. The respondents typically rejected a low proportion of erasure requests; however, in some cases, the rejection rate reached as high as 50% of requests.
While half of the media content providers surveyed have internal regulations governing the handling of erasure requests, the majority of political parties do not have such procedures in place. Both the political parties and the media content providers responded to the requests sent to them within a short timeframe. In the case of erasure requests, media content providers mainly refused to delete the personal data of those concerned in relation to articles on public affairs and crime reports. However, the findings of the investigation indicate that a problem for providers is the lack of a consistent legal practice for resolving conflicts between the right to freedom of expression and the data subject's right to erasure.

Dr Andrea Jeney, a data protection expert in the Licensing and Data Breach Reporting Department, compared the points of overlap between the GDPR and the NIS2 Directive, as well as the data security requirements set out in each, in her presentation. The provisions of the GDPR and the NIS2 Directive do not override one another; the two sets of regulations are to be applied in parallel. A significant difference, however, is that whilst the GDPR is increasingly characterised by a clear and largely uniform interpretation of the law and judicial prac-

tice by authorities and courts, the NIS2 Directive has resulted in differing rules across Member States, varying judicial practice and, as yet, few authoritative interpretations of the law. The presentation outlined the competent authorities, emphasising that the Authority does not exercise regulatory powers under the NIS2 Directive, but is obliged to cooperate pursuant to Section 18(i) of Government Decree No. 418/2024. (23 December) in the field of electronic information security. It is important to note that if a cybersecurity incident occurs alongside a data breach incident, both reports must be submitted separately to the competent authorities. Based on the PreDeCo principle, the primary objective in the event of an incident is prevention; if this is not possible, appropriate detection and corrective measures are required. He recommended to the audience the recently published white paper, 'NIS2 in Hungary', which is available for free download at https://www.nis2whitepaper.eu/hu.

Dr Gergely Barabás, the Authority's registered in-house counsel and Head of the Legal Counsels' Department, first outlined the downward trend in the number of legal proceedings seeking to review the Authority's decisions, and then, in his presentation entitled 'The Scope and Limits of the Principle of Data Minimisation in Judicial Practice', he explored the practical aspects of the principle of data minimisation within the legal system governing disputes. The approach set out in the Court of Justice of the European Union's judgment in Case C-268/21 ("Collect less, but better!") has so far been applied only to a limited extent in Hungary, as in an administrative case pending before the Curia, the data protection implications of the norms applicable to the fundamental scope of judicial activities (Code of General Administrative Procedure and Act on Government Administration) were not considered; only the GDPR's principles of purpose limitation and data minimisation were addressed, whilst in a criminal case before the Budapest-Capital Regional Court, sector-specific legislation was also considered, yet it was not demonstrated that the data protection interests of the data subject (the defendant) had been infringed. Finally, French case law, recognised as representing best practice for data subjects, has established that the two processes (controller activities and judicial activities) must be integrated, and that the balancing criteria and the interests of the data subject must be given due consideration.

Dr Péter Horváth, Head of the Licensing Department, gave a presentation on the Authority's current cases relating to data breaches and data security, focusing on the relationship between controllers and processors, their organisational and technical measures to minimise risk, and their respective areas of responsibility. In the first case, the data breach occurred due to a faulty firewall protocol.

In the other case, there was also a failure on the part of the processor: when the system was brought into operation, the controller's database containing a large volume of personal data was made accessible for a few minutes on a previously public interface. In addition to the negligence, the controller was also found liable (although they were unaware of the programme code published on the website and the public nature of the uploaded personal data), as they failed to exercise due care in selecting a suitable processor and in developing protocols to deal with potential breaches at the time of contracting.

Dr Anita Román, Head of the Regulatory and Data Protection Department, gave a presentation on experiences regarding data transfers falling within the scope of the Privacy Act.
Several complaints have been received regarding situations where proceedings are underway to establish criminal liability against a person practising as a lawyer registered with a regionally competent bar association, but where proceedings are also initiated to establish other, non-criminal (e.g. disciplinary) liability. Even if this data transfer is initiated by a law enforcement agency, the information required to establish disciplinary liability will be treated in accordance with the GDPR and other sector-specific legislation. Consequently, the principle of data minimisation also applies, meaning that it is sufficient to disclose the fact of the criminal proceedings (or certain stages thereof) and to transfer the personal identification data to the competent chamber for the initiation of disciplinary proceedings. The other data processing practice complained about is when a request for data disclosure regarding criminal personal data is made to the authority conducting the criminal proceedings. If there is no appropriate legal basis for the transfer of data, a mere practice of mutual information exchange cannot justify (unrestricted) data transfer. The third scenario was where a case (or part of the case file) is transferred due to a lack of jurisdiction. Thus, during criminal proceedings, a circumstance is identified that necessitates proceedings by another authority; however, in such cases, it is not lawful to transfer the entire file (including criminal proceedings documents) to that other authority.

István Csajági, Head of the Freedom of Information Department, highlighted the findings of monitoring procedures, noting that it is often the case with public organs and local authorities that they fail to fulfil their disclosure obligations, schemes are not organised, there is no central link providing access, and the published data are invalid or incomplete.
In the case of requests for data of public interest, there have been several instances where organs have been unable to identify the original data requester

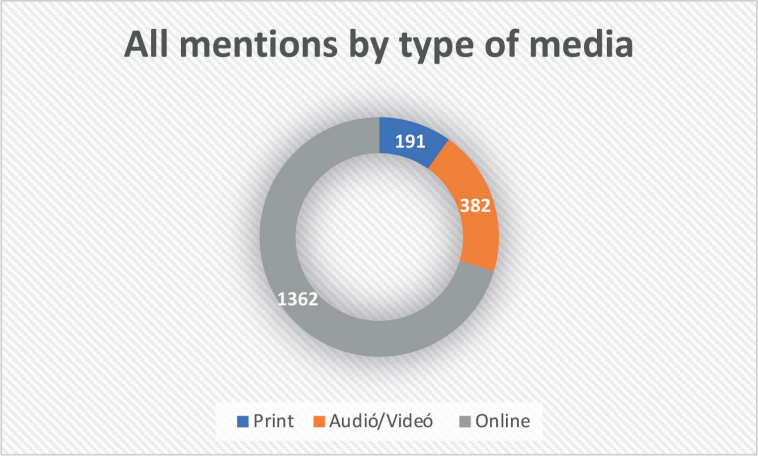
and their request, and in many cases there is confusion between the concepts and procedures of requests for data of public interest and data provision.
A change in transparency procedures is that local authorities are now also included among the organs subject to data disclosure requirements regarding their contracts.
In connection with so-called ‘borderline’ procedures, he highlighted the conflicts arising from the intersection of the right to the protection of personal data and journalistic activity. Journalists are subject to data processing obligations even if they are unaware of them; therefore, the right to freedom of the press and freedom of expression, which may restrict the right to the protection of personal data, can only be exercised following a proper balancing of interests. Journalistic activity is not a public authority activity; typically, the legal basis relating to the performance of a public task cannot be applied to this data processing.

Dr Attila Kiss, Head of the Data Protection Compliance and Public Relations Department, answered some of the questions received from data protection officers that concerned a wider range of controllers, and drew attention to the Authority’s position statements and recommendations published in 2025. A frequent question continues to be the legal basis that may be invoked by persons and organs performing public tasks, or by commercial companies supervised or controlled by them; on this occasion, the focus was specifically on the legal basis for data processing activities concerning staff. He emphasised that the legislator often fails to carry out a data protection impact assessment when prescribing mandatory data processing and public tasks; consequently, the controller cannot be exempted from the duty to conduct a substantive data protection impact assessment merely on the basis of the statutory requirement.

I.3. The National Authority for Data Protection and Freedom of Information in the media

Between 1 January and 31 December 2025, a total of 1,935 news items were published in the media about the National Authority for Data Protection and Freedom of Information. Among the different media types, online media continued to feature the most reports on the Authority's activities, with a total of 1,362 mentions. The NAIH appeared 191 times in the print media and 382 times in the electronic media.

The proportion of NAIH mentions across different media in 2025



Source: Observer Budapest Médiafigyelő Kft.

II. Data protection cases

II.1. Application of the General Data Protection Regulation

II.1.1. Camera-related cases

1. Camera surveillance by an employer

The Authority received a complaint challenging the data processing carried out by a company manufacturing electronic consumer goods using a CCTV system.

The controller carried out continuous camera surveillance in canteens and other areas used for breaks during working hours, based on images recorded by the cameras. It based its data processing via the camera surveillance system on the legal basis set out in Article 6(1)(f) of the GDPR, citing the protection of human life, physical integrity, property, as well as the protection of trade secrets and personal data as legitimate interests in the data processing.

The Authority did not consider the monitoring of the entire area of the canteens used by employees and the processing of data via CCTV cameras monitoring food and drink vending machines to be proportionate to the property protection objective indicated by the controller. The purpose of monitoring the canteens was to prevent theft from the fridges used by employees, whilst the purpose of the camera operating in the canteen foyer was to protect the food and drink vending machines; however, the cameras' field of view did not cover exclusively the property to be protected, nor did the controller substantiate the existence of circumstances – e.g. theft from refrigerators or vandalism of vending machines – that would justify the monitoring of these areas. The cameras were thus capable of unjustifiably monitoring employees in the rooms used for taking breaks or eating during working hours.

In view of the above, the Authority found that the controller monitored its employees whilst they were spending their work breaks in a manner incompatible with the original purpose of data processing, namely the protection of persons and property; furthermore, the cameras' field of view was not directed exclusively at areas or property relevant to that purpose, thereby breaching the principles of data processing for specified purposes under Article 5(1)(b) of the GDPR and data minimisation under Article 5(1)(c). The Authority further found that the in-

formation provided to data subjects was incomplete, as it did not contain all the mandatory information; thereby, the controller breached Article 13(1) and (2) of the GDPR by failing to provide data subjects with adequate prior information regarding the circumstances of data processing carried out via the camera system. Due to the infringements established, the Authority imposed a fine of 7 million forints on the controller. [NAIH-9460/2025]

2. Camera surveillance of communal areas in a rented flat by the landlor

A data subject renting a room in a flat in a block of flats initiated proceedings with the Authority regarding cameras installed in the common areas of the flat (corridor and kitchen). The complainant stated that the tenancy agreement mentioned that the owners had installed cameras in the flat, but they had not been informed as to who would have access to the live feed or recordings, for what purpose, or for how long. After moving in, the tenant received messages from the landlord's husband stating that the light had been left on in the hallway and that dishes had been left on the kitchen drainer. When the tenant requested information, the person operating the camera refused to respond. Following an enquiry from the Authority, the landlord removed the cameras in question, although he maintained that he had been lawfully monitoring his own property. The Authority found that, until the cameras were removed, the landlord had carried out camera surveillance in connection with his business activities, which falls outside the scope of so-called data processing for domestic purposes; he was therefore required to apply all the provisions of the General Data Protection Regulation set out for controllers, the landlord breached the principles of transparency and lawfulness under Article 5(1)(a) of the GDPR, Article 6 of the GDPR, and Article 13(1) and (2) of the GDPR. [NAIH-14124/2025]

3. CCTV surveillance in public spaces on the grounds of public safety

A local police station approached the Office of the Commissioner for Fundamental Rights regarding a private individual operating an extensive CCTV system on their solar farm and other properties, which not only monitors and records their own premises but also public spaces and the private property of others to a significant extent. The Office of the Commissioner for Fundamental Rights forwarded the report to the Authority, on the basis of which the Authority launched an investigation

During the investigation, the controller itself admitted that it carries out surveillance using multiple cameras in such a way that it fully records, in high resolu-

tion, both video and audio footage of the public areas surrounding its properties, other building blocks and neighbouring properties. According to the controller's statement, it began the camera-based data processing at the request of the local council, the police and neighbouring residents, in order to maintain public order, which is in the legitimate interest of both itself and the other owners. The Controller also pointed out that the local authority and the police had, on several occasions, been happy to use the recordings it had made in various cases.

In its notice, the Authority found that the controller had failed to substantiate the existence of these legitimate interests. It did not demonstrate any actual damage or a specific, direct and real threat; camera-based data processing cannot be based on the occurrence of a future, potential infringement of rights; the legal basis for data processing must be objectively real and direct. The data processing purpose indicated by the controller – the protection of solar panels and property from thrown stones and other types of vandalism – can be achieved without the continuous and extensive surveillance and recording of neighbouring properties and the surrounding public areas, by restricting the monitored area to the controller's own property, the cessation of audio recording, and can also be achieved by other means that are less restrictive of the rights of data subjects (e.g. the installation of a higher fence or protective netting).

In this regard, the Authority specifically emphasised that, in the absence of a separate agreement and given its content, a reference to the rules governing neighbourhood watch schemes does not justify a person installing their own system of equipment and using it to carry out surveillance in the capacity of a neighbourhood watch member; at most, their role may consist of assisting in the monitoring of live footage from equipment lawfully operated by other authorities. As a private individual, they have no obligation, duty or right to ensure the security of the neighbourhood by arbitrarily assuming the duties of law enforcement agencies, using equipment selected at their own discretion. [NAIH-499/2024, NAIH-8031/2025]

4. Camera surveillance for the protection of vehicles parked in public spaces

In his petition, the petitioner stated that the owner of the neighbouring building had installed a camera on the street-facing façade of that building, which monitors the entrance to the petitioner's property, the cars parked in front of the property, the movements of the petitioner and guests visiting the petitioner, as well as the public space. It was established that the neighbour had carried out video surveillance using the camera in question for 18 months, during which time the camera's field of view was directed specifically at the public space; however, the

neighbour had neither displayed a pictogram nor made a data processing notice available. He stated that his vehicle, which was parked in the public area, had previously been vandalised, and that he was therefore monitoring the area for the purpose of protecting his property. However, he was unable to demonstrate the primacy of his legitimate interest or the necessity of the data processing, either in relation to himself or to other individuals. Although a request may only be submitted in relation to data processing concerning the data subject, the Authority, in its decision, found ex officio that the neighbour, by processing camera data for 18 months using a camera mounted on the façade of the property, had breached the fundamental requirement set out in Article 5(1)(a) of the GDPR, namely the principles of transparency and lawfulness, the principle of data minimisation set out in Article 5(1)(c) of the GDPR, and Article 6(1) of the GDPR, and put the controller in the wrong. [NAIH-66/2025] [NAIH-66/2025]

5. *Use of video footage recorded during the surveillance of a public space in a criminal case*

In his petition, the petitioner objected, amongst other things, to the fact that whilst he was present in front of the property owned by the petitionee, the camera system operated by the petitionee recorded him, and that the petitionee used this recording as evidence in criminal proceedings before the local police station.

The Authority found that the petitionee had continuously monitored the public space with his cameras and had also made video and audio recordings of the petitioner, which the petitionee had used in the ongoing criminal proceedings

Since the petitionee carried out surveillance and image recording specifically in public spaces, its activities fell within the scope of the General Data Protection Regulation, including the use of the recordings in administrative or judicial proceedings In its decision, the Authority also drew attention to the fact that everyone has the right to appeal to a public authority and/or a court; and to seek legal redress against any judicial, administrative or other public authority decision that infringes their rights or legitimate interests [see, for example: Article XXVIII(7) of the Fundamental Law of Hungary]. It is therefore the client's right to initiate proceedings, as the Petitioner did by submitting a request to the Authority to initiate an authority procedure for data protection and attaching evidence containing the petitionee's personal data. In light of the above, the petitionee was therefore also entitled to file a complaint and attach recordings supporting his claims to the investigating authority. Based on the definition in Article 4(9) of the GDPR, the term 'recipient' does not include authorities acting in individual cases (such as,

for example, the police station handling the case in question). In view of this, the petitionee was not required to inform the Petitioner (in advance) of the use of the video recording depicting him in the police proceedings. However, this does not mean that the petitionee did not breach the requirements regarding the transparency of data processing by failing to place a pictogram indicating data processing at the boundary of the monitored area, or provided basic information, or that it has an appropriate legal basis for the future for such continuous surveillance of public spaces and the recording of video and audio footage. In its decision, the Authority, in view of these omissions, ordered the petitionee to bring his data processing into line with data protection requirements or to restrict the monitored area to the property in his own use, so that the data processing would fall within the scope of the private-purpose exemption from the application of the Regulation. [NAIH-7876/2025 (preceding case number: NAIH-8872/2024)]

II.1.2. Data protection issues relating to cameras mounted by neighbours

The Authority receives an increasing number of complaints and requests each year concerning cameras or camera-like devices installed by the complainant's neighbour, which are directed at the data subject's property, or which may also be potentially suitable for monitoring public areas leading to the data subject's property (pavement, driveway), or areas held in undivided joint ownership (shared courtyard, communal garage, communal stairwell). In 2025, 539 such 'neighbourhood camera' investigation procedures were conducted, and 133 authority proceedings for data protection were initiated on the basis of petitions; in addition, the Authority initiated ex officio authority proceedings for data protection in 15 cases relating to camera surveillance due to the seriousness of the infringement or failure to comply with a request made during the investigation procedure.

Improperly implemented camera surveillance, image and audio recording may infringe upon data subjects' right to the protection of personal data and may also contravene the GDPR's principles of transparency and data minimisation.

Proving that data processing falls within the scope of the GDPR and clarifying the facts of the case places a significant burden of proof on the Authority during the proceedings. In a significant proportion of cases, an on-site inspection becomes necessary due to the parties' conflicting statements; thus, the Authority – exercising the option provided for in Section 71(1b) of the Privacy Act – typically contacts the competent municipal executive to have the circumstances of the data processing recorded in a public document. In cases involving neighbourhood cameras, however, camera systems nowadays operate mainly via mobile phone applications and cloud services; blurring or unblurring the images, adjust-

ing the monitored area, or switching off the device is a matter of a single button press. However, the person operating the device cannot be compelled to remove or reposition the device, as a camera monitoring an area that is either out of service or restricted by blurring no longer constitutes data processing falling within the scope of the GDPR, which forms the basis of the Authority's jurisdiction.
In a significant proportion of the submissions, however, the alleged infringement of rights concerns the intrusive effect of the neighbour's cameras and their impact on the complainant's privacy and personal rights. The essence of the complaints and requests is typically that the complainant cannot know whether the neighbour is actually monitoring them, or has merely installed a dummy camera, or whether the neighbour is actually digitally masking the image from the cameras directed at them or not; therefore, they request that the Authority order the removal or repositioning of the camera. However, it cannot be the Authority's task to manage strained neighbourly relations and the resulting mistrust.
Accordingly, the Authority has no remit or jurisdiction regarding the potentially trespass-like conduct arising from the installation of the camera in question. In the event of a breach of privacy rights, recourse may be had to the remedies provided for in Section 2:51 of the Civil Code; as the adjudication of cases concerning privacy rights, including the determination of the fact of the infringement and the imposition of an obligation to pay compensation for non-pecuniary damage, falls within the exclusive jurisdiction of the courts; the Authority cannot establish an infringement of privacy rights due to the lack of competence and jurisdiction.

The Authority's experience regarding the referral of petitions for protection of property by municipal executives and the consultation with the competent minister

In recent years, it has become increasingly common for municipal executives to refer to the Authority petitions for the conduct of property protection proceedings submitted to the municipal executive in question specifically concerning disturbances caused by neighbours' cameras in their orders or other submissions, citing a lack of competence and jurisdiction.,. As the reason for the referral, the municipal executives typically cite that they lack the competence to examine the processing of personal data within the framework of property protection proceedings. However, in the Authority's view, in the referred property protection complaints (whether submitted via the standard form or in free text), the complainants' request relates to the conduct of property protection proceedings and the cessation of the disturbance; and they seek the removal or relocation of devices targeting their property; the complainants do not formulate a specific claim for legal protection falling within the Authority's remit and based on the General

Data Protection Regulation, either by reference to legislation or in the content of their submissions.
In the referred cases, the Authority almost without exception initiates a consultation procedure with the locally competent municipal executive who referred the petition to the Authority, drawing their attention to the distinction between examining the lawfulness of data processing and the related case law.

In view of the above, the Authority has on several occasions approached the competent government office regarding the municipal executive's proceedings. In the majority of cases, thanks to the intervention of the government offices, the municipal executives ultimately conduct proceedings for the protection of property in the matter.

On one occasion, the competent government office informed the Authority that the government office has jurisdiction solely to adjudicate appeals against decisions made in enforcement proceedings, and acts as the municipal executive's supervisory body only in proceedings initiated for the enforcement of the obligation set out in the property protection decision. In view of this position taken by the government office, on 4 December 2025 the Authority submitted a request to the Minister for Public Administration and Regional Development, who is responsible for the professional supervision of the activities of the metropolitan and county government offices. On the basis of the above, the Authority informed the Minister of its comments and position as follows [NAIH-8378-10/2025]:

1. The Authority's position, as set out in its submission, is that the Authority cannot take over the application of the legal institution of property protection from the municipal executives; the Authority would only be able to examine data processing carried out by means of the camera, not the orientation of the camera (as a device).

2. It drew the Minister's attention to the fact that, pursuant to Section 7(1)(b) of the Government Decree, the municipal executive shall reject the petition by way of a decision if he or she finds that he or she lacks the power or jurisdiction to act, in which case the petitioner is entitled to a right of appeal.

3. Municipal executives do not forward petitions to the Authority via an official repository (but, for example, by post), without an electronic signature, as documents that are not electronically authenticated or certified; yet, under the Act on the digital State, they are classified as organs obliged to conduct electronic administration and provide digital services.

4. Municipal executives often forward petitions received via simple email to the Authority without attempting to verify the client's identity, and do not request that petitioners provide missing personal identification details.

5. Complainants generally attach to petitions forwarded to the Authority 'only' external photographs of the device appearing to be the camera in question, and no evidence suggesting data processing or indicating the processing of personal data.

6. The Authority informed the Minister that numerous court decisions have also been made to the effect that a camera operated by a neighbour is capable of infringing the complainant's right to privacy, and that this is therefore a matter falling within the scope of proceedings for the protection of property rights (Pfv.21.318/2016/4.; EBH2001.519.; PJD2018.8.; BDT2019.4000.).

In order to avoid future disputes over jurisdiction and competence, to prevent the protracted nature of conciliation proceedings and to ensure efficient administration, the Authority has requested the Minister to set out a legal position which the Authority could rely upon before the government offices and municipal executives in individual cases, as the legal practice of government offices and municipal executives could be effectively standardised in this area through such ministerial guidance, or possibly by clarifying the Government Decree on property protection.

In his reply [JHÁT/7-2/2026-KTM, 2 February 2026], Dr Szilárd Horvát, State Secretary for Public Administration at the Ministry of Public Administration and Regional Development, informed the Authority of the following:

The State Secretary for Public Administration agreed with the Authority's finding that the mere perception of being under observation is not a data protection issue but a matter of protection of property rights, and that the Authority cannot deprive municipal executives of the right to apply this legal institution.

The State Secretary for Public Administration also noted that the option provided for in Section 71(1b) of the Privacy Act provides the Authority with the opportunity to involve the municipal executive in its proceedings to verify the actual circumstances of camera-based data processing, thereby enabling a preliminary investigation of the facts, on the basis of which the aspects specified in the Authority's request can also be examined.

On the basis of the above, the State Secretary for Public Administration took the view that a solution which would reduce the administrative burden and also be appropriate in terms of clients' rights would be for "the municipal executive to examine the existence of data protection circumstances relating to the case within the scope of the legal institution of property protection", and, in the absence of jurisdiction, would notify the client in a decision of rejection of the possibility of enforcing their claim through the data protection authority, thereby dispensing with the practice of automatic referral by order. In the event that the complainant subsequently turns to the Authority, the Authority may, in the proceedings it initiates, continue to request the municipal executives to clarify the facts of the case, on the basis of which it may conduct proceedings falling within its jurisdiction or close the investigation.

Legislative initiatives proposed by the Authority

The Authority has not identified any provision in the current legal framework that would enable a natural person, in relation to a device appearing to be a camera installed by a neighbour and directed towards them, to ascertain whether the camera is actually monitoring, or recording images—or possibly both images and sound—of the property they use, the part of the jointly owned property which they themselves are lawfully using, or that part of the public space through which they would lawfully pass and thereby become the subject of surveillance.

The owner is entitled to protection of property against unnecessary disturbance; however, in the majority of cases, no such disturbance actually occurs – the devices are dummy cameras, their images are restricted to their own premises by physical or digital blurring or masking, and the camera does not monitor the neighbour – however, this only comes to light during proceedings, and establishing this within the framework of such proceedings places a significant burden on municipal executives and the courts, which could be avoided by exercising this new right.

Data subjects may also exercise their right of access under Article 15(1) and (3) of the General Data Protection Regulation (GDPR) vis-à-vis their neighbour; however, this right alone is not sufficient to address the problem effectively. This is because, as a result of exercising this right, the data subject can only access their own data, not the entire camera image. On the other hand, if the camera does not monitor a public area or a private area owned or exclusively used by another party (e.g. due to the use of masking or the installation of a dummy camera), then the activities carried out by that private individual do not fall within the

scope of the General Data Protection Regulation, and therefore the person installing the camera (or a device resembling a camera) is not obliged, nor can they be compelled, to respond to or comply with a request to exercise the right of access. Another common problem arises when the complainant or petitioner in a previous case remains convinced, or continues to believe, that the camera operator has since removed the digital blurring and resumed audio recording due to the poor relationship between them. The individual, previously classified as a controller, may then lawfully remain silent in response to the data subject's exercise of their rights; as a result, the data subject initiates proceedings with the Authority or the municipal executive, in which the conduct of an inspection, and the formal taking of statements from the persons involved in the proceedings results in significant administrative burdens and costs, even though repeated unlawful data processing is only brought to light in very few cases.

The Authority intends to address the above issues by initiating legislation from two regulatory angles: on the one hand, by expanding the rights of neighbours enshrined in civil law with a new, specifically named right; and on the other hand, by appropriately amending the relevant building regulations. In this regard, the Authority has made the following proposals to the legislator:

1.) The Authority proposed that the Civil Code should specifically define as a neighbour's right the right of a neighbour to view the camera's image, type and settings – upon request, at specified intervals or on specific occasions – in order to ascertain that the camera surveillance and recording is not directed at their property or an area under their exclusive use. The detailed rules governing this new neighbour's right could be further regulated in Act CLXXIV of 2013 on the special rules concerning neighbour's rights and the limitations of property rights.

2.) In addition to the above, the Authority has also proposed amendments to the relevant building regulations, such that if a decision is made to install a camera (system) during the design, construction and commissioning of buildings, the installation and operation of the camera (system) may only be installed and operated in accordance with the provisions of the legislation in force (in particular, in such a way that the field of view of the camera(s) does not face a public space or an area owned or exclusively used by a private individual, and an appropriate first-level data processing notice or pictogram is displayed).

Even if adopted, the above legislative amendments would not restrict data subjects in the exercise of their rights under the General Data Protection Regulation (in particular, the right to request a copy in the context of exercising the right of

access); similarly, in the event of interference, there would be no change to the right to initiate proceedings for the protection of data, nor, in the event of unlawful data processing, to the right to initiate proceedings with the Authority.

II.1.3. Politics related cases

1. The Authority's measures taken in relation to the databases of Tisza Party

1. Early in October 2025, articles about a data breach affecting the databases of the Tisztelet és Szabadság Párt (Party of Respect and Freedom, hereinafter: Tisza Party) were published in the press. On 8 October 2025, Tisza Party reported a data breach to the Authority, which was amended by the Party with a submission dated 5 November 2025 in view of the escalation of the data breach at the end of October or in early November 2025.

Following the notification of the data breaches, the Authority launched an authority procedure for data protection against Tisza Party ex officio on 11 November 2025.

2. Early in November 2025, a person of unknown identity published a file containing all the personal and special category data through a website expressly specialised in the storage and trade in databases acquired illegally (earlier at the beginning of October 2025, unknown persons published only a minor part of the Tisza Party database).

Several media content providers reported on this disclosure in their articles, using the personal and special category data for their reporting. The Authority received several submissions on account of the reports of the news portals, in view of which the Authority issued a communiqué on 6 November 2025[4]. In this, the Authority underlined that the vulnerability of an IT system used by a political party for its political activity may qualify as a matter of public interest, this in itself, however, does not create a lawful basis for the person exploiting the data security deficiency for storing an disclosing the personal and special category data of the data subjects in the database. If a media content provider reports on this matter of public interest and while doing so uses the personal and special category data disclosed as a result of the actions of the person in violation of the law, the content provider must abide by the provisions of the General Data Protection

4 https://naih.hu/dontesek-adatvedelem-tajekoztatok-koezlemenyek/file/1303-kozlemeny-a-politikai-partok-adatbazisaibol-nyilvanossagra-kerulo-szemelyes-es-kulonleges-adatok-mediaszolgaltatok-altali-felhasznalasanak-adatvedelmi-kovetelmenyeirol

Regulation and the judicial practice determining the balance between the freedom of the press and the right to the protection of personal data. In this context, the Authority declared that in the case of the storage of personal data and their use in media content, the media content provider is solely responsible for its data processing activities.

3. A person of unknown identity created a website early in November 2025 using the personal and special category data originating from the databases of Tisza Party, in which anyone could search the disclosed data of the data subjects based on address using a map, learning inter alia the names, phone numbers and e-mail addresses of the data subjects and thereby could draw conclusions concerning their political opinions. The person of unknown identity made the website accessible to anyone on 7 November 2025.

The Authority learned of the launching of the website from the press and on the very same day, on 7 November 2025, issued a communiqué concerning the map[5]. In this, the Authority declared that the person of unknown identity perpetrated a criminal act by using the personal and special category data, hence it was necessary to erase them immediately. The Authority underlined that if the website was not erased, the Authority would apply the legal means available to it to achieve the removal of the website.

The website containing the map became inaccessible on 9 November 2025. Nevertheless, on that very same day a person of unknown identity created a new website publishing the personal and special category data from the databases of Tisza Party as a searchable database. In this website, the data of the data subjects could be accessed based on keyword searches.

4. A number of media content providers reported on the accessibility of personal and special category data from the Tisza Party databases on a map through their online news portals. Several news portals also published the link pointing to the map in their articles. Because of rendering the link accessible, an extraordinarily large number of people turned to the Authority: in just a few days, the Authority received altogether 685 petitions requesting procedures. Of those contacting the Authority, 250 initiated an investigation, while 435 submitted petitions to conduct authority procedures for data protection. During the existence of the Authority, there has never been a case where such a large number of submis-

5 https://naih.hu/hirek/787-koezlemeny-a-partszimpatizansok-adatainak-terkepen-keresztueli-koezzetetelenek-jogellenessegerol

sions were received within such a short time in relation to the same alleged violation of the law.

In view of the outstanding number of the submissions, the Authority launched authority procedures for data protection against five media content providers on account of their articles published on their websites and other data processing activities related to their reporting activities. In the course of this procedure, the Authority called upon the media content providers to make statements and enclose documents with a view to clarifying the facts of the case.

In view of the fact that the subject matter of the authority procedures for data protection launched ex officio and the authority cases initiated by the petitioners were closely related based on Section 60/A (2a)(b) of the Privacy Act, the Authority suspended the authority procedures launched based on petitions submitted by the petitioners. This provision of the Privacy Act enabled suspension of a procedure, if without another decision by the Authority closely related to the specific case, the case could not be reasonably decided. The suspension of the procedure initiated by the petitioners lasts until the Authority makes its decision in the authority procedures for data protection launched ex officio.

In parallel, the Authority rejected the submissions initiating investigation of the media content providers without consideration of the merits based on Section 53(3)(g) of the Privacy Act as the Authority had launched authority procedures for data protection ex officio because of the processing activities objected to in the petitions for investigation. Based on this provision of the Privacy Act, the petition is to be rejected without considering the merits of the case, if the Authority is pursuing an authority procedure concerning the subject matter of the submission.

5. On 12 November 2025, the Authority lodged a report with the police against unknown perpetrators on account of the offence of abuse of personal data extending to special category data through unlawful data processing according to Section 219(1)(a) of Act C of 2012 on the Criminal Code. In its reports, the Authority addressed the alleged clash of both the first publication of the databases of Tisza Party and their disclosure through the map and as a searchable database with the relevant provisions of the Criminal Code. On 1 December 2025, the police notified the Authority of having ordered an investigation in the case.

6. Ex officio, the Authority launched an investigative procedure to study the lawfulness of the database concerning the special category personal data of the data subjects who had volunteered with the Tisza Party and compliance with the

data protection requirements of the database managed by the Tisza Party as there was a data breach related to the database (see 7.Data breach concerning the app TISZA VILÁG of Chapter II(3)(1)).

The Authority qualified the purpose of processing as lawful as it was the conclusion of the volunteer agreement, its implementation, the performance of the tasks of volunteers and the selection of volunteers.

As to the data processed in the database, the Authority focused on the examination of the lawfulness of the comments concerning volunteers. In this context, it established that the data entered in the comments field of the database related to the data subjects, but they represented information that could also be interpreted as the opinion of the person interviewing the volunteer; hence they were personal data of both parties. The comments contained the opinions, assessments and conclusions of the interviewer whether the data subject applicant would be suitable for discharging the tasks of volunteer, hence there may be a need to record the data. The opinions could play a role in whether or not the agreement would be concluded with the applicant for a volunteer position. In view of this, as soon as the agreement is concluded or an unambiguous decision is made that the party would not enter into an agreement with the applicant, the data set forth in the comments field must be erased. It is, however, important that the data subjects be informed of the processing of these data and Tisza Party failed to meet this obligation to provide information.

The Authority investigation disclosed that the comments field contained sensitive information about the applicants, including, in some cases, morally objectionable descriptions. The Authority underlined that, based on their right to access, a data subject is entitled to learn what kind of data the controller processes on them and is also entitled to request a copy of their data, in this case the part of the party's records or database concerning them, including the opinions on them set forth in the comments field. The controller, i.e. the party, is responsible for providing training and information to those interviewing on behalf of the party, enabling them to be aware of the contents of the right to access, and to enter comments and opinions, which contain correct, ethical statements and refrain from defamatory, rude or vulgar statements.

In addition to establishing a violation of the obligation to inform, the Authority called upon the controller in its decision closing the procedure to erase the already purposeless and unnecessarily personal data in the comments field of the volunteer database and to provide appropriate information on the processing of

data related to the conclusion and performance of the volunteer agreement in the future. [NAIH-12827/2025.]

7. In relation to the data breach affecting the Tisza Világ [Tisza World] application run by the Tisza Party, data subjects submitted access requests to the Authority as controller on 37 occasions in November and December 2025, in which petitioners requested information from the Authority on whether they were concerned in the data leakage and if so, which of their personal data were affected by the data breach and requested information on the possibilities of legal remedy.
More than half of the petitions were sent simply by e-mail; with regard to these, the Authority notified the alleged data subjects of the data subject rights regulated under Chapter III of the General Data Protection Regulation and informed them that they would be able to submit their petitions in the manner identified in the information published by the Authority.
In the case of petitions, received in an identified manner, in which the petitioners did not provide sufficient data for their identification in the database processed by the Authority, which had become accessible on the Internet as a result of the data breach (hereinafter: database), the Authority requested the petitioners to submit additional data assisting in their identification with a view to meeting the data security requirements and the protection of data subject's rights.
With regard to the petitions submitted in the identified manner containing the personal data required for identification in the database, after reviewing the database the Authority notified the data subjects – if they were indeed affected – exactly which of their personal data were included in the database processed by the Authority and further informed them that if they deemed that their personality rights were violated, they could turn to the courts and in the case of suspicion of abuse of their personal data, they may file a report with the investigative authorities. With regard to the exercise of data subject's rights in cases where the data of data subjects were not included in the database processed by the Authority, the Authority informed them of the absence of their capacity as data subjects. In addition, the Authority notified the data subjects that they could also exercise their data subject's rights at the controller of the Tisza Világ application, the Tisza Party or through its data protection officer.

2. The lawfulness of processing data for campaign purposes

The petitioner received election campaign materials from the petitionee nominating organisation by mail in relation to the 2024 election of the Members of the European Parliament, municipal representatives and mayors. The petitioner's

name and address were shown on the mail objected to. In view of the fact that the petitioner had earlier forbidden the issue of his personal data for campaign purposes in a verifiable manner at the National Election Office (hereinafter: NVI), he deemed that the petitionee processed his personal data above indicated without appropriate legal basis. In his petition, the petitioner requested the Authority to establish the fact of unlawful processing affecting him.

In the course of the procedure, the petitionee wished to verify the validity of the petitioner's consent as data subject by sending the Statement of Consent completed by the petitioner in June 2021. As a matter of fact, the Statement of Consent included a call for maintaining contact in the future: "If you wish to remain in contact with [...] and receive information of news deemed to be important by it, we request you to mark the following circle" (the circle shown next to this part of the text was marked with two intersecting lines).

The petitioner acknowledged the completion of the Statement of Consent, however, in his view that did not extend to the use of his personal data for campaign purposes and in view of the fact that the petitionee had not used his personal data for an extended period of time since the completion of the Statement, he regarded the use of his personal data as a violation of the law.

The Authority did not accept the objection of the petitioner, according to which the petitionee was not entitled to use the personal data he had provided for the purpose of an election campaign. In this context, the Authority pointed out that the Statement of Consent accepted by the petitioner expressly stated: the person marking the circle consented to the nominating organisation providing information on subject matter that it held to be important. In the absence of an expressly restricting or excluding provision this consent reasonably included the sending of campaign materials to the petitionee, in view of the fact that during the campaign period related to municipal and European Parliament elections, such content would qualify as relevant and important information for the nominating organisation.

Furthermore, the Authority established that according to the text of the Statement of Consent, the petitioner consented to having the petitionee processing the data provided by him "for the purposes of maintaining contact, requesting opinion, providing electoral and other information until the withdrawal of the Statement of Consent to the processing". In view of the provision also accepted by the petitioner, the Authority took the position that the petitionee lawfully used the petitioner's personal data for the purpose of sending campaign materials, irrespective of the

fact that they had not been used for a purpose corresponding to the purpose of processing for an extended period of time – in the present case for three years. As the provision "process until withdrawn" applied by the petitioner does not specify a pre-recorded objective restriction in time, the petitioner does not have any good ground to refer to the fact that the nominating organisation had not provided information to him over an extended period of time earlier with regard to the campaign material sent to him.

Finally, the Authority also pointed out the need to distinguish the legal institution for forbidding the issue of personal data for campaign purposes before the NVI and the case when the petitioner directly enters into contact with a nominating organisation and provides his personal data voluntarily for the purpose of sending information. The two cases presume separate processing activities and databases. In the former case, NVI issued the personal data of voters to nominating organisations wishing to run at the given election for the purpose of their campaign activities provided that these voters had not given their express objection to that. However, this regulation does not extend to the case when a voter actively and voluntarily provides his personal data himself to a nominating organisation specifically for the purpose of receiving information. [NAIH-10767-2025]

3. Processing by politicians affecting children

The notifier turned to the Authority against a Member of Parliament controller because the Member of Parliament published photos of under-age children made of them and taken together with them in the course of a parliamentary visit to an elementary school class in his Facebook profile. According to the position of the notifier, the controller violated the principle of lawful processing set forth in the GDPR (Article 6) through his processing related to the disclosure. Presumably, the publication of the facial images of children for political purposes was not done on the appropriate legal basis, thus in particular on the consent of their legal representatives. Based on the conditions of consent (Article 7), it is doubtful that the parents even if they gave their consent received appropriate information of the fact that the facial images would be used for the purposes of a political campaign. According to the arguments of the notifier, the personal data of the children enjoy special protection; first and foremost, the overarching interest of the child has to be taken into account and participation in a political campaign cannot be considered to be in the best interests of the children; the entry may carry political messages and serve the purpose of popularising the political activities of the Member of Parliament and assist in the individual political branding of the controller. The Authority launched an investigative procedure because of

the making and disclosure of the facial images in the Facebook entry. Upon being contacted by the Authority, the Member of Parliament controller erased the Facebook entry under investigation. The Authority's investigation is still in progress. [NAIH-165/2026., antecedent: NAIH-16738/2025.]

In another similar case, the notifier turned to the Authority against a Member of Parliament controller because the Member of Parliament made photos of underage children and taken together with them as part of a "headmaster's class" with students of an elementary school class in his Facebook profile. The Authority launched an investigation because of the making and disclosure of the facial images displayed in the Facebook entry, but the Member of Parliament controller failed to respond to the Authority. The Authority's investigation had not yet been closed. [NAIH-699/2026., antecedents: NAIH-15016/2025.]

4. Investigation into the lawfulness of processing related to a mother-to-be beauty contest

The Authority received numerous notifications in which the notifiers disputed the data protection compliance of a photo competition announced in the Facebook page of a Member of Parliament. According to the invitation, photos of pregnant women could be submitted for the photo competition of the Member of Parliament without the knowledge or consent of the data subject, even including photos made of the mothers-to-be in secret.
Based on the notifications, the Authority conducted an investigation, and on the basis of the available information established that the Member of Parliament as controller violated the principle of transparency according to GDPR Article 5(1)(a) and failed to verify a legal basis for the processing of the photos according to GDPR Article 6(1), and furthermore, breached his obligation to provide information according to GDPR Articles 13-14.
In view of the above, based on Section 75/A of the Privacy Act, the Authority issued a warning according to GDPR Article 58(2)(a) and based on Section 56(1) of the Privacy Act called upon the Member of Parliament twice to immediately take action to terminate the unlawful processing implemented in relation to the mother-to be beauty contest associated with the photo competition; align his processing operations with the legal regulations, including erasure of the part of the invitation to compete, on the basis of which the photos showing the data subjects could also be made in secret; irrevocably and verifiably erase the photos made of data subjects in secret and provide information on the processing in compliance with the provisions of the GDPR linked to the invitation to compete and to the data subjects who had earlier sent their data to the Member of Parliament.

In view of the fact that the Member of Parliament did take the measures indicated in the Authority's calls and notify the Authority of the measures taken in writing, the Authority closed the investigation. [NAIH-4488/2025]

5. Detailed guidance on the data protection aspects of the 2026 parliamentary election campaign

With a view to the protection of citizens' rights and to provide information to the nominees and nominating organisations participating in the electoral process, the Authority published its detailed guidance[6] on the data protection aspects of the 2026 parliamentary election campaign. The purpose of the document is to assist the controllers in developing lawful and transparent processing practices. The Authority underlined that the principles of the GDPR must govern every stage of the campaign activity because a specific feature of processing operations for political purposes is that these data may concern the most sensitive areas of the privacy of the data subjects. To ensure the lawfulness of processing, controllers must act with particular circumspection in the campaign when processing personal data.
The published guidance presents the Authority's practice related to the campaign period in detail including, inter alia, the interpretation of the individual principles, the roles of the controller/processor, the legal basis related to processing, the importance of providing information on processing, the efficient guaranteeing of data subject rights and requirements for the individual specific means of campaigning, thus in particular, newsletters and campaign calls.
In this document, the Authority particularly dwells upon the use of social media, particularly, the use of photos made of children for political purposes, the role of the press and the importance of the freedom of the press.
Through specific cases, the Authority provided guidance to controllers pointing out the typical mistakes, which resulted in authority procedures in the course of earlier campaign periods, and in this context, also presented good practices.
Similarly to earlier election periods, the Authority will continue to pay specific attention to the oversight of the lawfulness of processing for political purposes and in the event of data protection breaches it will take the necessary measures to protect the rights of data subjects. [NAIH-14834/2025]

6 https://www.naih.hu/tajekoztatok-kozlemenyek?download=1321:a-nemzeti-adatvedelmi-es-informacioszabadsag-hatosag-tajekoztatoja-a-2026-evi-orszaggyulesi-valasztasi-kampany-adatvedelmi-vonatkozasairol

II.1.4. Processing of health data

1. Data processed by a hospital and disclosed by the press

The Authority launched an investigation following notifications in the public interest, as an article published on a website revealed that the President of the Respect and Freedom (TISZA) Party, his relatives and a close acquaintance (hereinafter: the data subjects) had received healthcare services at a specialised centre within a hospital since 2014, including the number of occasions and the nature of the services received.

The Authority found the user permission settings in the hospital's medical system to be appropriate, and no credible evidence emerged during the proceedings to suggest that the publisher had gained knowledge of the data subjects' personal data published in the article from the medical system. Nor was there any evidence that any data access had taken place at the hospital or within its medical system that would constitute unlawful data transfer, given that all employees with access rights had access to the data subjects' personal data in the medical system in the course of medical treatment.

An internal IT and information security investigation conducted by the hospital found that the medical system's database contained data that differed in part from that reported in the press.

Consequently, using the tools at its disposal, the Authority was unable to determine whether any of the hospital's employees had leaked the data, as, in the absence of further direct evidence, it was not possible to establish a clear causal link between the data stored in the medical system and the press article. [NAIH-72/2025.]

2. Case study published publicly on a website

The Authority received a notification in the public interest stating that a homeopathic case study was publicly available on a website offering homeopathic and psychotherapeutic treatments, containing data on the mental state of a patient suffering from an obsessive-compulsive disorder, as well as information regarding their sexual orientation and religious affiliation. According to the complainant, the data subject can be identified on the basis of detailed personal circumstances (age, education, place of work).

With regard to the data processing carried out via the website, the Authority found that the controller is the company operating the website, as the homeopathic doctor carrying out healthcare and therapeutic activities performs these activities within the organisational framework of this company, in its name and on its behalf. In contrast, with regard to the writing of the case study published on the website, the Authority found that the controller is the doctor. In the Authority's view, the author of an article, study or written work becomes a controller if they include personal data or identifiable individuals in their work, and bring the work – and thereby the data – to the attention of others, communicate it, publish it or transmit it. Copyright protects literary, scientific and artistic works, as well as the acts associated with their use. The homeopathic case study was prepared and written by the doctor based on one of his therapeutic cases; therefore, he is clearly the author and the holder of the copyright. In writing the study, he decided which personal data to use and how, and which scope of personal data was necessary for the study. Furthermore, the doctor decided to send the case study to others, to make it accessible and to publish it.
The Authority found that the homeopathic case study had not been adequately anonymised, and therefore held the doctor liable for breaching the principle of data minimisation, as well as the company liable in connection with the publication, since it failed to check whether the data subject could be identified prior to publishing the case study on the website and published the study without doing so. [NAIH-7724/2025.]

3. Access to health data

In the case under review, the petitioner submitted a request for access to the petitionee healthcare institution, asking for all health data processed during the petitioner's outpatient care to be sent electronically. However, the petitionee informed the petitioner that it could only provide the petitioner with a copy for a fee of 200 HUF per page, , as the document provided at the time of treatment is supplied free of charge, which is considered the first copy to be provided free of charge. Furthermore, the petitionee informed the petitioner that, in accordance with data protection legislation, the petitioner could not receive their medical records electronically, but only in person. During the proceedings, in response to the Authority's request, the petitionee stated that the provision of incorrect information to the petitioner was the result of an isolated administrative error, and that, upon realising the error, the requested medical records were ultimately sent to the petitioner free of charge by electronic means.

The distinction between the rules of the healthcare sector and the data subject's rights under the GDPR is of fundamental importance for the assessment of this case. Act CLIV of 1997 on Healthcare (hereinafter: the Healthcare Act) stipulates that medical records must be kept regarding treatment, and that at the end of treatment the patient is entitled to receive a document issued regarding their illness and treatment, the outpatient record, or the final report. The Health Act also stipulates that the General Data Protection Regulation must apply to the data subject's exercise of rights in relation to their personal and health data. Whether or not the data subject has received a medical report in accordance with sectoral regulations, if the data subject requests a copy of their documentation within the scope of their right of access, the request must be assessed in accordance with the General Data Protection Regulation. Thus, when the data subject requests a copy from the controller for the first time of a report which they may otherwise already be in possession of, the controller may not, in the course of the data subject's exercise of their rights, rely on the fact that the report has already been issued to the data subject under sector-specific regulations. In the present case, it was established that the petitioner had submitted a request for a copy for the first time since the mandatory application of the GDPR, and therefore the petitionee should have provided the documentation free of charge.

The Authority also examined the method of fulfilling the right of access and found that, if the data subject so requests, the copy must also be provided in electronic form. The General Data Protection Regulation does not state that if the request was submitted electronically, it must be answered electronically, but rather that if the request was submitted electronically, the information must be made available (where possible) in electronic format. The petitionee replied to the petitioner's request for access on the same day and made compliance with the request subject to payment of a fee; subsequently, months later, after becoming aware of the initiation of the administrative proceedings, the petitionee complied with the request electronically and free of charge. In view of the above, the petitionee did not commit an infringement by failing to comply with the petitioner's request for access within the one-month deadline set by the General Data Protection Regulation via email, i.e. electronically, as it could lawfully have complied by post on a DVD attached as an enclosure or by personal delivery on a DVD in electronic format. However, it committed an infringement by making the fulfilment of the petitioner's right of access subject to the payment of a fee. Consequently, the Authority found the petitionee at fault. [NAIH-2306-1/2025]

II.1.5. Data processing in the public sector

1. Transfer of personal data in administrative proceedings

In this case, the Authority examined whether it was lawful for the petitionee to include and transfer the address details of the petitioners (the Mother and her two minor children) in the summons sent to the maternal grandparent in the authority proceedings conducted before it at the request of the maternal grandparent concerning grandparental contact.

According to the facts established in the case, the maternal grandparent submitted a petition for grandparental contact to one of the district guardianship offices; according to this petition, contact between the maternal grandparent and the mother had been severed for 10 years, the petitioner does not speak to the grandparent, and so the maternal grandparent does not know her grandchildren born in the meantime, nor is she aware of the petitioners' addresses. The district office, based on data from the personal data and address register, determined that it lacked jurisdiction and transferred the petition to the petitionee with jurisdiction. The order directing the transfer did not contain the address details of the petitioners in the present case – which determined the petitionee's jurisdiction. The district office notified the petitionee and the petitioner in the main proceedings, namely the maternal grandparent, of the transfer.

On the basis of the contact petition transferred to it, the petitionee scheduled a settlement hearing, to which it summoned the Mother, her spouse and the maternal grandparent as parties. Each of the summonses contained the petitioners' address details, whereas the summonses sent to the petitioners did not contain the maternal grandparent's address details.

The petitioners brought an action against the petitionee's decision on the merits in the authority proceedings concerning contact with the grandparents. The court found the action to be well-founded, and therefore set aside the original decision and ordered the petitionee to conduct new proceedings. In the final decision on the merits issued in the new proceedings, the petitionee regulated contact with the grandparents within the framework of supervised contact at the contact service of the child welfare centre competent for the children's place of residence, the location of which was amended, at the parties' request and in view of the petitioners' move, to the contact service of the competent child welfare centre at the children's place of residence. The amending decision does in-

clude the petitioners' place of residence but does not contain the address details of their place of residence (with the exception of the name of the settlement).

A fundamental condition for the lawfulness of data processing is the existence of an appropriate legal basis, which the controller must select for each individual instance of data processing and data processing operation. The fact that the controller has an appropriate legal basis for accessing and recording the personal data in question does not mean that, on the basis of the same legal basis, the inclusion of the data in a decision or its transmission is also necessary, and that this would thereby be lawful. The lawfulness of data processing also requires that the controller has an appropriate legal basis for these latter data processing operations.

In the proceedings, the petitionee argued, in relation to the inclusion of the petitioner's address details in the summons and the disclosure thereof, that in authority proceedings concerning the arrangement of contact, the clients' address details play a decisive role both in general (e.g. in determining jurisdiction) and specifically (e.g. in determining the distance between the clients' places of residence when designating the place of contact), their inclusion in the documents is a mandatory element of content, knowledge of this is also essential for opposing parties, as without precise knowledge of it – as relevant information underpinning the decision – they cannot make a well-founded statement on the merits during the proceedings, furthermore, it also noted that the petitioners had not requested restricted data processing and had not cited any circumstances which, had they existed, would have raised the question of ordering restricted data processing ex officio.

In the proceedings, the Authority – without disputing the petitionee's right to access and process clients' address data, the significance of such address data as a factor influencing the substantive decision beyond the determination of the competent authority's jurisdiction, and agreeing with the requirement for the accuracy and up-to-date nature of the data contained in the decisions, and that it is essential for clients to be aware of the relevant information on which the authority's decision is based – found that none of the provisions cited by the petitioner requires the authority to include all relevant data arising in the case in all its decisions, or to forward such data to all clients.

Section 81(1) of the Code of General Administrative Procedure requires that the data necessary for the identification of clients and the case be included among the substantive elements of the decision; it does not specifically mention address

details. Although address details are suitable for identifying the client, in the present case other natural person identification data, which were already known to both parties, were available for identification purposes; consequently, the inclusion of the petitioners' address details for this purpose was clearly unnecessary on the part of the petitionee. Furthermore, this argument by the petitionee was not acceptable because the petitioner in the main proceedings, the maternal grandparent, was also classified as a client in the main proceedings; yet, with regard to her identification as a party, the petitionee did not deem it necessary to include the same set of data in the summonses sent simultaneously to the opposing parties. In this regard, the Authority also pointed out that, in addition to the Code of General Administrative Procedure and other legislation governing the case, the authorities must also comply with the provisions of the GDPR, including the principle of data minimisation, which requires the acting authority to specify the narrowest possible scope of personal data, even if no order for restricted data processing is made during the proceedings, either upon request or ex officio.

With regard to the role of the address in determining jurisdiction, the Authority takes the view that in a procedural decision, including the summons under review here, it is sufficient to state that the authority is acting as the competent authority based on the place of residence of the parent exercising parental care over the children concerned; furthermore, in accordance with the principle of data minimisation, it is not necessary to include precise address details – more specific than the name of the municipality or the district of the capital – in the decision sent to the opposing party.

In the present case, in the summons addressed to the maternal grandparent, the Authority considers that, in accordance with the principle of data minimisation, it would have been sufficient for the identification of the case and the parties to include the names of the parties and one of the natural person identification data specified in the Personal Identification Code Act, which were already known to the maternal grandparent in other contexts, particularly given that the opposing parties were notified of the proceedings at the same time as the summons was issued, and thus the petitioners had no prior opportunity to request the restricted processing of address details previously unknown to the maternal grandparent, or to present circumstances which, if they existed, would give rise to the question of ordering restricted data processing ex officio.

Furthermore, since in the specific case – as the court also noted in its decision – only supervised contact was possible, the Authority considers that the petitionee

was required to take the children's address details into account ex officio when making the substantive decision, from the perspective of the competence of the institution to be designated as the venue for contact; the need to disclose the petitioner's address details to the maternal grandparent could not therefore have arisen as an issue in the first place, nor was it relevant to the maternal grandparent's right to make a statement as a client.

The Authority noted that it is precisely the subject matter of the main proceedings, namely the arrangement of contact, that requires particular attention from the acting guardianship authority with regard to what personal data it discloses to opposing parties, particularly where – as in the case under review – it can be clearly established from the petition itself that contact between the parties has been severed, the opposing party involved in the arrangement of contact 'is not on speaking terms' with the petitioner for contact, they do not know each other's addresses, and indeed, in the present case, the maternal grandparent does not know her own daughter's family, and thus the children concerned by the contact arrangements either.

In the Authority's view, taking the foregoing into account, the fact that no petition for restricted data processing was submitted in the main proceedings, or that no further circumstances giving rise to an ex officio order for restricted data processing emerge from the petition for contact (nor is it in the interest of the person requesting contact to report such circumstances), it cannot, in principle, mean that the addresses of the minors or the parent(s) exercising parental authority may be disclosed to the person requesting contact without due consideration, particularly not in such a way that the guardianship authority discloses the address of only one party whilst remaining silent on the address of the other party.

In view of all this, the Authority could not accept the petitionee's argument that the inclusion of the petitioners' address details was a necessary mandatory element of the content and – in the absence of a request for restricted data processing or relevant circumstances – was therefore lawful in the summons sent to the maternal grandparent, and concluded that the inclusion of the contested data in the decision was unnecessary, and that their disclosure to the opposing party was unlawful in the absence of an appropriate legal basis.

On the basis of the above, the Authority upheld the petitioners' complaint and found the petitionee in breach of Article 5(1)(c) and Article 6(1) of the GDPR. As a legal consequence, it ordered the petitionee to bring its data processing operations into line with the provisions of the GDPR by establishing internal rules re-

garding the decisions it makes to determine the minimum personal data content required for client identification. [NAIH-8686/2025.]

2. Data processing by a police organ as employer

The Authority conducted an investigation into the data processing activities of a police station (hereinafter: the controller), which was the complainant's employer. According to the controller's statement, a report had been received concerning an act giving rise to a suspicion of a criminal offence in relation to the complainant. A senior inspector from the controller's Inspection Service – acting on verbal instructions from the head of the department at the time – made a video recording of the complainant. The controller handed over the CD containing the recording to the head of the Human Resources Department, who forwarded it to the public prosecutor's office.

The controller argued that, on the basis of a report concerning an act giving rise to a suspicion of a criminal offence, a police officer acting within the scope of his official powers is under a duty to take action. The controller cited Section 13 as well as Section 42(1) and Section 42(6)(a)(aa) of the Police Act as the legal basis for making the video recording. According to the controller, the video recording was made for the specific purpose of obtaining data necessary for the conduct of criminal proceedings as evidence.

The video recording was made by the Inspection Service, acting as the controller and the complainant's employer, on the basis of verbal instructions. It can be established from the Inspection Regulations that it is not the role of the Inspection Service to investigate criminal offences on the basis of a complaint. According to the Inspection Regulations, the Inspection Service is authorised to carry out professional police inspections, including the making of video and audio recordings in this context. It is obliged to identify itself before commencing the inspection, to state the subject, purpose and procedure of the inspection, and, if video or audio recordings are being made of the inspection, to disclose this fact. Even in the case of a covert inspection, the fact of the inspection is disclosed following the observation, thereby ensuring the inspected party's right to seek redress.

In the present case, the person conducting the inspection did not identify themselves before commencing the inspection, did not inform the complainant of the subject, purpose and procedure of the inspection, nor of the fact that video and audio recordings were being made of the inspection; furthermore, at the time the video recording was made, the complainant was not on duty, so a professional

inspection could not have taken place. According to the controller's statement, no professional inspection was carried out in relation to the complainant; rather, the controller stated that they had observed the complainant and made a video recording of him following a report of a criminal offence.

Pursuant to Section 42(1) of the Police Act, in connection with a police operation or the performance of official duties, visual recordings, audio recordings, or combined visual and audio recordings may be made of the person concerned by the operation, their surroundings, or circumstances and objects relevant to the police operation. In the present case, no police action was taken against the complainant at the time the video recording was made. At the time the video recording was made, no criminal or disciplinary proceedings were pending against the complainant.

The Inspection Service does not perform law enforcement tasks and has no authority to adjudicate on criminal complaints; consequently, it is not authorised to make video and audio recordings in this context.
On the basis of the above, the Authority found that the controller does not have an appropriate legal basis for the making and use of the video recording or for the processing of these personal data.

In addition to the video recording, the controller processed the complainant's criminal personal data arising from criminal proceedings, as well as the health-related personal data of the complainant's minor child in connection with this, in the disciplinary proceedings conducted against the complainant. Disciplinary proceedings are internal employer proceedings conducted against a member of the professional staff, the purpose of which is to establish that the person has become unfit for professional service. During disciplinary proceedings, the processing of personal data is not carried out for law enforcement purposes; therefore, the processing of personal data falls within the scope of the GDPR.

In the misconduct proceedings against the complainant, the controller disclosed the personal and criminal personal data arising from the criminal proceedings conducted by the public prosecutor's office and used in the unfitness proceedings, which formed the basis of the allegations against the complainant (the criminal offence that was the subject of the proceedings, the dates, manner and means of its commission, and the location), as well as the personal health data of the complainant's minor child to the person heard as a witness.

The Authority found that the disclosure of the personal and criminal personal data arising from the criminal case initiated by the Public Prosecutor's Office, to the witness heard during the misconduct proceedings which formed the basis of the allegations against the complainant, as well as the health-related personal data of his minor child, took place in the absence of an appropriate legal basis; this data transfer was not necessary for the performance of the task (conducting the disciplinary proceedings) carried out within the framework of the exercise of public authority vested in the controller; consequently, the controller infringed Article 6(1) of the GDPR.

The Authority called upon the controller to amend its practice regarding the hearing of witnesses during disciplinary proceedings, to inform the witness solely of the matter in which they are to be heard, to delete the unlawfully made video recording, and that, in connection with police professional inspections, the Inspection Service should make video and audio recordings in accordance with the provisions of the Inspection Regulations, and, in the event of a report of a criminal offence, should initiate proceedings with the competent investigating authority or public prosecutor's office. [NAIH-13678/2025]

II.1.6. Data processing in the private sector

1. Decision on data processing by the Bar Association

The petitioner approached the Authority requesting a finding that the data processing by the competent Bar Association was unlawful on the grounds that the petitionee had obtained judgments containing the petitioner's personal criminal data from the Debrecen Regional Court. The judgments were obtained because, approximately one month after the petitioner's admission to the Bar, the petitionee began to suspect that the petitioner was the person about whom it had been reported in the press some 10 years earlier that he had been convicted of criminal offences while practising as a lawyer. Following the procurement of the judgments, the petitionee's Executive Committee formally initiated proceedings against the petitioner, who was registered as a practising lawyer, on the grounds of unfitness for public trust at its meeting held in March 2024, and subsequently terminated the petitioner's membership of the Bar in May 2024 pursuant to Section 22(1)(f) of Act LXXVIII of 2017 on the professional activities of attorneys-at-law (hereinafter: the Attorney Act) (on the grounds of unfitness for public trust).

The petitioner complained that the petitionee had obtained the judgments containing his personal criminal data without his consent. He also pointed out that he did not even appear as a defendant in the judgments. The petitioner argued that, in his view, pursuant to Article 10 of the GDPR, the petitionee was not entitled to process his personal data relating to criminal matters at issue in the objection, as the processing of such data did not take place under the supervision of a public authority and is not permitted under either EU or Member State law. The petitioner explained that, in his view, pursuant to Section 146(3) and Section 175(3) of the Attorneys Act, a request for data may only be made to ascertain whether the petitioner has a clean criminal record, and the Bar Association is only entitled to consult the criminal records if the petitioner fails to prove that they have a clean criminal record. The petitioner claims that the case referred to in the judgments is the same case for which another court had previously found him guilty. He argued that, in relation to the offences he had committed, he had already been relieved of the adverse legal consequences associated with a criminal record, and therefore the petitionee should not have been able to obtain the judgments, as he was to be regarded as having a clean criminal record, which was also why he was admitted as a member of the petitionee's organisation in August 2023. The petitioner also referred to Constitutional Court Decision No. 144/2008. (26 November 2008), and concluded from this that if access to personal criminal data contained in the criminal records is unconstitutional following expungement, then the acquisition of such data held by the authority conducting the criminal proceedings, which were not included in the records in the first place, by other means could be regarded as even more so. He complained that he had objected to the processing of personal criminal data in the disciplinary proceedings before the Bar Council, and that the petitionee had rejected this objection. The petitionee cited Article 6(1)(e) of the GDPR as the legal basis for the processing of criminal personal data contained in the judgments, and applied the cases specified in Article 9(2)(d) and (g) of the GDPR to the data processing.

In the authority procedure for data protection before the Authority, a key issue was determining which date should be regarded as the start of the authority proceedings before the Bar that were pending at the time of the petition. If the judgments were obtained prior to the commencement of the Bar's authority proceedings, then the processing of criminal personal data cannot be considered lawful, as in this case the processing did not take place within the framework of the Bar's proceedings conducted by the petitionee in the exercise of its public authority. In determining the start date of the Bar's administrative proceedings pending before the petitionee, the Authority proceeded from the findings set out in the Curia's order No. Kf.II.37.183/2020/8 in this regard, according to which

“Pursuant to Section 104(3) of the Code on General Administrative Procedure, ex officio proceedings commence on the date on which the first procedural act is performed. Accordingly, despite the fact that the petitionee only decided ex officio to initiate the Bar’s disciplinary proceedings after obtaining the judgments in November 2023, it is to be regarded that the Bar’s disciplinary proceedings had already commenced prior to the obtaining of the judgments, when, in September 2023, the petitionee contacted the Szeged Bar Association pursuant to Section 25(1)(b) of the Code on General Administrative Procedure to request the petitioner’s disciplinary records, due to suspicions arising from press articles regarding the petitioner’s unfitness for the profession. This resulted in the processing of personal data relating to criminal convictions taking place whilst the Bar’s disciplinary proceedings were ongoing (the courts were contacted in November 2023, and the judgments were received in February 2024). This meant that the processing of the requested data was justified, as the processing of this personal data relating to criminal matters was necessary in the Bar’s disciplinary proceedings to establish that the petitioner was unfit to practise as a lawyer and that his membership of the Bar should therefore be terminated. The petitioner’s consent was not required for the data processing in question, as the legal basis was not Article 6(1)(a) of the GDPR. The data processing was necessary for the performance of a task carried out in the exercise of the petitionee’s public authority powers; its legal basis was therefore Article 6(1)(e) of the GDPR, and the lawfulness of the data processing was further established by Article 9(2)(d) and (g) of the GDPR. The petitionee also acted lawfully when it rejected the petitioner’s objection to the processing of his criminal personal data contained in the judgments, deeming it unfounded. The petitioner drew an erroneous conclusion from Constitutional Court Decision No. 144/2008. (26 November 2008). The cited decision actually refutes the petitioner’s position: “From the perspective of the right to work and to pursue an occupation, any provision relating to the person choosing the activity constitutes a subjective restriction on entry into the occupation in question and on the maintenance of the legal relationship. The constitutional right to the free choice of occupation does not preclude the relevant legislation from prescribing specific conditions and requirements for the pursuit of various activities.” Even after the exemption has taken effect, the petitionee may examine the background of an applicant for membership or an existing chamber member, including data and circumstances relating to any previous convictions. According to Section 98(1) of the Criminal Code: “Upon expungement – unless otherwise provided by law – the convicted person is exempt from the adverse legal consequences associated with a criminal record.” Under the Criminal Code, certain legal provisions impose further restrictions on persons classified as having a clean criminal record, depending on the type and severity of the offence

they have actually committed. Such cases are set out, for example, in Section 4(2)(c) of Act CLXII of 2011 on the legal status and remuneration of judges, and in Section 22(2)(f) of the Act on the Status of Public Servants. The Authority therefore rejected the Petitioner's requests. [NAIH-7680-2025]

2. Transfer of criminal personal data to the Hungarian Bar Association and the regional bar associations

The Authority conducted several data protection proceedings concerning the lawfulness of the transfer of Petitioners' criminal personal data to the Hungarian Bar Association and the regional bar associations.

In one case, the police station handling the case sent a notification regarding criminal proceedings initiated against the petitioner to the President of the Hungarian Bar Association (MÜK), who forwarded the notification to the president of the regional bar association competent to handle the case, whilst also informing the police station that the President of one of the regional bar associations was competent to act. The police station notified the secretary of the regional chamber. The information sent to the President of the MÜK and the secretary of the regional bar association contained the petitioner's personal details as well as his criminal record: his status as a suspect, the classification of the offence under the Criminal Code, and a summary of the facts established in the case.

In the other case, the Public Prosecutor's Office sent a notification to the President of the MÜK regarding criminal proceedings initiated against the petitioner in his capacity as a practising lawyer. As the legal basis, it referred to Section 140(2) of Act LXXVIII of 2017 on the on the professional activities of attorneys-at-law (hereinafter: Attorneys Act.) and Section 111 of Act XC of 2017 on the Code of Criminal Procedure (hereinafter: Code of Criminal Procedure) , and stated that the purpose of the data transfer was to inform the body authorised to initiate and conduct disciplinary proceedings against a person practising as a lawyer.

The Authority found that the provision of information to the president of the competent regional bar association regarding criminal proceedings initiated against a person practising the legal profession already falls within the scope of disciplinary responsibility of persons practising the legal profession. Therefore, this data processing operation (transfer) is not carried out for law enforcement purposes,

but for the purpose of fulfilling the legal obligation set out in Section 140(2) of the Attorneys Act, and falls within the scope of the GDPR.

The police station and the public prosecutor's office were also under a duty to inform the petitioner in connection with the criminal proceedings brought against him. However, pursuant to Section 140(2) of the Attorneys Act, this duty to provide information clearly and exclusively applies to the president of the regional bar association (and not even to the regional bar association itself), meaning that the legislation expressly requires the information to be provided to a specific official of the bar association.

Pursuant to Section 111 of the Code of Criminal Procedure, personal data may be transferred to the body authorised by law to process personal data and entitled to initiate and conduct disciplinary proceedings. The President of the MÜK had no authority to either initiate or conduct proceedings in relation to the petitioner's disciplinary case; consequently, he could not have been the addressee of the notification under Section 111 of the Code of Criminal Procedure.

In accordance with Section 140(2) of the Attorneys act and the principle of data minimisation, only the personal data necessary to identify the petitioner, the fact that criminal proceedings have been initiated against the petitioner, and the classification of the offence under the Criminal Code are relevant; all other personal data including a summary of the facts established in the case, are unnecessary for the purposes of data processing.

The police station and the public prosecutor's office forwarded the petitioner's personal data and criminal personal data to the President of the MÜK and the secretary of PVÜK (Pest County Bar Association) without a proper legal basis, thereby breaching Article 6(1) of the GDPR. Furthermore, in determining the content of the notifications forwarded by the police station, it breached the principle of data minimisation laid down in Article 5(1)(c) of the GDPR.

The Authority instructed the police station and the public prosecutor's office to amend their data processing practices so that data transfers are addressed to the president of the regional bar association, and that data processing complies with the principle of data minimisation. [NAIH-87/2025, NAIH-295/2025]

3. Data processing by forensic experts

The petitioner, a father, requested the Authority to initiate proceedings against the forensic psychologist acting as an expert, alleging a breach of his and his minor child's right of access to personal data generated during an expert examination.

During the proceedings brought against him to determine the exercise of parental custody, the petitioner, the father, submitted a request to the court-appointed expert psychologist and asked the expert to provide all data relating to him and his child collected during the examination, (including the complete psychodiagnostic data set, examination reports, drawings and audio recordings).

The petitionee responded to the data subject's request within the one-month time limit prescribed by law, but made the fulfilment of the request contingent upon the decision of the court that had appointed him; consequently, he did not send the requested data to the petitioner until that decision would be made.

The petitioner objected to the failure to comply with the request and asked the Authority to instruct the petitionee to comply with the data subject's request.

Act XXIX of 2016 on Forensic Experts (hereinafter: the Forensic Expert Act) defines the expert as the controller with regard to the expert opinion and the materials serving as the basis for its preparation. In the case under review, the petitionee is to be regarded as the controller, as the court order appointing the expert personally designated him to carry out the expert examination. The expert's data processing is specific in that it is based on the court or administrative order appointing the expert, and the expert is bound by this appointment.

Pursuant to Section 40(2) of the Forensic Expert Act, the expert is bound by a duty of confidentiality regarding the facts and data that come to his or her knowledge in the course of his or her activities; he or she may only provide information on the facts and data relating to the case to the authority, or to another body or person authorised to process the data; however, the data subject is entitled to a right of access but not to information regarding the data provided by them. The data subject is the owner of the data provided by them and may also grant an exemption from confidentiality; therefore, confidentiality cannot be interpreted as applying to them. Under their right of access, the data subject is entitled to request a copy of the data pursuant to Article 15(3) of the GDPR. The exercise of the data subject's rights may be restricted in accordance with Article 12(5) and

Article 15(4). Under Article 15(4), the right to request a copy must not adversely affect the rights and freedoms of others. Article 23(1)(i) of the General Data Protection Regulation allows Member States to introduce restrictions through legislation on the application of the provisions relating to the exercise of rights in order to protect the rights of the data subject or of others. Section 42(5) of the Forensic Expert Act may be regarded as a restriction corresponding to Article 23(1)(e) of the GDPR. Accordingly, the expert may only deny the data subject's right of access in justified cases, upon the instruction of the appointing authority or court, pursuant to Article 15(4) of the General Data Protection Regulation.

On the basis of the above, the petitionee applied to the court that had appointed him, which, in its order, informed the petitionee that the expert was not required to disclose to the parties any investigative materials going beyond the scope of the expert opinion. Accordingly, the petitionee, in accordance with Section 42(5) of the Forensic Expert Act, was justified in not complying with the petitioner's request for access. In light of the above, the Authority rejected the petitioner(s)' request.

However, the court's order regarding the disclosure of the investigation material applies only to 'the parties', that is, to the claimant and the petitioner as the defendant, but not to the minor petitioner. The Authority therefore had to examine whether the father, as the child's legal representative, was entitled to access the child's personal data.

The Authority's position is that in such cases – despite the fact that the court order may not have prohibited access – the expert, in their professional capacity as a controller, may nevertheless deem it necessary to restrict the right of access, having regard to the right to confidentiality. After all, in such cases, the findings of the investigation form the basis for the restriction of rights; the expert may observe during the investigation that the parent's knowledge of what the child has said is contrary to the child's best interests, and it is not always possible to stipulate this in advance in the court order.

In the case under consideration in the present proceedings, the expert in question stated during the authority procedure that the disclosure to the petitioner parent of personal data concerning the minor child generated during the expert examination would infringe the rights of the child concerned. Consequently, although the order of the appointing court decided only on the refusal to disclose the data to the parties – that is, the parents – the Authority took the view that the petitionee had lawfully restricted the petitioner parent's right of access exercised

as a legal representative due to the conflict of interest of legal representatives as set out in the Civil Code, and thus the Authority also rejected that part of the request which concerned instructing the petitionee to disclose data relating to the child. [NAIH-8100-3/2025]

II.1.7. Borderline authority and investigation procedures for data protection

In this sub-chapter, we summarise those investigation and authority cases in which there is a conflict between the fundamental right to the protection of personal data and two other fundamental rights – freedom of expression/freedom of the press and the right to informational self-determination – and, during the investigation of the cases, Recitals (4), (65) and (153) and Article 17(3) and Article 85 of the General Data Protection Regulation are at the centre of the assessment of the alleged infringement.

1. Borderline investigation cases

In one case, the complainant alleged that, at an event promoting the creation of an amusement park, the event organiser had displayed posters and photo booths featuring the complainant's photograph alongside an offensive caption, in which the complainant was recognisable and identifiable, and that the complainant's name had been published in a newspaper article, thus, his personal data, name and photograph were processed and used without his consent. According to the complainant, his personal data were misused, his character was discredited, his honour was violated, his reputation was damaged, hatred was incited against him, and he was subjected to ridicule, unfounded criticism and disparaging remarks in full public view. The event organiser did not respond to the complainant's letter of protest; it stated that it had no knowledge of the purpose or duration of the images' use, where they were stored, or whether any records were kept of the photographs taken of the complainant. In the complainant's view, the purpose of the event was to incite hatred against him, as he had contributed to the failure of the theme park project. The Authority launched an investigation into the disclosure of personal data, the placement of his likeness and caricature on posters and at a photo booth, and their display at the event. The controller defined the purpose of the data processing as seeking to persuade the data subjects, with the involvement of the public, not to hinder development and not to deprive young people of the promoted experiences. The Authority was unable to accept the controller's statement and found a lack of a legitimate purpose for the data processing, constituting a breach of Article 5(1)(b) of the GDPR. With regard to the legal basis, the controller argued that it had

processed the complainant's personal data on the basis of the right to freedom of expression and information, as set out in Article 17. Freedom of expression primarily protects the expression of opinions on matters of public interest. In the specific case, the data subjects were activists from a local civil society organisation who, by championing local issues, brought them to the attention of the public, sparking significant public interest and debate on both sides of the argument; thus, the data subject could even have been classified as a public figure. However, in the Authority's view, the mere fact that the data subject could have been classified as a public figure did not justify the sharing of his image with the public, since in the absence of an appropriate legal basis, the existence of public debate – an essential conceptual element of the legitimate interest legal basis – and the associated balancing of interests are irrelevant. The Authority found that there was a lack of an appropriate legal basis for the data processing, constituting a breach of Article 6(1) of the GDPR. During the data processing, the controller obtained the complainant's personal data and image not from the data subject but from Facebook; therefore, the controller was subject to the prior information obligation set out in Article 14 of the GDPR. As the data subject was not informed in advance, the Authority found a breach of Article 14 of the GDPR. The event organiser, as the controller, failed to fulfil its obligation to provide information upon the data subject's request, as set out in Article 12(3) of the GDPR; the Authority therefore found a breach of Article 12(3) of the GDPR. On this basis, the Authority did not find the data processing to be lawful overall. In view of all this – and with particular regard to the fact that, according to its statement, all three posters had been destroyed – the Authority called upon the controller to comply without delay with the data subject's request submitted pursuant to Article 12(3) of the GDPR, and to ensure that its communications are displayed in accordance with the provisions of the legislation in future. The controller downloaded the Authority's request sent electronically but did not respond to it, nor did it comply with the request, thereby failing to fulfil its obligation to cooperate with and provide information to the Authority under Section 54(1)(a) and (c) of the Privacy Act. In view of this, the Authority issued a report. On the basis of the Authority's information, the complainant brought a privacy lawsuit, as a result of which the court found that the event organiser had infringed the privacy rights of three representatives of the civil society organisation and ordered the defendant to pay compensation for non-pecuniary damage. [NAIH-2397/2025., https://naih.hu/files/infoszab_jelentes_naih-2397-1-2025.pdf]

In another data protection investigation case involving a border area, several complainants from a small village approached the Authority because photos of contracts concluded by the previous local government had appeared in an offi-

cial newsletter published by the local authority and distributed free of charge to all households in the village, as well as on the mayor's Facebook page, in such a way that the personal data of the complainants (contracting parties, witnesses, local government employees) were displayed without being redacted. In the information provided to the Authority following repeated requests, the mayor argued that prior to taking office, in September 2024, on the former mayor's last day in office, several questionable contracts had been concluded, the circumstances of which had also been a matter of public concern, and requests for information of public interest had been received by the local authority in relation to them. In his letter, the mayor stated that he had disclosed these documents partly to comply with this request and partly to ensure the transparency of the institution's operations. In its opinion, the Authority explained that, with regard to personal data accessible on the grounds of public interest, it is important to distinguish that, although the rules governing access to data of public interest must be applied to their disclosure pursuant to the second clause of Section 28(1) of the Privacy Act, the personal nature of such data remains intact despite their public nature; therefore, the most important guarantee of data protection—the requirement of the principle of purpose limitation, which is expressly laid down in Section 26(2) of the Privacy Act—must be fully observed. Anyone may access data of public interest or data accessible on the grounds of public interest, but even when disseminating personal data falling within this category, the requirements arising from the principle of purpose limitation set out in Article 5(1)(b) of the GDPR must be observed; the data processing (and disclosure) carried out by the mayor did not comply with this, during which the data subjects' personal data were 'put on public display' in the local newspaper and on a social media page, meaning they became accessible to anyone. The Authority therefore called upon the mayor to remove the data content objected to by the complainants from his Facebook page, and, in accordance with the statutory provisions, to comply with requests for data of public interest relating to the case by sending documents containing personal data that are in the public interest – with any data requiring protection redacted so that it cannot be identified by the person requesting the data, to the email address provided by him. In his reply, the mayor welcomed the Authority's detailed information and complied with the request. [NAIH-6923/2025.]

2. Borderline authority cases

In his petition, the petitioner stated that in a post published on a page created on Facebook (hereinafter: the Page), the group administrator was discussing him. In his view, the Page had infringed his rights relating to the protection of his per-

sonal data, in particular his special categories of personal data; it had processed such data without a proper legal basis; and that its data processing does not comply with the requirements of fairness and lawfulness. He explained that the question of whether criminal proceedings are pending against him, as well as the possible outcome of such proceedings, constitutes criminal personal data. The Website processed his name and other information relating to him, including a photograph taken of him, which constitute personal data, without justification and without a legal basis or a legitimate, lawful purpose for data processing. The Authority rejected the petition for the following reasons:
In this case, the function and purpose of the social media page is to inform the local population about public affairs, and the purpose of the post in question was specifically to present a local public matter to the population. In relation to the subject matter set out in the post in question – which is why the petitioner's name arose – the Authority identified the following public affairs issue at local level: it is of particular importance that, in a given municipality, the staff of local leaders and those municipal employees who assist the public with personal matters hold a certificate of good conduct. Possession of a certificate of good conduct is defined as a mandatory requirement by Section 39(1)(a) of Act CXCIX of 2011 on Public Service Officials and Section 44/A(4) of Act I of 2012 on the Labour Code. The content of the contested entry does not merely address whether the office staff hold a certificate of good conduct, but the petitionee also expresses an opinion as to which person(s) may have been identified as having a criminal record, and therefore do not hold a clean official certificate of good conduct, which is why the requested data of public interest were not provided. Beyond the identification of the petitioner, the public issue raised by the petitionee concerns accountability and transparency, in relation to which the legitimate interest of the municipality's population requires that citizens have knowledge as to whether immediate colleagues who enjoy the trust of the municipality's leader – such as the petitioner – have a clean criminal record. [NAIH-2258-12/2025.]

II.1.8. Recommendations, statements and reports issued by the Authority

1. Recommendation on ensuring access to medical records generated during the provision of paediatric care

In recent times, several notifications with related content have been received in which minors (acting through the same legal representative) have complained that their paediatrician refused to release their medical records, failed to respond to their request, or took no action in response to the request. In his letters to the paediatricians, the legal representative stated in every case that the copies were

intended for use in a vaccination exemption procedure, and in most cases set a five-day deadline for compliance. During its examination of the documents attached to the reports, the Authority found that, in connection with requests for the release of documentation, the actions taken by paediatricians in several cases were not in accordance with the provisions of the GDPR regarding the exercise of data subjects' rights; and therefore published a recommendation at the end of 2025 to promote the development of uniform, lawful data processing practices within the primary healthcare system.

In the recommendation, the Authority drew attention to the fact that information relating to a child's state of health, examinations and treatment constitutes health data, which falls within the special category of personal data. The controller must comply with the data subject's request to exercise their rights; in this case, these conditions are met by the child's GP, who provides healthcare services to the child and records, registers and retains the resulting medical documentation. In the case of a data subject who is a minor, the data subject exercises the rights guaranteed by the GDPR through their legal representative.

Under the right of access, the data subject is entitled to receive a copy of the complete set of personal data processed about them (the first copy free of charge). If the data subject submits the request electronically, the controller is obliged to make the information available in a widely used electronic format, unless the data subject requests otherwise. It is also important to emphasise that the right to request a copy must not adversely affect the rights and freedoms of others; therefore, doctors must ensure that documentation is released in such a way that the data of third parties is not disclosed without authorisation.

It should be emphasised that, in the case of medical records, the data subject is not required to justify the purpose for which they are requesting the release of their personal data, and the controller has no right to examine the data subject's intentions or to consider whether to comply with the request on that basis. Although in the cases examined the petitioners state that they are requesting the release of medical records for the purpose of a vaccination exemption procedure, this does not constitute a lawful ground for refusal in the present case – even if the intended use is contrary to the treating doctor's personal judgement. The controller may refuse to act on the data subject's request if the request is manifestly unfounded or – particularly due to its repetitive nature – excessive. However, even in this case, the controller must inform the data subject without delay, and at the latest within one month of receiving the request, of the reasons for the failure to act, as well as of the data subject's right to lodge a complaint

with a supervisory authority and to seek judicial remedy. The five-day deadline for compliance usually set by the legal representative in requests is therefore irrelevant, as the GDPR sets the deadline for complying with the data subject's request, and the deadline for taking action following the request, at one month.

Finally, the Authority emphasises that compliance with the GDPR is not sufficient; in accordance with the principle of accountability, it must also be demonstrated to the Authority.

2. Position statement for organisers of children's camps regarding the obligation for parents to present a special official certificate of good conduct

Under the legislative amendments introduced by Act XXX of 2024 on the Protection of Children, organisers of children's camps are required, from 1 January 2025, to ensure that only those persons can supervise children who, by presenting an official certificate of good conduct with the appropriate content, prove that they are not registered in the criminal records for offences committed against minors and are not subject to criminal proceedings, disqualification from a profession, or compulsory medical treatment. The legislator has stipulated that camp organisers must verify, through the presentation of this special certificate of good conduct, that no person who fails to meet the statutory criteria participates in the implementation of the camp. In 2025, several submissions were received from parents indicating that, in practice, differing interpretations had emerged regarding the scope of persons considered to be involved in child supervision and the related controller obligations. One report concerned a case in which organisers planned to collect the certificates of good conduct of those involved in the organisation simply by email and intended to store copies of them in order to demonstrate compliance with the new requirements.

The Authority issued a position statement to support the development of lawful data processing practices, setting out the specific rules applicable to camp organisation. Section 4/B of Act XI of 1991 on Health Authority and Administrative Activities defines the verification process, which primarily requires the person wishing to participate in the organisation or implementation of a camp to present an official certificate of good conduct to the camp organiser. The organiser records the fact of this presentation in a declaration containing the identification data of the natural person concerned, which must be retained for three years following the camp.
The Authority first noted that, during the organisation and operation of the camp, organisers qualify as controllers under the GDPR, and that the personal data

contained in the certificates of good conduct required for the verification process constitute criminal personal data. The law governing the verification process provides only for an obligation to present the certificate for subsequent inspection, and the practice of making and storing copies is contrary to the GDPR's principle of data minimisation. At the same time, the organiser is permitted – and the implementation of the legislator's intent also justifies – to verify the authenticity of the official certificate of good conduct on the designated website and to record the fact and date of such verification in its own records (or even on the declaration itself).

Regarding the determination of the group of persons involved in camp activities who may be required to present the certificate, the Authority drew attention to the provisions of Decree 6/2025 (II.25.) of the Ministry of the Interior on the conditions of children's camps, which precisely defines who qualifies as a person involved. Thus, although parents visiting the camp may come into direct contact with the children, if they are not in a legal relationship with the camp organiser for performing activities related to the organisation or implementation of the camp, they are not subject to any statutory obligation that would require them to present an official certificate of good conduct. Consequently, the camp organiser has no legal basis for processing the parents' criminal personal data.

Finally, the Authority explained that, in order to comply with the principles of accountability and transparency, it is necessary for organisers to inform the data subjects in advance, in an easily accessible manner and using clear, understandable language, of the information required under Articles 13–14 of the GDPR. [NAIH-10404-5/2025]

3. Position statement regarding the recording of calls to local government customer service

A local government requested the Authority's position on the preliminary assessment of the customer service call centre it intended to introduce. According to the submission, the municipality planned to automatically record all telephone calls received on its central phone number, primarily for quality assurance purposes.

Under Section 18(4) of Act CIII of 2023 on the Digital State and Certain Rules for the Provision of Digital Services (hereinafter: the Digital State Act): "The organisation providing the digital service — independently or in cooperation with other organisations providing digital services — shall operate a customer service that is accessible by telephone and by other electronic means, in accordance with

the rules of the Act on Consumer Protection applicable to enterprises carrying out public service activities, with the deviation that the customer service must be available for at least 40 hours per week." The Authority also pointed out that, under Section 17/B(3) of Act CLV of 1997 on Consumer Protection (hereinafter: Consumer Protection Act): "All oral complaints made by telephone to the customer service, as well as the telephone communication between the customer service and the consumer, must be recorded. (…)."

In view of the above, the Authority drew the municipality's attention to the fact that, as an organisation providing a digital service, it is required to record the communication between customer service and the client by means of audio recording, in accordance with the consumer protection rules applicable to enterprises performing public service activities. For the purposes set out in the above provisions of the Digital State Act and the Consumer Protection Act, the data processing operation concerned (recording) may be based on Article 6(1)(e) of the GDPR as the legal basis necessary for the performance of a task carried out in the public interest. If, during a call received by the municipality, special categories of personal data are disclosed inadvertently, the Authority considers it good practice for the privacy notice, under the legal basis of processing, to also include references to Article 9(2)(f) and (g) of the GDPR. To promote proper information for data subjects, the Authority further recommended placing a detailed privacy notice in a separate menu item, in addition to the sample text of the automatic first-level notice played immediately before the call, and encouraged publishing the privacy notice on the municipality's website on the page used to display the telephone menu system.
[NAIH-10731/2025]

4. The enforcement of the right to erasure in the course of processing by political parties and media content providers

In 2025, the European Data Protection Board (hereinafter: EDPB) examined the enforcement of the right to erasure as set forth in the General Data Protection Regulation by controllers in relation to the Coordinated Enforcement Framework (CEF).
The Authority also participated in the work within CEF and wished to survey the practice of a segment of the business sector related to ensuring the right to erasure according to the GDPR, using a common questionnaire compiled by the experts of the supervisory authorities. (This report is presented in detail under IV.7.2. Coordinated action by the supervisory authorities.)

Starting out from, but independently of the CEF survey, the Authority reviewed the practices, the current state and tendencies in two additional sectors of domestic data protection law enforcement in Hungary through a questionnaire-based survey.
One of the focus groups of the survey concentrated on online media content provision; within this, the survey focused on the practice of 10 content providers relating to 12 websites with regard to erasure and the right to be forgotten. The other group of the survey included political parties: the data processing practices of 14 political parties regarding erasure were reviewed through the questionnaire.

Acting within its responsibilities set forth in GDPR Article 57(1)(a), (b), (d) and (i), the Authority's objective in assessing the answers to the questionnaire was to receive a comprehensive overview of how the right to erasure, as a data subject right, is enforced in Hungary. The Authority summarised the experiences of the surveys in reports published on its website.
Based on the responses sent by political parties and media content providers, the report presents the practice of the application of the law by Hungarian controllers in a summarised manner and in extracts. The purpose of the reports is the presentation of good practices, the formulation of recommendations for content providers and political parties as controllers, and to provide a status assessment for the public in relation to the right of erasure. (https://naih.hu/adatvedelmi-jelentesek)

II.1.9. Authority inspections

In 2025, in accordance with its inspection plan, the Authority carried out authority inspections of 21 online shops regarding the adequacy of the general data processing information provided on their websites.

Clear and recurring patterns emerged during the inspections: for a significant proportion of the controllers operating the online shops, the data processing information was fragmented, contradictory and difficult for users to understand, both in terms of content and form. A frequent problem was the use of outdated, template-like information texts copied from other websites, which did not describe the actual data processing procedures but reflected an approach aimed at the superficial, documentation-centred fulfilment of data protection compliance. In some cases, the privacy notice was not simply difficult to find on the website; indeed, access to it was technically obstructed, as the website would only jump to product offers despite continuous scrolling. In a significant number of privacy

notices, the Privacy Act was still cited as the applicable legislation instead of the GDPR.
Taken together, the shortcomings identified suggested that the majority of the companies operating the online shops examined lacked adequate data protection expertise regarding the drafting of privacy notices, and had not meaningfully integrated data protection compliance into their operations.

II.2. Cases relating to the processing of personal data for law enforcement, defence and national security purposes (data processing operations falling within the scope of the Privacy Act)

1. The lawfulness of the processing of data relating to housing support provided by the armed forces, which forms part of the records of a national defence administrative organ

In a data protection authority procedure, the Authority examined the lawfulness of data processing by a defence administration organ (hereinafter: the Controller) in connection with the register of housing support provided by the armed forces. The petitioner objected to the photographing of the meter readings for his service accommodation, contested the legal basis for their processing, and complained that he had not been informed of this data processing beforehand.

A decision was taken to sell certain properties managed by the Ministry of Defence to eligible parties. To implement this, the controller prepared the documents required for the sale process, including a privacy notice; having read this, the petitioner expressed an intention to purchase the service flat they were renting. As part of the flat disposal procedure, the controller carried out inspections and took photographs of the service flat's meters.

The Authority found that, pursuant to Section 137(2)(d) of Act CCV of 2012 on the Legal Status of Servicemen (hereinafter: Servicemen Act) , the option to purchase the service flat constitutes housing support; furthermore, pursuant to the provisions of the Act on the Data Processing for Defence Purposes (hereinafter: Act on Processing for Defence) and the Privacy Act, the processing of data relating to the registration of housing support constitutes data processing for defence purposes.

The photograph taken of the meter – as it relates to the property rented by the petitioner, and thus constitutes information concerning the petitioner – is considered to be the petitioner's personal data.

The processing of meter data and photographs took place within the scope of the housing benefit register; the legal basis is Section 5(1)(a) of the Privacy Act and Section 24/J of the Act on Processing for Defence, as well as Section 75 of the new Act on Processing for Defence, the purpose of data processing is to review eligibility for housing support.

Data processing in connection with the inspections, including the taking of photographs, did not infringe the data processing principles set out in Section 4(1), (2) and (5) of the Privacy Act; the inspection of housing benefits as a data processing purpose is lawful. The processing of meter readings is essential for the fulfilment of the purpose of reviewing eligibility for housing benefit, and is suitable for this purpose as it contains information regarding the use or non-use of the rented property.

However, the Authority found that between 1 January 2012 and 28 April 2019, the petitionee failed to fulfil its obligation to facilitate the exercise of the right to prior information. Furthermore, the privacy notice drawn up in 2019 did not comply with the statutory provisions, thereby infringing the petitioner's right to prior information. [NAIH-1315/2025., NAIH-2118/2026]

2. Data processing by the Hungarian Defence Forces concerning health data

An investigation has been launched into a case involving a data processor in the Hungarian Armed Forces. The complainant was a contract soldier who had undergone a drug test. A rapid test performed on the so-called A sample taken from him yielded a positive result, so the sample was sent for laboratory testing by the competent body of the Hungarian Armed Forces (hereinafter: Data Controller), which also came back positive. The B sample taken was not used. Following the test, the Data Controller continued to process the samples together with the personal data contained in the documentation related to the test.

The complainant contacted the controller on several occasions with questions regarding the processing of his personal data and to request copies of such data. The controller responded to the written requests during the Authority's proceedings. The Authority examined the compliance of the personal data processing and the issue of fulfilling the request for access.

The controller processed data for national defence purposes in this case, to which the provisions of the Privacy Act apply, not those of the GDPR.

The relevant provisions of the Act on Data Processing for Defence Purposes define the scope of the data processed and the persons authorized to process it, as well as the retention period for the documentation. The data controller processes certain personal data of personnel for the purpose of verifying their fitness for duty or work, as well as for conducting screening tests aimed at maintaining and enhancing military discipline and security. This includes samples taken during screening tests, such as observed, examined, measured, imaged, or derived health data.

However, the relevant provisions do not address the retention period for collected samples as health data or special categories of personal data. The retention period for some of these samples is governed by an administrative order: if Sample A tests positive, the controller retains it for 3 months. This order also does not contain any provisions regarding the retention period for Sample “B”. In cases of mandatory data processing, the types of data to be processed, the purpose and conditions of data processing, access to the data, the identity of the controller, and the duration of data processing or periodic review of its necessity must be determined by the law or municipal ordinance mandating the data processing. However, the controller also extended the 3-month retention period specified in Sample A’s administrative order.

Exercising the right of access does not entail the obligation to provide the sample or the resulting documents, but rather the obligation to disclose the information specified by law; there is no legal obligation to provide the sample.

The Authority determined that, since the Data Controller extended the retention period for Sample A – in the absence of a statutory provision – and since the retention period for Sample B is not specified by law, the retention period must be reviewed every three years. It also found that the controller provided the complainant with information regarding the processing of their personal data beyond the timeframe specified in the Privacy Act.

The Authority called on the controller to rectify its unlawful practices and, at the same time, recommended that the Ministry of Defence establish statutory regulations governing the retention period for samples. The Ministry of Defence accepted the recommendation, and the controller also indicated that it would ini-

tiate the process of establishing statutory regulations governing the retention period.. [NAIH-7546/2025]

3. Reference to the disclosure of documents made during criminal proceedings when exercising the right of access

In its response to the data subject's request for access to their personal data, the investigating authority did not disclose the recipients of the data transfers, nor did it specify the purpose or legal basis for these transfers. It considered this to be lawful on the grounds that these bodies and individuals would become known to the petitioner during the inspection of documents, and therefore a detailed list of them was unnecessary when fulfilling the request submitted under the right of access.

The Authority emphasised that access to documents under the Code of Criminal Procedure is independent of the institution of the exercise of rights by data subjects under the Privacy Act. The suspect is entitled, in accordance with the rules on access to documents set out in the Code of Criminal Procedure, to inspect the case files generated during the proceedings; the purpose of this is to enable the person entitled to inspect the documents and evidence generated during the proceedings, on the basis of which they may exercise their rights during the criminal proceedings. Furthermore, when exercising their right of access under Section 14(b) of the Privacy Act, the data subject may request information as to whether the controller is processing their personal data; if so, they may request that the information set out in Section 17(2) of the Privacy Act be made available to them. On this basis, they can ascertain whether the processing of their personal data is lawful. The provision of access to documents under the Code of Criminal Procedure does not exempt the controller from the obligation to ensure the right of access under Section 14(b) of the Privacy Act. Although there are similarities in the content of the two types of information, they do not fully overlap; they have different roles and specific information content.

The Authority found that the investigating authority breached Section 17(2)(b) and (d) of the Privacy Act because it failed to inform the petitioner of the purpose and legal basis of the data transfers, as well as the recipients of the data transfers. [NAIH-120/2025]

4. Data processing at the Csenger National Penitentiary

The Authority has launched a comprehensive investigation to review the data processing practices of penal institutions, the electronic records used by these organs, the data processing operations carried out therein, and their practices regarding the enforcement of data subjects' rights, taking into account new data processing methods and technologies to be introduced in the future. As part of the above comprehensive investigation, the Authority also examined the data processing activities of Hungary's penal institutions equipped with smart devices and artificial intelligence systems, the Csengeri National Penitentiary (hereinafter: the Institution), during which, on the occasion of the on-site inspection, it familiarised itself with and reviewed the data processing carried out using the new technologies and devices employed at the Institution.

As a tool involving new data processing procedures, the Institute has introduced the monitoring of staff and prisoners using wristbands fitted with transmitters. The wristband serves as a secondary identifier for both inmates and staff, and is equipped with an emergency alarm and location tracking function. Its primary purpose is to protect life and physical safety. The wristband monitors heart rate and alerts staff if readings fall outside a medically acceptable range. The alert does not contain any health data.

A camera system equipped with facial recognition software has been installed at the Institute, serving as the primary means of identification for staff and detainees. The system ensures that the movements of detainees within the building can be tracked. The artificial intelligence software of the cameras installed in the corridors and certain special cells is capable of identifying certain movements in addition to facial recognition (behavioural analytics smart camera system). The camera system analyses behaviour (e.g. climbing walls, fighting, lying on the floor) and sends an alert to staff if it is classified as deviant. Following the automated data processing procedure, and after the alert has been verified, the decision on whether any action is required is always made by the staff. Since their installation, the above camera systems have functioned flawlessly, without any false positives or alerts. The facial recognition system does not store the facial images themselves, but rather facial templates extracted from photographs; that is, it processes image data and compares this with the photographic data stored in the officially recognised FŐNIX system.

The legal basis for the data processing carried out using the aforementioned new technologies is provided by the provisions of Sections 150(4a) and (4b) of the Penitentiary Act, which came into force on 1 August 2024.

The administration of prisoners is aided by so-called KIOSK devices placed in the cells, through which prisoners can submit requests to the prison management, receive information on the planned daily schedule, medical examination dates, financial balances, etc., and can access information notices relating to specific data processing activities carried out by the institution (e.g. the information notice on data processing via the wristband). The KIOSK device can be used by the prisoner following two-factor authentication (wristband and facial recognition or PIN code).

The Institute holds data protection training for staff twice a year – in a documented manner – and new recruits receive separate training. From 1 January 2026, data protection training for staff will be delivered via a dedicated system. [NAIH - 10326/2025]

II.3. Reporting of data breaches

In 2025, the Authority received 682 new data breach reports, representing an increase compared to previous years. Controllers continue to report the majority of incidents via the data breach reporting system available on the Authority's website, which is specifically designed for this purpose; more than half of the incidents (368) were reported via this platform.

II.3.1. Significant data breaches falling within the scope of the General Data Protection Regulation

1. Data breach at a government office

The controller's employment department sent an email regarding job offers to jobseekers. A controller's administrator drafted the email and attached a list of clients to be contacted in an Excel spreadsheet. The attachment contained the details (name, social security number, MASZ number, address, start date of registration in the specialist system, educational qualifications, email address) of the jobseekers who had an email address. The following day, they began sending out the emails, but due to an oversight, the Excel spreadsheet containing the details of the email recipients remained in the sent message, and approximately seven hundred people received this email. The controller detected the data breach on the same day and informed the data subjects of the data breach on

the same day, asking them to delete the message. The controller also reported the data breach to the Authority.

In this case, the data breach arose because the controller had failed to implement appropriate technical and organisational measures to ensure the confidentiality of personal data relating to job applications. The inclusion of the Excel spreadsheet containing job seekers' data as an attachment should have been detected, and, fundamentally, work processes must be established to ensure that such carelessness cannot result in the disclosure of data.

The data set in the spreadsheet was extensive, making each data subject individually identifiable; sharing such data with third parties without appropriate security measures poses high risks to the data subjects' privacy. A factor increasing the risks was that the Excel spreadsheet containing the data subjects' data was not protected by any access controls or encryption. The handling of a large volume of data, combined with the circumstances of the incident, resulted, in the Authority's view, in a high-risk data breach.

Following the incident, the controller incorporated a provision into its IT policies stipulating that when generating spreadsheets containing personal data, only those data strictly necessary for the task may appear in the exported spreadsheet (e.g. an email address is sufficient for a non-personalised newsletter). Once the task has been completed, the tables must be deleted, and tables containing personal data may only be saved in a password-protected file. Furthermore, before sending, it must always be checked that the message contains only the prepared document, approved by the manager, as an attachment.

The Authority found a breach of Article 32(1)(a) and (b) and Article 32(2) of the GDPR, and imposed a data protection fine of two million forints on the client.

In similar cases, the Authority considers it good practice for the controller to carry out such activities using a dedicated newsletter distribution service. When subscribing to the newsletter, the data of subscribers may be automatically recorded in the service's database, and these data may be used when sending out newsletters without having to manually copy the recipients' details from an Excel spreadsheet. [NAIH-8429/2025]

2. Data breach at a headhunting firm

The Authority learned from the press that the controller's database had been publicly accessible for some time, containing thousands of personal data records. Subsequently, the controller also reported the data protection incident. The controller originally stored the personal data under its control on its own server, but commissioned an external developer, the processor, to develop an enterprise management system, which it now operates not on its own server but on a server located at an external third-party service provider. The processor wrote the code in its GitHub repository, which it made public for some reason. The processor uploaded the completed system with personal data, which it had requested from the controller. However, the processor uploaded these data not only to the controller's system but also to its own public GitHub repository. The controller was unaware of the above events.

The data leaked in the data breach were the data sent in March 2023 as described above; therefore, no data leaked from the controller's operational system. In this incident, the personal data of approximately 6,000 individuals were made public (name, email address, telephone number, LinkedIn profile, language skills and work experience).

Based on the above, the breach of confidentiality in the data processing operation fell within the processor's sphere of responsibility, as it was entrusted with the IT implementation of the operation in accordance with the clients' statements and the attached contract. In the Authority's view, the controller was able to demonstrate that the data security deficiencies did not arise within its sphere of responsibility; at the same time, the Authority found that the processor infringed Article 32(1)(b) and (2) of the General Data Protection Regulation by carrying out the data processing operations entrusted to it without adequate data security measures. A data protection fine of HUF 700,000 was imposed on the data processor.

The Authority established the controller's liability on the grounds that, in accordance with the principle of data protection by design and by default set out in the GDPR, in the case of implementing a more complex information technology process involving the processing of a large volume of personal data, it could have exercised greater care and diligence in selecting a processor with the appropriate expertise. Furthermore, in addition to the general data security obligations, and with particular regard to the database containing a large volume of personal data, the controller should have included more detailed rules in the data process-

ing agreement concerning the operation most vulnerable in terms of personal data, namely data transfer.

On the basis of the above, the Authority found that the controller had failed to comply with its obligation arising from the principle of data protection by design and by default set out in Article 25(1) and (2) of the GDPR; therefore, the Authority imposed a data protection fine of HUF 1,500,000 on the controller. [NAIH-899/2025]

3. Data security issues during the migration of a customer database by a processor

The Authority initiated an authority procedure for data protection ex officio to investigate a data breach that occurred during the migration of an IT system affecting the personal data of a large number of users. The case was based on a data breach reported by the controller, during which an unauthorised external attacker gained unauthorised access to a database containing the personal data of more than 900,000 users of the service.

According to the findings, the controller had commissioned an IT service provider, acting as processor, to migrate the database it managed from one server hosting provider to another. During the migration, the server was restarted; however, the processor failed to verify that the firewall and network settings applied would continue to provide adequate protection against unauthorised access following the restart. As a result, the system's firewall settings reverted to the default configuration, which allowed all external traffic, whilst the network connection of the application in question was configured in such a way that the service was also accessible from the internet. The security breach persisted for several days, during which time an external attacker gained unauthorised access to the database and retrieved personal data from it. Neither the controller nor the processor detected the attack or the vulnerability; it was the attacker who notified the controller of the breach, alongside a demand for a ransom payment.

The Authority's investigation also covered an assessment of the legal status and scope of responsibility of the controller and the processor. According to the findings, following the discovery of the breach, the controller fulfilled its obligations under Articles 33 and 34 of the GDPR, reported the data breach to the Authority within the prescribed time limit, and informed the data subjects appropriately. In contrast, the Authority found that the processor had failed to implement the technical and organisational measures required by Article 32(1) and (2) of the GDPR,

proportionate to the risks, and had failed to ensure the ongoing confidentiality of the systems used for the processing of personal data.

The Authority considered it an aggravating circumstance that the migration affected the personal data of a large number of data subjects, including data that could give rise to identity theft. As a result of the proceedings, the Authority found that the processor entrusted with the database migration, and responsible for implementing the technical configurations, had breached Article 32(1)(b) and (2) of the GDPR, as it had carried out the data processing operations entrusted to it without adequate data security measures. The Authority imposed a data protection fine of 2,000,000 forints on the processor, whilst it discontinued the proceedings in respect of the controller.

The case highlights that data processors also bear independent responsibility for the adequacy of the data security measures applied during the data processing operations entrusted to them, and that, particularly in the case of high-risk data processing operations, continuous monitoring and documented control of security settings is essential, including a review following the restart of the IT systems used. [NAIH-7395-6/2025]

4. Data breach concerning the TISZA VILÁG application

Based on press reports and notifications in the public interest, the Authority launched an authority investigation against the Tisztelet és Szabadság Párt (Respect and Freedom Party – Tisza) concerning the implementation of obligations set forth in GDPR Articles 25 and 32-34 in relation to data processing by the Tisza Világ application on 7 October 2025. Based on the facts of the case found in the course of the authority investigation, the data breach notification made by the Client on 8 October 2025 and the press reports published in the meantime, the Authority closed the authority investigation on 11 November 2025 and, at the same time, launched an authority procedure for data protection ex officio against the Client based on Section 60(1) of the Privacy Act. This authority procedure is still in progress at the time of closing the report. (More about the Authority's measures taken in relation to the databases of the Tisza Party in II.1.3. Politics related cases.)

II.3.2. Data breaches falling within the scope of the Privacy Act

1. Data breach during a data request in criminal proceedings

A police station (hereinafter: controller) issued a request to a limited liability company (Kft.) during criminal proceedings, which the controller, in view of the urgent nature of the case, sent from one of its official email addresses to the email addresses support@.....com and ugyfelszolgalat@naih.hu, the addressee of the request being the managing director of the limited liability company. The Authority initiated an authority procedure for data protection ex officio in connection with the data breach that occurred as a result of the delivery of the request – containing personal and criminal personal data – to the email address support@.....com.

In connection with the email request sent to the email address support@....com, the Authority drew the controller's attention to its obligation to assess the risk associated with the data breach on two occasions and to report it to the Authority. Despite this reminder, the controller did not report the data breach. It did not consider it to be high-risk, did not identify any consequences that would significantly affect the exercise of fundamental rights, and did not inform the data subjects during the handling of the data breach.

The investigation revealed that messages received in the support@...com email account are first routed to the company's general customer service system, to which, according to the company, 5,087 employees and other contracted staff worldwide had access at the time of the incident. In this case, three individuals gained access to the criminal personal data contained in the email; however, it can be established that, as a result of the email being sent to the support@... com, more than 5,000 people who were not authorised to access the data gained access to it, and that persons (customer service staff) who, given their roles, were not authorised to respond to the police enquiry or to view its contents, actually became aware of it. The Authority therefore classified the data breach as high risk.

According to the controller's statement, sending the information via email is not standard practice; in this instance, it was chosen due to a temporary fault in the system used to send the information through the company portal. Nevertheless, the Authority found that the controller had breached the statutory provisions governing the handling of data breaches, as it had incorrectly failed to classify the

data breach as high-risk, had not reported it to the Authority, and had not informed the data subjects.

During the investigation of the same data breach, the Authority also examined the lawfulness of the data transfer involving the disclosure of personal and criminal personal data contained in the request. In a request under Section 261 of the Code of Criminal Procedure, pursuant to paragraph (5), the conditions and purpose of the data request, the data necessary for the provision of the information and for identifying the subject matter of the data provision, as well as the scope of the data to be provided and the method and deadline for the provision of the data must be specified. Only the transfer of such data may be considered lawful.

Sections 4(1) and (2) of the Privacy Act, meanwhile, establish as a fundamental principle that personal data may be processed solely for clearly defined, lawful purposes, for the exercise of a right or the fulfilment of an obligation. Furthermore, only personal data indispensable for the realisation of the purpose of data processing and suitable for achieving that purpose may be processed. Personal data may only be processed to the extent and for the duration necessary to achieve the purpose. Where this principle is observed, the controller shall process only such personal data as is necessary for the performance of its tasks and the exercise of its powers. The requirements of purpose limitation and data minimisation apply to all stages of data processing, including data transfer.

In the request, the controller specified the classification under the Criminal Code of the criminal offence forming the basis of the suspicion, and indicated the scope of the data to be provided. In doing so, it effectively specified the conditions and purpose of the data request in accordance with the Code of Criminal Procedure, and provided the data necessary to identify the subject of the data provision. However, the request also included the victim's name and address, as well as a detailed description of the criminal offence forming the basis of the charge and the established facts. These criminal personal data can no longer be regarded as data serving to identify the subject of the data provision. It can be established that these personal data were entirely unnecessary for the purpose of the data processing – fulfilling the data request. To comply with the request, it would have been sufficient to state the number of the ongoing criminal proceedings and the classification of the criminal offence forming the basis of the charge under the Criminal Code.

In view of this, the Authority found that the controller had breached the principle of data minimisation set out in Section 4(2) of the Privacy Act during its proceedings. [NAIH-10593/2025]

III. Freedom of Information

Pursuant to Section 71/D(8) of the Privacy Act, the Authority shall prepare a report on its monitoring activities regulated in Chapter VI/B of the Privacy Act "annually – as part of the report specified in Section 38(4)(b)". Given that these monitoring activities are closely linked to the other tasks and powers relating to the monitoring and promotion of the right of access to data of public interest and data accessible on the grounds of public interest, and in certain respects overlaps with them in an inseparable manner, the Authority publishes the entirety of Chapter III of this Report as the report prescribed in Section 71/D(8) of the Privacy Act and commends it to the attention of the Reader

III.1. The Authority's monitoring procedures and the fulfilment of the RRF commitment

To implement Hungary's Recovery and Resilience Plan, reform C9.R26 entitled 'Enhancing transparency and access to information of public interest' (milestones 229–233), it is necessary to prepare half-yearly reports for the second half of 2022 and every subsequent year up to the first half of 2026 (under the commitment, a total of 8 reports must be published)

In order to fulfil the milestone [C9.R26.] entitled 'Improving transparency and access to information of public interest' set out in the European Commission's proposal COM(2022) 686, Act CI of 2023 on the system for the utilisation of national data assets and on certain services added a new Chapter VI/B to the Privacy Act, which assigned a new set of tasks and powers to the Authority and, in connection with this, established an expanded reporting obligation for organs performing public tasks. Under the statutory provisions, organs performing public tasks, specifically local authorities and publicly owned companies, are required to provide data by 31 January each year in respect of the previous year from 2024 onwards

a) the number of requests for access to data of public interest and data accessible on the grounds of public interest that were granted and refused, and the typical reasons for refusal,

b) the average number of days required to process requests for access to data of public interest and data accessible on the grounds of public interest, and

c) the exact internet address where data of public interest and data accessible on the grounds of public interest are published (hereinafter: freedom of information reporting).

Pursuant to Section 30(3) of the Freedom of Privacy Act, organs performing public tasks must keep a record of rejected requests for data and the reasons for such rejections. Furthermore, pursuant to Section 42 of Government Decree No. 335/2005 (XII. 29.) on the general requirements for document management by organs performing public tasks, requests for data of public interest received by the organ must also be filed in a manner that allows them to be retrieved by subject. This register forms the primary basis for the present report, but where justified, the organisation may also maintain a separate register for the purpose of fulfilling the reporting obligation. The provision of data constitutes one of the cornerstones of a procedure falling within the Authority's remit – the monitoring of compliance with the requirements regarding the transparency and accessibility of data of public interest and data accessible on the grounds of public interest. This is known as the monitoring procedure.

In addition to the above, the Authority is required to perform the following tasks within the framework of freedom of information monitoring, pursuant to Section 71/D of the Privacy Act:

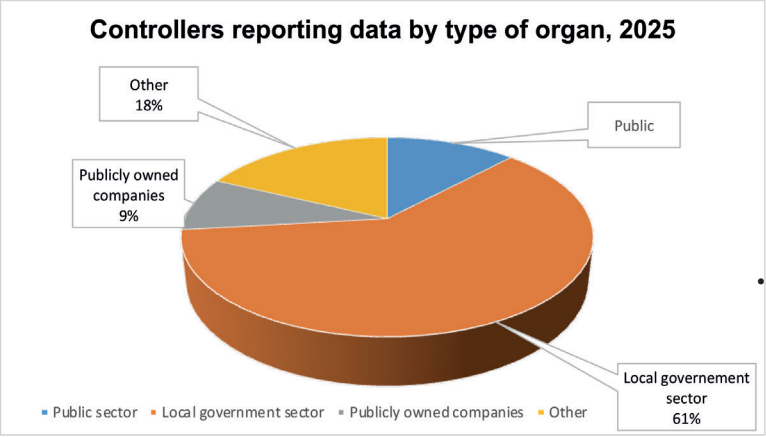
- It monitors the obligated organs twice a year on the basis of the data provided. The Authority's monitoring covers the examination of the publication of data of public interest and data accessible on the grounds of public interest.
- It shall also carry out separate monitoring activities on the basis of notifications.
- For the purposes of conducting monitoring, the Authority may request data from the organs, which are obliged to comply within 8 days of receipt of the request.
- The Authority may make recommendations to the organs subject to inspection in order to ensure compliance with the requirements regarding the transparency of data of public interest and data accessible on the grounds of public interest, and the provision of access to such data.
- The head of the organ concerned by the recommendation shall draw up an action plan to implement the necessary measures and shall send it to the Authority within 15 days of receipt of the recommendation.
- The Authority shall prepare an annual report on the monitoring as part of its public report.

III.1.1. Statistical data on freedom of information reporting

For 2025, the Authority received reports from a total of 6,547 obligated organs, covering the following types of organs:

- state-owned companies, state public authorities, state public institutions, budgetary organs under the Act on Public Finances, legal persons registered in the register of legal entities, public organs (public sector);
- local authorities, representative organs and their organs, budgetary organs established and supervised by local authorities, national minority self-governments and their organs, organs established and supervised by national minority self-governments (local government sector);
- publicly owned non-profit companies, state-owned companies performing public tasks specified by law, state-owned companies operating with a shareholding in state assets of priority importance to the national economy, and local government-owned companies (publicly owned companies);
- church-run institutions, KEKVA, public foundations, private-law organisations performing public tasks, legal entities established by law, other (other organs performing public tasks).

The distribution of reporting organs by type of organ is shown in the figure below.

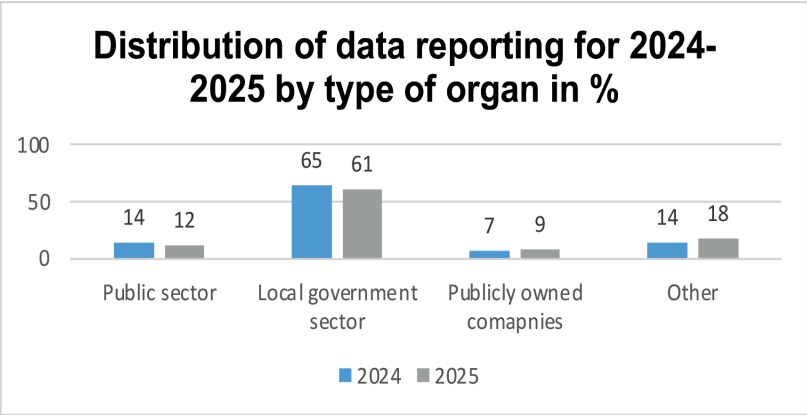


The number of organs providing data continues to show an upward trend. The reporting obligation, which came into force in 2024 with expanded data requirements

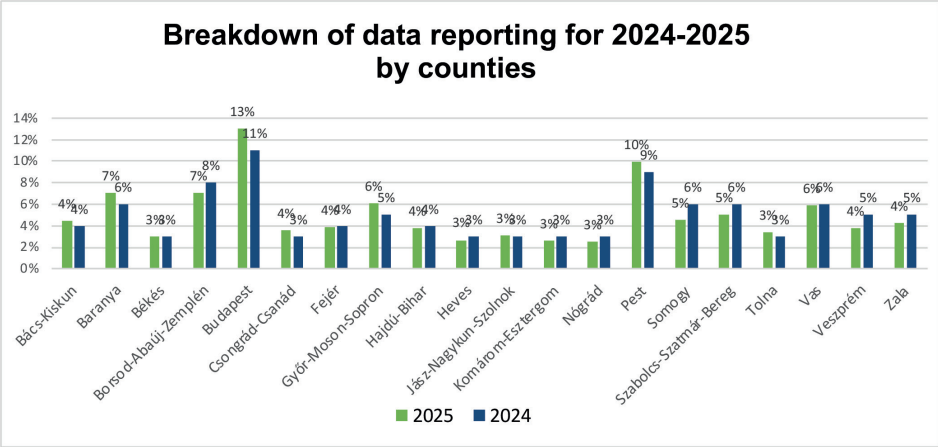
- in 2024 (for the year 2023) 5895,
- in 2025 (for the year 2024) 5952,
- in 2026 (for the year 2025) 6547

organs performing public tasks met the statutory deadline (by 31 January of the year following the reference year).

The largest group of data providers, in terms of the total number of data providers, continues to be the local government sector (local authorities, national minority local authorities and their organs). The number of data providers in the 'other' category has increased: higher education institutions, KEKVAs, and educational institutions maintained by churches or foundations have also joined the group of data providers. The willingness of publicly owned companies to provide data has also increased. In the public sector – as in the local government sector – the number of reports for 2025 fell short of last year's figures.



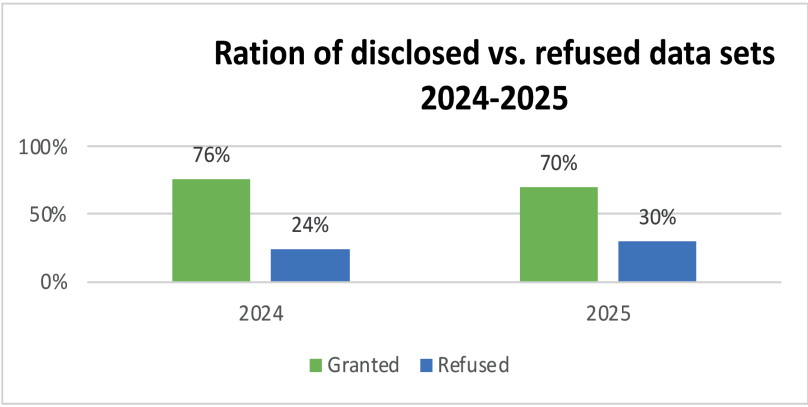
In terms of the geographical distribution of data-reporting organs, the majority of submissions continued to come from Budapest and Pest County. At the same time, a slight increase can be observed in several counties: there was a rise of 1 percentage point each in Borsod-Abaúj-Zemplén, Somogy, Szabolcs-Szatmár-Bereg, Veszprém and Zala counties.



The ratio of fulfilled vs rejected requests for data of public interest has shifted in a negative direction compared to the 2024 figures.

- According to the aggregated data for **2024, 76%** of the data sets specified in requests for data of public interest submitted to the 5,952 organs performing public tasks **were granted**, whilst **24%** of the data sets **were refused**.

In the aggregate for **2025** – first and second halves – a total of 14,965 requests for data of public interest were received by 6,547 organs, covering 41,394 data sets. Access to data (**data disclosure**) was granted in 28,958 cases [70%], whilst in 12,433 cases [30%] controllers **refused** to comply with the requests for data of public interest.

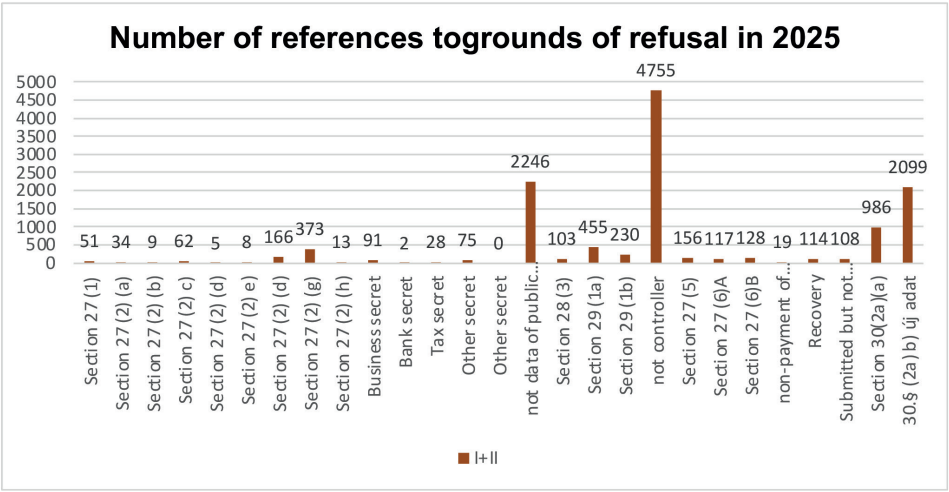


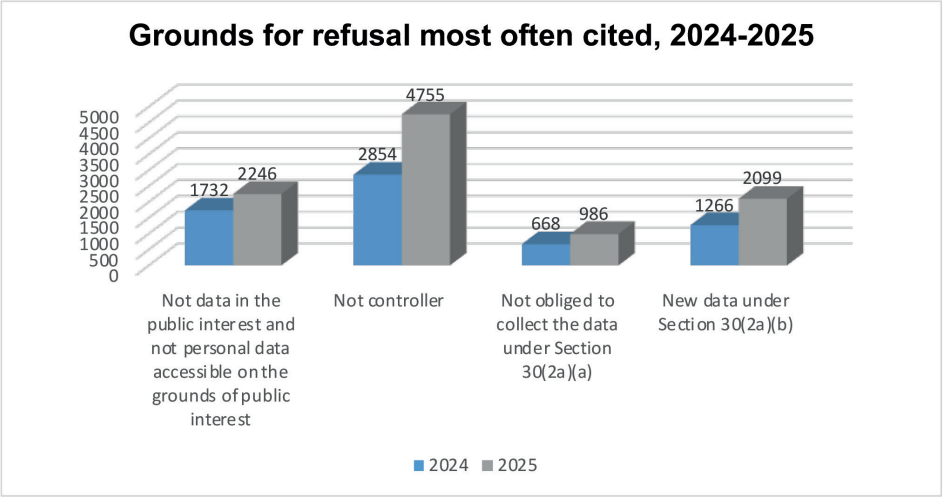
The 2025 data show that controllers most frequently applied four restrictions on access when refusing to disclose data:

1. the data sought is not in the public interest and is not personal data accessible on the grounds of public interest;
2. the organ performing a public task does not process the data sought;
3. pursuant to Section 30(2a)(a) of the Privacy Act, the organ performing a public task is not obliged to obtain or collect data not under its actual control;
4. pursuant to Section 30(2a)(b) of the Privacy Act, comparing data of public interest or data accessible on the grounds of public interest that are actually processed by the public organ with the data in its possession would necessitate the generation of new data.

According to statistical data, in 2024, the two new grounds for refusal introduced at that time (Section 30(2a)(a) and (b)) and references to 'non-controller' status accounted for 57% of all grounds for refusal.

In 2025, the four most frequently applied grounds for refusal [10,086] accounted for 81% of all grounds for refusal [12,433].





According to the statistical data, public organs cited the grounds for refusal most frequently used in previous years significantly more often in 2025 when refusing to disclose data:

Grounds for refusal	2024	2025	difference + %
Data not of public interest and not personal data accessible on the grounds of public interest	1732	2246	29.7%
Not controller	2854	4755	66.6%
Section 30(2a) a) of the Privacy Act	668	986	47.6%
Section 30(2a) b) of the Privacy Act	1266	2099	65.8%

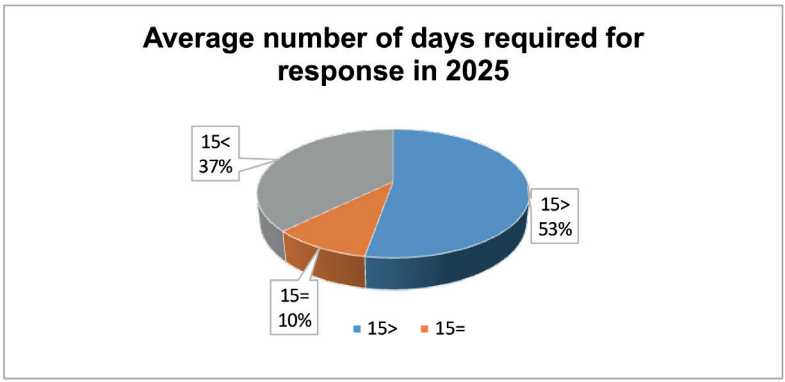
Of the public organs and organisations managing public funds that are required to report data, **4,440 organs** – 68% of all data providers – **submitted what is known as a 'zero' data report in terms of data requests**. Of the 32% of organs accounting for the difference, **897 controllers refused to comply in respect of a total of 12,433 data sets**.

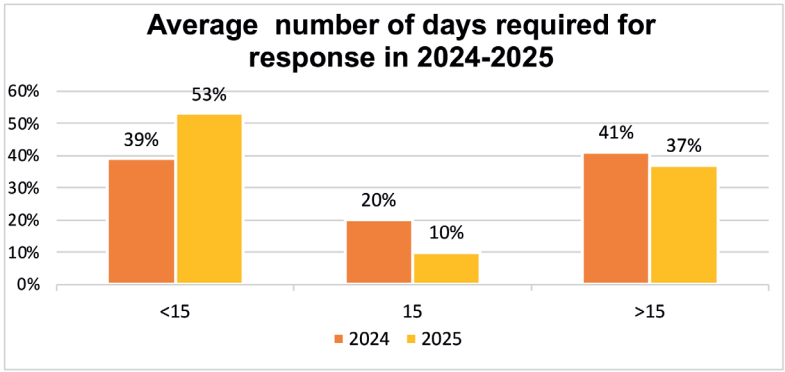
The content of the report also includes the determination of the average number of days spent fulfilling data requests in the given year. **In 2024 – bearing in mind that the report covers a period spanning two half-years – the average number of days spent fulfilling data requests was 12.5 days for those public organs to which data requests were submitted**.

In 2025, the statistics were as follows: in the first half of 2025, 12.5 days; in the second half, 9.7 days; and for the whole year, 11.1 days were taken for the organs to respond to (grant or refuse) the requests for data of public interest received by them.

An analysis of the data received shows that of the authorities assessing data requests [**total: 2107**]

- 53% responded in less than 15 days,
- 37% took more than 15 days to respond
- to the data requests submitted to them; whilst
- on the 15th day specified in the Privacy Act, 10% of controllers provided a response to the data requester.





A comparison of data provision figures for 2024 and 2025 shows that compliance with the specified deadline (15 days) for responding to requests for data of public interest has improved among data-providing organs. The number of organs that provided a response before the 15-day deadline has increased, whilst the number of organs that failed to meet this deadline when responding to data requesters has decreased

III.1.2. Monitoring procedures to verify compliance with the provision of access to data and to examine the practice of fulfilling individual data requests

In 2025, the Authority initiated a monitoring procedure to examine individual data requests in respect of the following organs pursuant to Section 71/D(1) of the Privacy Act:

- the National Water Authority and the regional directorates (13 organs),
- the national park directorates (10 organs), and
- the following organs performing public tasks:
  - Municipality of Balatongyörök,
  - Municipality of Budapest District XII (Hegyvidék),
  - Diákhitel Központ Zrt.,
  - Duna-menti regionális Vízmű Zrt.,
  - Municipality of Felsőmarác,
  - Municipality of Gyúró,
  - Mayor's Office of Nyíregyháza City of County Rights,
  - Municipality of Pécs City of County Rights,
  - Pest County Government Office,
  - Municipality of Tarnazsadány,
  - Joint Municipal Office of Tarnazsadány,
  - Municipality of Und,
  - Municipality of Zákány,
  - MÁV Személyszállítási Zrt.,
  - MÁV Zrt.,
  - MÁV-Start Vasúti Személyszállító Zrt.,
  - Volánbusz Zrt.

During its monitoring, the Authority not only examined the requests for data of public interest submitted to and assessed by the monitored organ in 2025, along with the responses provided to them, but also reviewed the procedures of the monitored organs for ensuring access to data of public interest. In addition, where applicable, it requested the judgments handed down in public data litigation cases arising from refusals to disclose data

During the monitoring, the majority of public organs cooperated, responding to the Authority's requests within a short timeframe, accepting the Authority's recommendations and drawing up action plans to address the issues raised in the recommendations, with many of the points outlined in the recommendations having been implemented by the time the action plan was submitted. The monitoring

covered the legality of the extension of the response deadline, the clarification of the data request, the appropriate application of the restriction on access to data cited when refusing to disclose data, and the provision of information on the right to seek legal redress.

The Authority summarised the shortcomings identified during the monitoring, its recommendations, and the results of the monitoring in individual reports published in full on the Authority's website. [https://naih.hu/monitoring-jelentesek-menu-heading/kozerdeku-adat-kiadasi-monitoring]

Typical errors identified in the internal rules governing the disclosure of data of public interest and in the practices of public organs

Freedom of information is a 'Janus-faced' right, with the data requester and their fundamental right and its exercise on one side, and the public organ performing a public function as the party bound by that fundamental right on the other. This also underpins the position consistently upheld by the Authority, namely that when fulfilling requests for data of public interest submitted to them under the Privacy Act, public organs are not providing a service, but are facilitating the exercise of the fundamental right to access and disseminate data of public interest. The most important task in the context of fulfilling requests for data of public interest is the development of a set of rules for the organisation governing the data disclosure process, in which the organ performing a public function sets out the organisational units involved in the process of fulfilling the data request, their tasks and the associated internal deadlines. Generally, the internal rules drawn up and in force by public organs regarding the procedure for responding to data requests adopt the provisions of the Privacy Act almost word for word, alongside the Act's definitions. There have also been instances where a public organ has identified its internal rules on the handling of reports and complaints of public interest within the procedural rules for fulfilling requests for data of public interest. During all monitoring activities, the Authority examined and analysed the internal rules of the monitored organ setting out its data disclosure procedures, in which it identified the following typical errors and shortcomings:

- the absence of a data provision obligation under Section 71/D(4) of the Privacy Act,
- failure to maintain records, as required by Section 71/D(4) of the Privacy Act, regarding requests for data of public interest that have been granted or refused and the reasons therefor,

– the obligation to provide the applicant with information on the legal remedies available to them under the law, to give reasons for the rejection of the data request, and to extend the deadline for compliance,
– informing the data requester, in accordance with Article 5 of the Tromsø Convention, of the identity of the organ holding the data sought, if the authority itself does not hold the requested data.

In addition to the above shortcomings, several of the monitored organs did not apply the mechanism for extending deadlines correctly. It is the Authority's consistent position that an organ performing a public function is entitled to extend the deadline for fulfilling a data request only in the cases specified in the Privacy Act. Consequently, if a public organ extends the deadline for fulfilling a data request, it can no longer lawfully refuse to fulfil the request within the extended deadline. In other words, the extension of the compliance deadline also implies that the public organ has already examined the data request, and as part of this process, has satisfied itself that the request can be fulfilled and has determined that there are no grounds for refusal that would prevent compliance; however, it requires a longer period of time for actual compliance

This is a recurring problem; therefore, the Authority considers it important to highlight the conditions for the lawful application of Section 30(7) of the Privacy Act in its report. In the Authority's interpretation, Section 30(7) of the Privacy Act provides for a simplified method of fulfilling requests for data of public interest in the case of controllers performing public tasks by stipulating that – in the event of fulfilling a data request aimed at accessing a presumably large volume of data of public interest – the organ performing a public task is not obliged to comply with a request for access to data aimed at a comprehensive, invoice-level audit of financial management in accordance with the request. The Authority emphasises that, with reference to Section 30(7) of the Privacy Act, a request for data cannot lawfully be refused. The public organ must comply with such data requests by providing information on the fundamental characteristics of the legal relationship in question. In doing so, the public organ acting as controller ensures that the data requester can precisely identify, from the data provided, the specific legal relationship in respect of which they may be requesting the disclosure of further data of public interest. By virtue of the law, fulfilment using the reduced set of data specified therein (a 'simplified' form of fulfilment), at the discretion of the organ, shall be deemed to be equivalent to the organ having fulfilled the data request in accordance with the original application. This legal presumption may be rebutted to the extent that the data requester disputes the facts and circumstances forming the basis of the method of fulfilment, namely that the request is aimed

at a comprehensive, invoice-level and itemised audit, and the controller performing a public task is unable to prove this, meaning that the method of fulfilment in question was applied unlawfully.
The drafting of the rules of procedure and their publication in the general publication scheme (point II.13) in accordance with Annex 1 of the Privacy Act is an obligation of the organ performing a public function as laid down in the Privacy Act; however, the mere existence of the rules of procedure does not in all cases imply the legality of the procedure followed in fulfilling data requests, the legality or lack thereof being most evident in the application and justification of data disclosure restrictions.
The results of the monitoring inspections carried out by the Authority will become apparent in the years following the inspection, as the new rules of procedure drawn up on the basis of the action plans prepared to remedy the identified shortcomings must be integrated into the day-to-day practice of the organs. The success or failure of the corrective measures can be determined on the basis of data disclosure practices in the coming years and the examination thereof.

III.1.3. Monitoring procedures for the disclosure practices of organs performing public tasks

Scope of the monitored organs

In 2025, the Authority reviewed the publication practices of 76 public organs listed below, either upon notification or ex officio, as part of the monitoring procedure under Section 71/D of the Privacy Act:

- Municipality of Nyírderzs,
- Municipality of Tiszanagyfalu,
- Municipality of Nyírcsászári,

Szent István tér Mélygarázs és Üzemeltető Korlátolt Felelősségű Társaság,

- EGERERDŐ Erdészeti Zártkörűen Működő Részvénytársaság,
- Municipality of Bánhorváti,
- DALERD Délalföldi Erdészeti Zártkörűen Működő Részvénytársaság,
- Gyulaj Erdészeti és Vadászati Zártkörűen Működő Részvénytársaság,
- Slovak Minority Self-government of Bér,
- Roma Minority Self-government of Bér,
- Municipality of Bér,
- Welfare Center of the Municipality of Szekszárd City of County Rights,
- Basic and Specialised Welfare Services Association of Szekszárd and Area,
- Municipality of Szekszárd City of County Rights,
- Kitchen of the Municipality of Gávavencsellő,
- Welfare Services Center of Gávavencsellő,
- Social Services association of Gávavencsellő,
- Art Centre and Municipal Library of Gávavencsellő,
- Joint Municipal Office of Gávavencsellő,
- Municipality of Gávavencsellő,
- Municipality of Nyírbogát,
- Municipality of Gyöngyösoroszi,
- Municipality of Pély,
- Municipality of Mátraderecske,
- Municipality of Bakonyszombathely,
- Municipality of Igrici,
- Municipality of Szegi,
- Municipality of Polány,
- Municipality of Balatonszemes,
- Municipality of Nagyszékely,
- Municipality of Bükkszentkereszt,
- Municipality of Tarján,
- Municipality of Szabadszállás,
- Roma Minority Self-government of Szabadszállás,
- Municipality of Ipolytarnóc,
- Municipality of Debrecen City of County Rights,
- Municipality of Szendehely,
- Municipality of Hódmezővásárhely City of County Rights and
- Mayor's Office of the Municipality of Hódmezővásárhely City of County Rights,
- Municipality of Fonyód,
- Municipality of Kistokaj,
- Kognitív Hungary Kereskedelmi és Szolgáltató Kft.,
- BKMFÜ Bács-Kiskun Megyei Fejlesztési Ügynökség Nonprofit Kft.,
- Mayor's Office of Tószegi,
- Municipality of Ömböly,
- Municipality of Újszilvás,
- Municipality of Biri,
- Municipality of Ajka,
- Municipality of Birjáni,
- Erzsébet Királyné Szálloda Kft.,
- MECSEKÉRC Környezetvédelmi Zrt.
- Szolgáltató és Kulturális Központ Nonprofit Kft.,
- NYÍRERDŐ Nyírségi Erdészeti Zrt.
- Municipality of Nagypáli,
- Municipality of Uzsa,
- Zalaegerszegi Városfejlesztő Zrt.,
- Municipality of Tiszabura,
- Municipality of Magyarhertelend,
- Municipality of Encsencs,
- Municipality of Vácrátót,
- Municipality of Atkár,
- ROTAQUA Geológiai-, Bányászati kutató Mélyfúró Kft.,
- Municipality of Kápolna,
- MÁV Szimfonikusok Zenekari Alapítvány,
- Municipality of Vasszécseny,
- Joint Municipal Office of Vasszécseny,
- Kindergarten Maintenance Association of Vasszécseny, Tanakajd and Csempeszkopács,
- Multi-purpose Association of the Szombathely Small Region,
- Municipality of Lakitelek,
- Municipality of Nagyigmánd,
- Municipality of Sülysáp,
- Municipality of Tárnok,
- Municipality of Kajászó,
- BONYCOM Nonprofit Kft.

The Authority has published reports containing the recommendations made during the proceedings and the findings of the review of the measures taken on its website at https://www.naih.hu/monitoring-jelentesek/kozzeteteli-gyakorlatot-erinto-monitorig for each case. A monitoring procedure launched in 2025 to review the publication practices of further 30 organs is still ongoing at the time of finalising this manuscript.

Good practices, negative experiences

The Authority's procedures were mostly successful; the publication schemes were posted on the websites of organs that did not have a publication scheme, and although the necessary data of public interest were not uploaded completely in any single case, they were uploaded with minor or major omissions. The Authority considers the general publication schemes available at the following link to be good examples:

- https://tiszapuspoki.hu/index.php?option=com_content&task=view&id=50&Itemid=136,
- the table on Bakonyszombathely's general publication scheme concerning data relating to the procedure for handling official matters https://www.bakonyszombathely.hu/kozerdekuadat/II.4%20v2.pdf,
- https://lszkk.hu/kozerdeku-adatok/, in the general publication scheme made available on the https://lakitelek.hu/kozzeteteli-lista/ website, the almost complete text of the relevant contracts was also published in connection with point III.4.

However, 20% of the monitored organs failed to publish a general publication scheme despite the procedure and did not cooperate during the procedure.

Typical errors in publication

The Authority identified the following typical errors, which continue to persist, during its 2025 monitoring investigations.
Despite the fact that Section 2(1) of Decree 18/2005. (XII. 27.) IHM Decree stipulates that organs must place a link to the publication scheme on the page that appears when the website for publication is opened, it is very often only found after a lengthy search, in a sub-menu of a menu item or at the bottom of the website in inconspicuously small print. Under the law, the link must be placed in a clearly visible manner on the organ's home page under the heading 'Data of public interest'. The date of the data update – which provides essential information to interested parties regarding the currency of the published text – is also usually

missing. In notifications concerning local authorities, the most frequently missing items are invitations to council meetings, proposals, minutes and resolutions (Annex 1 of the Privacy Act, publication units II/8 and II/9). Given the significant public interest involved, particular attention must be paid to ensuring that this information is published in a timely and complete manner. The results of tenders and the reasons for them are frequently missing (II./11.). As a result of the collection of statistical data on activities, the Authority expects, among other things, the publication of OSAP (National Statistical Data Collection Programme) data tables; these are often missing (II./14.). Budgets and reports are often published not for 10 years but for 1–2 years retrospectively (III./1.). It is not sufficient to update data on employees annually; this must be done quarterly, and the publication of local authorities' budget regulations is not sufficient in this regard; the organs are obliged to publish precisely the data required (III./2.). Only the support provided from the central subsystem of public finances qualifies as budgetary support; thus, local authorities and publicly owned companies do not provide budgetary support (III./3.). The full text of grant agreements and contracts for the implementation of development projects funded by the European Union must be published, not just a brief description of the project (III.7.). For public procurement information, the document uploaded to the 'Summary of the evaluation of tenders' section of the public procurement procedure data sheet in the EKR (Energy Efficiency Commitments System) procedure repository and the exact link to the contract's EKR data sheet (requiring no further identification) must be uploaded (III./8.).

Monitoring of disclosures by publicly owned companies

In 2025, the Authority paid particular attention to monitoring the disclosure practices of state- or local government-owned companies falling within the scope of Act CXXII of 2009 on the more economical operation of publicly owned companies (hereinafter: the Act). This focus was also justified by the fact that these companies do not fall within the scope of Section 37/C of the Privacy Act; consequently, the Authority does not monitor the disclosure of financial data by state- or local government-owned companies in its transparency proceedings. On several occasions, the organ under scrutiny disputed that it qualified as an organ performing a public function. The Authority emphasised that, in accordance with the consistent position of the Constitutional Court[7] and the Authority[8], publicly owned business associations qualify as organs performing a public function, and must therefore comply with all obligations imposed by the Privacy Act

7 See: Para [41] of Constitutional Court Decision AB 25/2014. (VII.22.)
8 https://naih.hu/files/2016-03-11-nemzeti_vagyonnal_gazd_2016_1911_V.pdf

on organs performing public tasks, including the disclosure obligation set out in Section 33(3) of the Privacy Act.
Pursuant to Section 37(2) of the Privacy Act, legislation may specify additional data to be published in relation to certain sectors or types of organs performing public duties (hereinafter: sector-specific publication schemes). The specific publication schemes, including those under the Act CXXII of 2009 on the more economical operation of publicly owned companies, must be included in point II/18 of the general publication scheme. Section 2(3) of this Act lays down special rules regarding the value of contracts and the retention period. Publicly owned companies shall comply with the publication of their contract-related data in point III/4 of the general publication scheme in accordance with these specific rules. [NAIH-11357/2025, NAIH/11259-6/2025, NAIH/1286-5/2025.]

Electronic publication obligations of public education institutions

In 2025, the Authority received several consultation requests regarding the electronic publication obligations of public education institutions operated by local authorities as independent budgetary organs. Four local authority-maintained nursery schools requested the Authority's opinion regarding Chapter IV of the Privacy Act on the "Publication of data of public interest". Pursuant to Section 33(4) of the Privacy Act, public education institutions and vocational training institutions fulfil their electronic disclosure obligations under this Act by providing data to the information system specified in sectoral legislation. In the case of public education institutions, the information system referred to in Section 33(4) of the Privacy Act is the Public Education Information System (hereinafter: KIR) pursuant to Government Decree 229/2012 (VIII.28.) (hereinafter: Nkt. Vhr.). However, the Nkt. Vhr. does not provide for the publication of data of public interest as set out in Annex 1 to the Privacy Act; it merely lays down detailed rules concerning the content and publication of data of public interest included in the specific publication scheme for public institutions[9]. At the same time, Section 37(1) of the Privacy Act requires organs subject to the publication obligation – which also includes the organs listed in Section 33(4) of the Privacy Act, to publish the data specified in the general publication scheme set out in Annex 1 in accordance with the provisions of Annex 1, in relation to their activities. In view of the fact that public education institutions are unable to fulfil their obligation to publish the data included in their general publication scheme set out in Annex 1 of the Privacy Act via the KIR, the Authority has determined that public educa-

9 The content of the financial and economic data of public interest set forth in Section 20 of Nkt. Vhr., as well as the data specified in the publication scheme for public education institutions set forth in Section 23, differs from the data content of the general publication scheme contained in Annex 1 of the Privacy Act.

tion institutions operated by local authorities as independent budgetary organs must fulfil their obligation to publish data of public interest as set out in Annex 1 of the Privacy Act by publishing such data on their own websites, on websites maintained by the supervisory organs, or on the central website established for this purpose (kozadat.hu). [NAIH-10556/2025.]

In order to clarify the legal issue, the Authority also contacted the Education Office (hereinafter: OH), which is responsible for operating the KIR, and received a response that was consistent with the Authority's position set out above. According to the OH's position, Section 33(4) of the Privacy Act is applicable only if the sectoral legislation actually and comprehensively defines the scope of data listed in Annex 1 to the Privacy Act, and further provides for their publication in a structured manner in accordance with the legislative framework. Section 37(1) of the Privacy Act clearly stipulates that organs subject to the publication obligation – including public education institutions – are required to publish the data set out in the general publication scheme in Annex 1, specifically in the structure defined in the Annex. This obligation encompasses both substantive and formal requirements: on the one hand, the publication of the full data content; on the other hand, a structured presentation with a uniform format. Furthermore, as a technical obligation, Section 37/B of the Privacy Act also requires the transfer of data to the public data search system. These obligations may only be superseded if sectoral legislation itself prescribes the same content and structure within the sectoral information system. However, as this is not currently the case, the general publication obligation cannot be fulfilled solely through the KIR. Sectoral regulations, namely the Public Education Act and its implementing decree (Nkt. Vhr.) define the content of the 'specific publication scheme' applicable to public education institutions and establish clear obligations in this regard. Sections 23–24 of the Nkt. Vhr. set out the data and documents that institutions are required to publish, and the relevant subsystems of the KIR have been developed to display these. However, the Nkt. Vhr. does not contain the data from the general publication scheme set out in Annex 1 of the Privacy Act, nor does it provide authorisation for the KIR to function as a platform for the publication of the general publication scheme. Sections 19–20 of the Nkt. Vhr., which concern financial and management data, prescribe the provision of data for statistical purposes, which has no publication function. The data provided in the data reporting are classified as data of public interest; however, the Nkt. Vhr. does not include the data provided therein among the elements of the publication scheme. Therefore, based on the legal interpretation followed by the OH, the current content of the KIR is not suitable for replacing the general publication scheme. The KIR institutional register, which is defined in Section 1(2)(1) of the Nkt. Vhr. as a register

operated as a KIR subsystem, does not qualify as a publication scheme. The institutional register contains the basic data of institutions; its function is for registration purposes, and it does not correspond to the legal content of either the general or the specific publication scheme. In view of all this, the general publication scheme must continue to be published on the website of the public education institution or its operating organ, or via the public data search system. [NAIH-11802/2025.]

Publication of the reported statistical data in the general publication scheme

The Authority requested an opinion from the Central Statistical Office (hereinafter: CSO) regarding the determination of the data to be uploaded to point II.14 of the general publication scheme set out in Annex 1 to the Privacy Act, specifically concerning the precise legal authorisation under which public organs and in respect of which data sets they are required to carry out statistical data collection(s) and provide data on their activities. In its reply, the CSO informed the Authority that the definition of statistical data collection based on legislation is broader than that of official statistical data collection. Official statistical data collection is to be understood as data collection ordered pursuant to Act CLV of 2016 on Official Statistics (hereinafter: Stt.) and Government Decree 388/2017. (XII. 13.) on the mandatory data reporting requirements of the National Statistical Data Collection Programme (hereinafter: OSAP Decree); however, other legal sources may also prescribe statistical data collection that does not qualify as official statistics. The definition of official statistical data collection under the Stt. means the collection of characteristics of a population defined by the statistical survey, relating to a given period or point in time, through the questioning of selected data providers or direct observation. The OSAP Decree specifies the scope of data on which members of the Official Statistical Service must carry out statistical data collection(s). In view of this, official statistical data collections carried out under the OSAP Decree are data collections based on legislation; and therefore, in the case of data sets relating to the activities of an organ performing a public function, the obligation of the organ performing a public function to publish such data may arise – with regard to point II.14 of the general publication scheme set out in Annex 1 to the Privacy Act. [NAIH-7995/2025.]

III.2. Transparency authority procedures

On the Central Public Data Register platform[10] (hereinafter: the Platform), interested citizens can obtain a comprehensive overview in one place of an organ's contracts – including not only contracts concluded as a result of public procurement –, the grants they provide and payments made for purposes other than their core functions. The Authority pays particular attention to ensuring that all data subject to this obligation are fully accessible on the Platform, and that obligated parties update these data following the conclusion of a contract and throughout its performance.

Section 37/C(1) of the Privacy Act was amended with effect from 1 January 2025. From 1 January 2025, legal entities registered in the register pursuant to Act CXCV of 2011 on Public Finances, such as local authorities, are also required to publish on the Platform. With the expansion of the scope of entities subject to this obligation, 12,398 organs are now required to publish their financial data on the Platform. Interested members of the public can check whether an organ is a legal entity registered in the register at the MÁK Register of Legal Entities[11].

In view of the fact that a large number of the newly obliged entities are local authorities, and that the Authority had previously identified significant shortcomings in local authorities' compliance with their general disclosure obligations as part of a comprehensive freedom of information project, the Authority specifically examined local authorities' disclosures on the Platform in 2025. In 2025, the Authority checked the disclosures of 556 local authorities on the Platform. Of these 556 local authorities, 351 were missing contracts from the Platform (63%). These local authorities had not submitted any data at all by the time of the inspection and were unaware of the new publication obligation

The Authority initiated 157 transparency authority proceedings in 2025, thereby making the use of approximately 16 billion forints of public funds more transparent. As in previous years, during the authority proceedings, the organs under scrutiny – without exception – rectified the infringement even whilst the proceedings were ongoing; there was no need to issue an order in any case. In its transparency authority proceedings, the Authority has not entirely departed from the ombudsman-style approach; during proceedings, it endeavours to ensure that clients understand exactly how to comply with the new obligation. In 2025, the

10 https://kif.gov.hu/
11 https://www.allamkincstar.gov.hu/Koltsegvetes/Torzskonyvi_nyilvantartas/ktorzs

local authorities under investigation did not appeal against the Authority's decisions on a single occasion.

The Authority found that, in the Electronic Public Procurement System (EKR), those required to publish information rarely update the data on contract amendments or on subcontractors used during performance following the conclusion of contracts. At the same time, data on subcontractors used provide important insights into the actual use of public funds; therefore, transparency regarding subcontractor data is a key tool in the fight against corruption. The Authority therefore pays particular attention to the publication of these data in its proceedings. If, during the public procurement procedure, the tenderer indicated the likely use of subcontractors and, despite this, the contracting authority did not publish data on subcontractors on the Platform, the Authority, in the course of clarifying the facts, calls upon the parties to make a statement regarding the subcontractors used during the performance of the contract and their fees.

Several of the organs examined interpreted the obligation to publish subcontractor fees as requiring only the publication of fees actually paid to subcontractors. However, in the Authority's view, in relation to the fulfilment of the obligation to publish on the Platform, it is irrelevant whether the subcontractor's fee was actually paid to the subcontractor(s) or not, as the fee must still be published on the Platform if the consideration stipulated in the subcontract has been notified to the contracting authority, even if the actual payment has not yet taken place. Section 37/C(3)(b)(bb) of the Privacy Act requires the publication of the subcontractor's fee where it is 'specified'. Subcontractor fees are determined in subcontracts; therefore, it is the conclusion of the subcontracts, and not the actual payment of the subcontractor fees, that gives rise to the obligation. [NAIH-12456/2025, NAIH-12380/2025]

In the data sheet published during the transparency procedure, a local authority named 6 subcontractors in relation to a contract, but did not specify the amounts of the subcontractor fees. The Authority drew the client's attention to Section 138(3) of Act CXLIII of 2015 on Public Procurement (hereinafter: Kbt.), which stipulates, regarding the content of the notification of subcontractors, that "The successful tenderer shall, together with the notification, provide the contracting authority with the subcontractor's name, tax number, contact details and the person authorised to represent them, as well as the expected percentage of the subcontractor's performance within the tenderer's performance and the value of the consideration under the subcontract." In the subcontracts, on the basis of which the successful tenderer presumably fulfilled its reporting obligation to the local authority regarding subcontractors—that is, not only the name of the sub-

contractor but also its fee was specified— therefore the local authority must have had access to the data on fees if the subcontractors used had been notified to it. [NAIH-15651-4/2025.]

In the case of contracts concluded as a result of a public procurement procedure, those required to publish information often provide an incomplete list of tenderers. A recurring error of legal interpretation is that only the tenderers of valid tenders are listed on the Platform. According to Section 3 of the Public Procurement Act, for the purposes of this Act, a tenderer is an economic operator who submits a tender in a public procurement procedure. The Public Procurement Act treats invalid tenders as tenders, and those submitting invalid tenders are also classified as tenderers. Pursuant to Section 6:64(1) of Act V of 2013 on the Civil Code, a tender is a legal declaration that clearly expresses the intention to conclude a contract and covers the essential matters. Consequently, the Authority takes the view that, in the case of contracts concluded as a result of a public procurement procedure, all tenderers must be named on the Platform, including those whose tenders were deemed invalid during the evaluation process. [NAIH-13664-4/2025]

Several local authorities cited Section 37/C(2)(a) of the Privacy Act as the legal basis for the publication of the grants they provided. However, in the Authority's view, the grants provided by local authorities cannot be classified as 'budgetary grants under the Act on Public Finances', given that the Act on Public Finances defines budgetary grants in Section 1(14) as grants provided from the central subsystem of public finances. The Authority's position was also confirmed by the Ministry of Justice which, having sought the professional opinion of the Ministry for National Economy, concluded that the concept of budgetary support under Section 1(14) of the Act on Public Finances covers support originating from the central subsystem of public finances; whereas, in relation to the local government subsystem, the main element of this concept is not met; therefore, Section 37/C(2)(c) of the Privacy Act may serve as the legal basis for the disclosure of such support. In the Authority's view, there is a significant public interest in the transparency of subsidies provided by local authorities, given that a large amount of public funds is used for this purpose. [NAIH-12094-/2025.]

With regard to grants, it is important to emphasise that where an implementing organ concludes the grant agreement on behalf of the organ subject to the disclosure obligation, the agreement creates rights and obligations directly between the organ subject to the disclosure obligation and the beneficiary; therefore, from the perspective of legal effects, it must be regarded as if the grant agreement

had been concluded by the organ subject to disclosure with the beneficiary. Even if the budgetary grants are transferred to the implementing organ's account, the implementing organ may not manage the amounts thus transferred. Its task is to transfer the specified grant amounts onwards. The implementing organ cannot therefore be the beneficiary of the grant, and as such cannot be published as such on the Platform, since the beneficiary – based on the general meaning of the term – is the person who may use the grant provided. (Fővárosi Törvényszék 105.K.704.156/2024/12; the Authority won the case; the proceedings are described in more detail in the section on litigation.)

Another recurring error relating to grants is that columns 18–23 of the data sheet to be published on the Platform are not only completed in respect of the grant provided by the party required to publish the information, but also contain details of grants received by that party.
Yet another recurring error when completing the data sheets is that the statutory designations are not used in relation to the type, legal basis and form of the contract; as a result, one or two of the three required data points are generally missing from this column.

Finally, the Authority draws the attention of organs subject to the disclosure obligation to the provision that came into force on 1 January 2025, which states *"Those subject to the disclosure obligation shall, when submitting data on a bimonthly basis, publish data generated up to the 30th day preceding the deadline for the next data submission."* The Authority emphasises that if a contract was concluded up to 30 days prior to the data submission on the Platform, it must still be published in the report even if two months have not yet elapsed since the conclusion of that contract (for example, a contract concluded on 13 February must already be published in a report dated 20 March).

III.3. Matters relating to local authorities

1. Invoice-level checking

In one case, the applicant requested access to invoices and bank statements relating to a local authority's income and expenditure for April and May 2024. The local authority refused to comply with the data request, citing Section 30(7) of the Privacy Act (comprehensive, invoice-level checking). During its investigation of the case, the Authority issued a statement in which it drew the local authority's attention to the following:

Data relating to the financial management of the local authority, as an organ performing public duties, constitute data of public interest within the meaning of Article 39(2) of the Fundamental Law and Section 3(5) of the Privacy Act. Access to financial data may only be restricted within the scope specified in Section 27 of the Privacy Act. Pursuant to Sections 27 (3) to (3b) of the Privacy Act, neither the organ performing a public function nor the parties contracting with it may invoke trade secrets when fulfilling a data request; only protected information may be rendered unrecognisable when making copies, pursuant to Section 30(1) of the Privacy Act.

The provisions of Section 27(3)–(3b) of the Privacy Act classify information relating to the management, ownership, use, exploitation, disposal and encumbrance of central and local government budgets, as well as the use of European Union funding, budgetary allowances and benefits, the management, ownership, use, exploitation, disposal or encumbrance of state and local government assets, the acquisition of any rights relating to such assets as data of public interest, as well as any data whose disclosure or publication is required by a separate law in the public interest.

On the basis of these provisions, therefore, data relating to contracts concluded with the State, local authorities or their organs are considered to be data in the public interest and accessible to anyone.

Section 30(7) of the Privacy Act allows organs performing public tasks to fulfil requests for access to data intended for a comprehensive, invoice-level or itemised checking of their financial management by alternative means of their choosing.

In the Authority's view, the mere fact that the data request is aimed at accessing copies of invoices does not, in itself, render a reference to Section 30(7) of the Privacy Act lawful; furthermore, Section 30(5) of the Privacy Act must also apply in this case, pursuant to which, if an Act allows the controller discretion as to whether to refuse compliance with requests for access to data of public interest, the grounds for refusal shall be interpreted in a restrictive way, and compliance with the request for access to data of public interest may be refused only if the public interest in refusal outweighs the public interest in compliance with the request for access to the data of public interest.

The Authority further emphasised that Section 30(7) of the Privacy Act does not serve as an automatic ground for refusal for organs performing public tasks; therefore – as in all other cases – the organ performing public tasks must be able to justify the circumstances that permit the application of this provision.

Section 30(7) of the Privacy Act states that "access to data for the purpose of comprehensively checking, on invoice level or systematically, the financial management of organs performing public duties shall be governed by the provisions of separate Acts". However, given that the local authority had not fully com-

plied with its fundamental disclosure obligation, the local authority, by invoking Section 30(7) of the Privacy Act, unnecessarily and disproportionately restricted individuals' fundamental right to access and disseminate data of public interest Following the Authority's request, the local authority – in accordance with prior arrangements with the petitioner – granted access to the data by way of inspection. [NAIH-611/2025.]

2. Publication of contracts of a business organisation owned by a local authority

In one case, the petitioner argued that a limited liability company (hereinafter: the Company) performing a public service and wholly owned by the relevant local authority is obliged to publish the full text of all its contracts on its website, going back two years. The submission highlighted that the Company also possesses the following data: 1. Data on the volume, price, pricing and flexibility terms of electricity and natural gas trading contracts, as well as data on committed capacities; 2. Commercial, financial and technical data relating to contracts for the procurement of electricity and heat.

The petitioner requested the Authority's statement on whether the Company (whose main activity is steam supply and air conditioning) is obliged to publish the data under its control that are of public interest and, accessible on the grounds of public interest – in this case, exclusively the contracts referred to above – in their entirety on its website, or whether, pursuant to Section 27(3) of the Privacy Act and Sections 7/I(2) and (3) of Act CXXII of 2009 on the more economical operation of publicly owned business organisations, to refuse or omit to disclose information regarding these contracts where the acquisition or disclosure of such information by others would cause disproportionate harm to the company's business activities.
The Authority found that, as an organ performing a public function under Section 32 of the Privacy Act, the Company is also obliged to facilitate and ensure the prompt and accurate provision of information to the public and to data requesters. To this end, the data of public interest at its disposal must be disclosed to any data requester or, in the present case, published. Nevertheless, pursuant to Section 30(1) of the Privacy Act, if a document containing data of public interest also contains data that may not be disclosed to the public, the non-disclosable data must be rendered unrecognisable on the copy. In light of this, the Authority's response to the query stated that data properly classified as trade secrets may

be redacted provided the above conditions are met and that this does not prevent access to the data of public interest.[12] [NAIH-12974/2025.]

3. A request for data of public interest received by a business entity wholly owned by a local authority

The company requesting the opinion indicated that the data requester had "referred to *"Part II, Point 11 of Annex 1 of the Privacy Act, according to which the technical specifications of tenders issued by organs performing public tasks, their results and justifications must (should) be published with continuous retention, and the previous version must be kept in the archives for one year"*.

Pursuant to Section 2(1) of Act CXXII of 2009 on the more economical operation of publicly owned companies (hereinafter: Taktv.), a publicly owned company is obliged to publish, based on data existing at the time of publication, the remuneration of senior officers, members of the supervisory board, employees in managerial positions as defined in Section 208 of Act I of 2012 on the Labour Code (hereinafter: Mt.), and employees authorised to sign on behalf of the company or to dispose of its bank account. The published data may not be removed for two years following publication.
The details of employees of a local government-owned company as set out above are therefore classified as data accessible on the grounds of public interest under the Taktv., and are thus accessible to anyone in accordance with the rules of the Privacy Act regarding access to data of public interest. However, in the case of data accessible on the grounds of public interest, the Privacy Act distinguishes between the accessibility and the dissemination or publication of such data. Such data may be published in accordance with Section 26(2) of the Privacy Act, i.e. made available to anyone, for example on a website. Data accessible on the grounds of public interest may be disseminated in compliance with the principle of purpose limitation, i.e. they may be transferred to third parties; the data requester must also be made aware of this. In the case of employees, the above data request may be fulfilled if the employee concerned falls within the scope of Section 26(2) of the Privacy Act, i.e. is classified as a person acting within the scope of the tasks and powers of an organ performing a public function. Otherwise, anonymised or aggregated data may be provided. In the Authority's view, among persons employed by publicly owned companies, senior officers and employees in managerial positions, their deputies, the chair and members of the supervisory board, employees authorised to sign on behalf

12 https://www.naih.hu/dontesek-infoszab-allasfoglalasok/file/1241-onkormanyzati-tulajdonban-allo-gazdasagi-tarsasag-kozzeteteli-kotelezettsege

of the company or to manage bank accounts, and employees holding positions at the head of organisational units directly responsible for the performance of public tasks, or those in positions deputising for them, the public interest in the disclosure of the above data may be established. Furthermore, the announcement of job vacancies also falls within the scope of tenders; the law makes no distinction regarding the categorisation of individual tenders. At the same time, the Authority considers it good practice in the case of job vacancies for the results and reasons to be published in general terms, without personal data. (For example, that the advertised job vacancy was successful and one person was recruited, or that the tender for the vacancy was unsuccessful and the post was not filled. The reason being whether the applicant met or did not meet the application criteria.)
The data requester's reference to point 11 of Section II of Annex 1 to the Privacy Act is not necessarily accurate, as there are certain positions/roles that can be filled without a recruitment process, and during the selection process, alongside objective criteria (qualifications/education, professional experience) may be complemented by subjective factors (such as personal rapport), which are not necessarily recorded. Furthermore, not all employees of a local authority-owned company fall within the scope of the provisions on public access and transparency.
In the context of data retention, there is a distinction between publication and the actual processing of data. Applications must be updated on an ongoing basis, but data already published must be retained for one year retrospectively, so that it remains accessible for one year either in an archive or on the active interface; however, reference must be made to the data's validity, its timeliness in relation to the specific publication period, and its validity. At the same time, once the publication period has elapsed, the data (depending on its type) must still be available to the data controller in accordance with the provisions of legislation and records management rules, and the data controller must provide information about it upon request. Furthermore, it is a lex specialis rule that the data referred to may not be removed for two years following publication. [NAIH-15353-2/2025.]

4. Submission of a request for data of public interest without providing genuine personal data (name)

The complainant objected that a mayor's office had refused to comply with his request for data of public interest that the refusal did not include information on legal remedies, and that the municipal executive had investigated his identity; in his view, this is expressly prohibited by established case law on freedom of information. In the complainant's view, the data request included the name of the

petitioner, ‘anyone’ (Dr Elüldözött Ügyvédúr – Dr. Prosecuted Lawyer), as well as the contact details for the release of the requested data (aljegyzo.[...]@gmail.com). The complainant objected that the refusal did not contain any registration details (case number, reference number, case handler, etc.), thereby raising the question of whether the controller lawfully complies with the mandatory annual statistical reporting to the Authority regarding requests for data of public interest, and whether it has regulations setting out the procedure for fulfilling requests for access to data of public interest, as these cannot be found on the municipality’s website. In the data request sent to the mayor’s office, the complainant requested the provision of the prior data protection notice and the full data protection register in relation to all data processing activities. In his response, the municipal executive did not send the requested data to the complainant on the basis of a data request submitted without a name, in accordance with Section 29(1b) of the Privacy Act. During its investigation, the Authority established that, in his request for data of public interest, the complainant, in accordance with the provision of Section 29(1b) of the Privacy Act, had provided his identity using a name and address that could not be identified (specifically, an address that was not authentic based on its description, using the name of an organ performing a public function) , therefore, with reference to the mayor’s office, pursuant to Sections 3(1), 3(1a) and 3(2) of the Privacy Act, and on the grounds for exemption set out in Section 29(1b) of the Privacy Act, the data request was lawfully and justifiably rejected, therefore, the Authority rejected the part of the complaint concerning the rejection of the request for data of public interest, without examining the merits of the case, on the grounds that it was manifestly unfounded. Despite the lack of information on legal remedies, the complainant turned to the Authority for redress; therefore, the Authority assessed the lack of information on legal remedies as a minor infringement of rights and rejected the part of the complaint relating to the lack of information on legal remedies without substantive examination. The Authority thanked the complainant for their report, considered the justification for any ex officio proceedings that might be initiated on this basis, and drew attention to the fact that the use of an email address created using the name of an official organ performing a public function may even entail criminal law consequences. [NAIH-3829/2025.]

III.4. Public access to environmental data

1. Rejection of requests for environmental information on the grounds of administrative proceedings

In 2025, among the legal grounds for rejecting requests for environmental information examined by the Authority, Section 27(2)(g) of the Privacy Act stood out by far; controllers referred to this provision in almost every case. Rejections were made automatically by referring to the aforementioned provision and citing the Curia's judgment No. BH 2024.9.208, without carrying out the balancing test required under Section 30(5) of the Privacy Act. The controllers also invited the petitioners to submit requests for access to documents.

Two complaints were also received regarding the rejection of requests for access to the report on the environmental inspection carried out at the Samsung factory in Göd on 4 March 2025 (hereinafter: the Report), and to documents containing the findings and conclusions of the investigation, as well as to the laboratory and other test documents forming the basis of those findings and conclusions [NAIH-9775/2025., NAIH-10276/2025.]

In both cases, the Authority called upon the government office to disclose the data, finding that the right of access to information of public interest had been infringed as follows.
The staff of the environmental protection authority recorded the findings of the annual supervisory inspection conducted pursuant to Section 22 of Government Decree No. 314/2005 (XII.25.) on environmental impact assessment and the integrated environmental permit procedure (hereinafter: Government Decree) in the Report. The Government Office therefore examined whether the provisions of the integrated environmental permit were being complied with during the operations of the environment user. The Report also refers to the authorisation granted under Section 99 of the Code of General Administrative Procedure. Under this provision, the authority – within the limits of its powers – verifies compliance with the provisions of the legislation and the fulfilment of the requirements set out in the enforceable decision.
The Report contains findings as to whether the technologies in operation have changed compared to those set out in the integrated environmental permit, whether there was any disruptive noise impact or odour nuisance in the vicinity of the site, and whether the storage of hazardous waste generated on site was appropriate; it also includes the environmental risk assessment in accordance with Annex 15 of the Government Decree. The Report makes numerous findings

regarding air protection, for example concerning the emission of solid, non-toxic dust, changes in its quantity, and whether carcinogenic substances were emitted. The Report also sets out the monitoring measures and findings regarding noise and vibration protection, and describes the monitoring system and data measured in boreholes in relation to the protection of the geological environment and remediation. With regard to waste management, it reviews, among other things, the collection, storage and transport of hazardous and non-hazardous waste generated, as well as the operation of the site of the partner contracted by the environment user.

The Authority found that – contrary to the assessment of the Government Office – the data recorded in the Report constitute environmental information within the meaning of Section 2 of Government Decree No. 311/2005. (XII. 25.), as the Government Office, in the course of its on-site inspection, examined compliance with environmental legislation, recorded its findings in a report, i.e. took measures relating to the environment, and the Report contains a significant amount of data relating to measures taken to protect the environment and environmental elements, as well as emissions into the environment.

At the time of the data request, the official inspection had already been concluded, the Report was ready and available, and was in the possession of the Government Office. The data in the Report were generated in connection with the activities of the Government Office; therefore, they are clearly data of public interest pursuant to Section 3(5) of the Privacy Act. Pursuant to Section 98 of the Code of General Administrative Procedure, its provisions relating to administrative proceedings shall apply to official inspections, subject to the exceptions set out in its Chapter VI. According to the Authority's consistently held position, the purpose of the restriction permitted by law under Section 27(g) of the Privacy Act does not apply to administrative proceedings that have already been concluded[13], furthermore, Section 33(3) of the Code of General Administrative Procedure "*specifies only those types of data whose disclosure is subject to conditions. According to the NAIH's position, with regard to data of public interest and data accessible on the grounds of public interest, this section does not contain any restriction; in its interpretation, the legislation requires only that personal data or other protected data be rendered unidentifiable*" [14].

In its decision No. Pfv.IV.20.452/2025/5, the Curia expounded with regard to judgment No. Pfv.IV.20.384/2024/5 cited by the Government Office, that "*In that case, the Curia interpreted Section 33(1)-(3) of the Code of General Administrative Procedure and Section 27(2)(g) of the Privacy Act in relation to access to the documents of an ongoing administrative procedure.[…] In relation*

13 Report of the Nemzeti Adatvédelmi és Információszabadság Hatóság on its activities in 2018; p. 119

14 Report of the Nemzeti Adatvédelmi és Információszabadság Hatóság on its activities in 2018; p. 119.

to the ongoing administrative proceedings, it emphasised that 'data of public interest and data accessible on the grounds of public interest in individual administrative proceedings, which may be accessed by third parties, are contained in the decision concluding the proceedings pursuant to Section 33(5) of the Code of General Administrative Procedure, which may be accessed by anyone'[15]*, and it was also established that "the fulfilment of a request for data of public interest arising from a concluded administrative procedure cannot be refused on the basis of Section 27(2)(g) of the Privacy Act and Section 33(5) of the Code of General Administrative Procedure.*" In its decision No. Pfv.IV.20.384/2024/5, the Curia considered that **procedural fundamental rights were at risk during administrative proceedings, not in the case of concluded proceedings**. The data requests sought a report produced in a concluded administrative inspection; therefore, the Government Office's reference to the Curia's judgment No. Pfv.IV.20.384/2024/5 was not valid from this perspective either.

The Authority emphasised that data requests concerning environmental information contained in the files of an administrative procedure cannot be automatically rejected on the basis of Section 27(2)(g) of the Privacy Act, because Section 27 (2)(g) of the Privacy Act must be interpreted in a manner consistent with Directive 2003/4/EC of the European Parliament and of the Council of 28 January 2003 on public access to environmental information and repealing Council Directive 90/313/EEC (hereinafter: the Directive) and the Convention on Access to Information, Public Participation in Decision-making and Access to Justice in Environmental Matters, adopted in Aarhus on 25 June 1998 (hereinafter: the Aarhus Convention). This was also established by the Budapest Court of Appeal in its judgment No. 9.Pf.20.384/2025/11-II dated 11 November 2025: "*The provision of access to environmental information is required not only by an international treaty, namely the Aarhus Convention, which was promulgated by an Act, but also by an EU legal act, Directive 2003/4/EC; hence the Act on Environment Protection and the Privacy Act must be interpreted accordingly by the appliers of the law*[16]*.[…] There is therefore no doubt that the Privacy Act applies to environmental information. However, Section 27(2)(g) of the Privacy Act cannot be interpreted as being contrary to the exceptions set out in Article 4 of the Directive*[17].

In view of the above, the Authority drew the Government Office's attention to Case C/ACCC/C/2010/51 of the Aarhus Compliance Committee, which states

15 Kúria Pfv.IV.20.452/2025/5, [45]
16 [66]
17 [68]

that the term 'proceedings' in Article 4 (4)(a) of the Aarhus Convention is to be interpreted as referring to specific events – such as meetings or conferences – and not to all acts of the authorities. The Authority highlighted the finding in Case C-266/09 of the Court of Justice of the European Union (hereinafter: CJEU) that the balancing of the public interest served by making environmental information available against the individual interest served by refusing access must be carried out before the competent authority in every individual case, even if the national legislature has laid down criteria in a general provision which ease this comparative assessment of the interests at stake.

The findings of the CJEU's judgment in Case C-84/22[18] highlighted by the Authority emphasise that "*in order to determine whether the refusal of access to information falling within the scope of that exception is justified, the weighing of the interests involved, namely those which oppose disclosing that information and those which justify disclosing it, must be tightly controlled', whereas the exception relating to 'deliberations of the authorities' applies only to the exchange of information within a very specific context. This exception allows Member States to protect only that information which relates to the final stages of the authorities' decision-making process", the exception provided for in respect of 'deliberations of public authorities' does not allow for the rejection of a request for access to environmental information relating to 'information on emissions into the environment'. The CJEU further emphasises that 'where the information requested does not relate to emissions into the environment, the competent national authorities must, pursuant to the second sentence of the second subparagraph of Article 4(2) of Directive 2003/4, weigh the public interest served by making that information available against the interest served by refusing access. Such a balancing of interests is also necessary where, in cases where the exception relating to 'deliberations of public authorities' does not apply, the exception relating to internal communications provided for in Article 4(1), first subparagraph, point (e) of Directive 2003/4 applies. […] Article 4(4)(a) of the Aarhus Convention provides that a request for environmental information may be refused where disclosure of the information would undermine the confidentiality of administrative proceedings – where such confidentiality is provided for by national law – rather than the administrative procedure as a whole, which concludes with the deliberations of those authorities*."

Restrictions on the disclosure of environmental information handled in administrative proceedings are therefore permitted only in a limited scope [Section

18 Paras [50]-[55]

27(2)(g) and Sections 27(5) and (6) of the Privacy Act must be applied with this in mind]:

- in the case of documents under preparation: these are documents on which the authority is still actively working; if the authority is no longer actively working on the document, it may be released, even if no decision has yet been made in the procedure to which it relates[19];
- internal communications of the authorities: factual material does not fall within this category, even if it is under preparation; the opinions of specialist authorities (authorities with the right to give an opinion) are also not considered internal communications within a decision-making process. Studies commissioned by the authorities from organs independent of the authority cannot be considered internal communications either; information shared by the authority with third parties cannot be classified as internal communication[20]; this is a broader exception, applicable at every stage of the authority's work, but the weighing of the interests at stake – that is, the interests against disclosure and the interests justifying it – must be strictly defined;
- where the confidentiality of administrative proceedings is prescribed by national law, this should not be understood to refer to the proceedings as a whole, but rather to the individual deliberations concluding the proceedings.

Therefore, in the Authority's view, an interpretation of Section 27(2)(g) of the Privacy Act, according to which:

- the disclosure of all environmental information dealt with in an administrative procedure may generally be excluded on the grounds of the administrative procedure;
- it is permissible to exclude the disclosure of information relating to emissions into the environment on the grounds of official deliberations;
- only the environmental information contained in the decision concluding the procedure is public; however, further environmental information processed in the administrative procedure is not public;
- when assessing the disclosure of environmental information contained in the administrative procedure file, the authorities are not obliged to balance the public interest served by disclosure against the interest served by refusal

19 Aarhus Convention: An Implementation Guide (second edition), p. 85, translation by the Authority
20 Aarhus Implementation Guide, p. 85, translation by the Authority

is not in accordance with Article 4 (3)(c) and (4)(a) of the Aarhus Convention and Article 4(1)(d) and (e) and Article 4(2)(a) of the Directive.

The Authority emphasised that it is made clear not only by the Aarhus Convention and the Directive, as well as the relevant EU case law, but also by Section 30(5) of the Privacy Act and the practice of the Constitutional Court, that a formal reference to the statutory provision permitting refusal is not sufficient; a balancing of interests must be carried out in relation to the requested data. The authorities must therefore examine whether the conditions laid down by law for restricting the disclosure of the requested data are met; in other words, a formal reference to a ground for restricting disclosure is not sufficient, and the actual existence of substantive justification for the restriction must be examined in relation to the requested data. The Constitutional Court summarised the aforementioned conditions for the lawful restriction of access in paragraph 43 of its Decision 4/2021 (I.22.) AB (hereinafter: the Decision), and emphasised that ***"a restriction on public access is legitimate only if the disclosure of the data in question could realistically undermine a constitutionally recognised objective***".
Paragraph [48] of the Decision emphasises that "***[o]verall, therefore, it can be stated that restrictions on freedom of information never arise automatically by virtue of the law: they always require an intervention by the controller****. This provision may be regarded as the essence and principal guarantee of the freedom of information, extending to all three types of restriction (classified data, data forming the basis of a decision, and withholding under a separate law). It is therefore not constitutionally possible to withhold data directly by law*".

In the balancing of interests under Section 30(5) of the Privacy Act, significant weight must be given to whether the data request relates to environmental information. Making environmental information widely accessible is essential for the enforcement of the right to a healthy environment guaranteed in Article XXI(1) of the Fundamental Law. Furthermore, when weighing up interests, account must be taken of the specific nature of administrative procedures concerning environmental information, namely that the decisions affect a wider circle of people than just the parties to the proceedings. The Authority shares the view expressed in the judgment of the Budapest Court of Appeal No. 9.Pf.20.384/2025/11-II, according to which "*in some administrative proceedings, the circle of those affected is clearly definable and there is no public interest involved; these primarily contain personal data rather than information of public interest. However, another part of these procedures is aimed at authorising activities involving significant use of the environment or affecting a significant, often difficult-to-define section of society (e.g. railways, motorways, major construction projects, battery facto-*

ries, power stations, mining licences, etc.), and contains data of public interest in this context. These have an impact even beyond the broadly interpreted circle of clients under the Code of General Administrative Procedure. Public debates concerning the official authorisation of such activities constitute one of the most important aspects of the free discussion of public affairs. According to the Court of Appeal, these debates are unnecessarily and disproportionately restricted by a legal interpretation which, by invoking the right of access to documents, makes it impossible to obtain and publicly discuss such fundamental and public-interest information as what has been authorised and on the basis of which plans".

In both cases, the Authority emphasised that there is a significant public interest in the disclosure of data relating to official inspections examining compliance with environmental legislation, particularly in the case of environment users that generate large quantities of hazardous waste and are classified as upper-tier establishments handling hazardous substances. [NAIH-9775/2025., NAIH-10276/2025.]

In one case, the complainant requested information from the local municipal executive regarding measures taken by the municipal executive concerning a motocross track operating near their place of residence. The municipal executive had carried out noise measurements both ex officio and in response to a complaint, and had taken noise protection measures; however, he did not provide the complainant with any further information on these matters. He argued that the complainant did not qualify as a client and that the requested data constituted 'working documents', and therefore refused to comply with the data request. The Authority ordered the municipal executive to comply with the complainant's data request and to send him the noise measurement results forming the subject of the request for data of public interest, together with the municipal executive's decisions based on them. In its opinion, the Authority summarised the Constitutional Court's case law regarding the concept of preparatory working documents, the constitutional limits on restricting access to information on this ground, and the statutory provisions concerning the disclosure of environmental data. The municipal executive complied with the request [NAIH-10360/2025.]

III.5. Access to data of public interest generated in administrative proceedings

1. Data relating to the Samsung factory in Göd

The petitioners submitted their data request as follows:

- "*Please be so kind as to send me an electronic copy of the building permits issued to the Göd site of Samsung SDI Magyarország Zrt. (2131 Göd, Schenek I. u. 1.) from 1 January 2023 until the date of this data request.*
- *Please kindly send me an electronic copy of the environmental declaration for the year 2023 submitted by the Göd site of Samsung SDI Magyarország Zrt. (2132 Göd, Schenek I. u. 1.) to the Government Office, which contains all data submitted by Samsung SDI Zrt. relating to air, surface and groundwater, and waste (emission quantities).*
- *Please could you send me an electronic copy of the decisions containing sanctions (warnings, fines, orders) issued by the Government Office from 1 January 2023 to the date of this request regarding the Göd site (2132 Göd, Schenek I. u. 1.).*"

In all three cases, the Government Office refused to disclose the data, citing the following:
"*It is not possible to comply with the data request pursuant to Section 27(2)(g) of the Privacy Act, taking into account the provisions of the Curia's decision published under reference number BH 2024.9.208. A request for the inspection of the documents may be submitted in accordance with the provisions of Act CL of 2016 on the Code of General Administrative Procedure*."
The Authority launched an investigation, in the course of which it made an enquiry to the government office responsible for processing the data. In response to the enquiry, the government office stated that it had complied with the requests for data. [NAIH-1987/2025.]

2. Access to documents relating to the designation of a listed building

The data request was formulated as follows:
"*I request copies of the relevant official decisions in electronic form in relation to the protected heritage assets known as the Hatvanpuszta Manor complex, granary and stables, registered under heritage number …*

- *the declaration of protection,*
- *changes to the level of protection,*

– *and decisions of significance from a heritage protection perspective (e.g. removal from the register, lifting of restrictions, etc.)"*
–

The Ministry refused to comply with the request. It based its refusal on Section 27(2)(g) of the Privacy Act – taking into account the provisions of the Curia's decision published under reference number BH 2024.9.208 – and here, too, drew the citizen's attention to the possibility of submitting a request for inspecting the documents in accordance with the Code of General Administrative Procedure. The Authority initiated an investigation; however, it became aware of a fact (court proceedings are pending) in respect of which it was obliged to discontinue the proceedings. [NAIH-11217/2025.]

3. The Authority's position on the applicability of the rules of the Code of General Administrative Procedure in connection with the fulfilment of requests for data of public interest

Freedom of information, as a fundamental right, is not absolute. This means that it may be subject to restrictions, and in certain cases, access to data of public interest or data accessible on the grounds of public interest may even be excluded. The cases in which access may be restricted are set out in Section 27 of the Privacy Act.
Pursuant to Section 27(2) of the Privacy Act, the right of access to data of public interest and data accessible on public interest grounds may be restricted by an Act, with the specific type of data indicated, if considered necessary for the purposes of

a) national defence;
b) national security;
c) the prosecution or prevention of criminal offences;
d) environmental protection or nature preservation;
e) central financial or foreign exchange policy;
f) external relations, relations with international organisations;
g) court proceedings or administrative authority proceedings;
h) intellectual property rights;
i) cybersecurity.

The Authority emphasises that Section 29(3) of the Privacy Act provides that the applicant may obtain a copy of a document or part of a document containing data, regardless of the manner in which it is stored. *Under current legislation, all data held by organs performing public tasks and relating to their activities, which do not constitute personal data, are data of public interest, regardless of whether*

their disclosure is restricted. With regard to individual documents, it is the data principle, not the document principle, that applies.
In practice, this means that a single document may contain personal data, classified information, protected knowledge, trade secrets or data used in the preparation of decisions; however, a request for access to an entire document cannot be refused on the basis of these; pursuant to Section 30(1) of the Privacy Act, any data that cannot be disclosed must be rendered unrecognisable in the copy. This follows clearly from the Fundamental Law itself and from the terminology used in the Privacy Act.

Pursuant to Section 27(2) of Act CL of 2016 on the Code of General Administrative Procedure "*The authority shall ensure that no secrets, or other data, protected by an Act (hereinafter jointly "protected data") are disclosed to the public or become known to unauthorised persons and that the protection of such protected data is guaranteed in the course of the procedure by the authority.*"
Pursuant to Sections 33(4) and (5) of the Code: "*In the course of inspection of documents, the person entitled thereto may make copies or excerpts or he may, for a fee specified in a government decree, request copies which shall, upon request, be authenticated by the authority*.
If no Act restricts or excludes access to the decision then, following the conclusion of the procedure, a version of the conclusive decision with administrative finality not containing any personal data or protected data, as well as the procedural decision annulling the conclusive decision of first instance and instructing the authority which adopted the conclusive decision of first instance to carry out a new procedure, may be accessed by anyone without restriction."

However, public organs have very significant obligations even in the event of a refusal to provide data. Section 30(3) of the Privacy Act stipulates that "*a refusal to comply with a data request, along with information as to the reasons therefor and the legal remedies available to the requesting party under this Act, shall be notified to the requesting party in writing or, if the requesting party has provided an electronic mail address in the request, by electronic mail within 15 days of the receipt of the request.*"

In the Authority's view, data must be disclosed in accordance with the Code of General Administrative Procedure, such that any non-identifiable data in documents containing protected data and personal data (e.g. the name of the data subject's mother) must be redacted; copies of these documents must then be made, which may be disclosed to the petitioner.

Section 30(5) of the Privacy Act and the practice of the Constitutional Court also make it clear that a reference to the statutory provision allowing for refusal is not sufficient; a public interest test must be carried out in relation to the requested data. The authorities must therefore examine whether the statutory conditions for restricting the disclosure of the requested data are met; in other words, a formal reference to a ground for restricting disclosure is not sufficient, and the actual existence of substantive justification for the restriction must be examined in relation to the requested data. The Constitutional Court summarised the aforementioned conditions for the lawful restriction of access in paragraph 43 of its Decision 4/2021 (I.22.) AB (hereinafter: the Decision), and emphasised that 'a restriction on access to information is legitimate only if the disclosure of the data in question could realistically undermine a constitutionally recognised objective'. Paragraph [48] of the Decision emphasises that "*Overall, it can therefore be stated that a restriction on freedom of information never arises automatically by virtue of the law: it always requires the intervention of a decision by the controller. This requirement may be regarded as the essence and principal guarantee of the freedom of information, extending to all three types of restriction (classified data, data forming the basis of a decision, and withholding under a separate law). It is therefore not constitutionally possible to withhold data directly by law*".

Thus, based on the practice of the Constitutional Court, an organ performing a public function must, in its decision to refuse a data request, demonstrate the grounds on which it reached the conclusion that the public interest in the disclosure of the documents sought by the petitioner is outweighed by the interest in excluding the public, if it rejected the data request by referring to Section 27(2) (g) of the Privacy Act, even though this provision does not directly provide for the imposition of a restriction on disclosure, it presupposes the existence of a sector-specific statutory rule establishing the criteria for restricting disclosure and the performance of the related public interest test.

In the Authority's view, the provisions of the Code of General Administrative Procedure. relating to access to documents contain provisions restricting access only in respect of personal data and protected data in the case of third parties exercising their rights – such as petitioners exercising their right to access data of public interest.

III.6. Certain other significant investigation cases of the Authority

1. Child protection – cases concerning the transparency of the child protection institutional system

A complainant approached the Authority objecting that, despite the extension of the response deadline, the child protection specialist care institutions providing residential care – numbering several dozen – had failed to respond to his requests for data of public interest.

The data requests sent to the institutions covered twenty data categories, including the number of places available, the number of children currently in care, the number and addresses of residential homes belonging to the institution, the type of the institution's professional programme, as well as data on the trend in the number of employees for the period 2020–2025, the number of vacant posts and average wages broken down by job category, and grants received for staff retention or training, disciplinary or criminal proceedings initiated against employees between 2020 and 2025, child protection reports concerning the institutions, complaints or the type and subject matter of deficiencies identified in official investigations, the number of extraordinary incidents, and records relating to peer abuse, prostitution or drug use.

Given that the data specified in the petitioner's request for information are data of public interest, by extending the deadline for compliance, the institutions also acknowledged that the data are in their possession and that access to them is not subject to restriction, – and that compliance within 15 days would encounter the obstacle referred to in Section 29(2) of the Privacy Act – and because, according to the documents attached to the submissions, the institutions' notification letters regarding the extension of the compliance deadline were entirely consistent in both content and timing, the Authority, pursuant to Section 54(1)(e) of the Privacy Act[21], requested the State Secretary responsible for care policy at the Ministry of the Interior to conduct an investigation at all institutions and to call upon them to provide a comprehensive and detailed response covering all questions raised in the data requests that were the subject of the complaints. The Authority requested the Ministry of the Interior to inform the Authority of the institutions' consolidated response.

21 Section 54(1) of the Privacy Act In the course of the inquiry, the Authority
(…)
e) shall have the right to urge the head of the organ supervising the controller authority to conduct an inquiry.

The institutions' reply letters – apart from the data provided in response to three questions – remained entirely identical in content regarding the refusals; therefore the Authority also informed the Ministry of the Interior of its position regarding the stated grounds for refusal, and again requested the Ministry to call upon the institutions to provide a comprehensive and detailed response covering all questions raised in the data requests that were the subject of the complaint. The investigation is ongoing. [NAIH-17125/2025]

2. Disclosability of data collected in the course of performing public education duties – data serving as the basis for a decision

Citing existing grounds for restriction regarding data used to support decision-making, the Ministry of the Interior refused to disclose data relating to the results of responses to parental questionnaires sent via the Kréta system in December 2022, December 2023 and October 2024. The petitioner requested the percentage of responses given for each of the answer options provided for the individual questions, the number of respondents for each question, and, for the specified questions in each year, which of the text-based responses represented the most common opinions and how many respondents had submitted them.
In its requests and report, the Authority explained that the Ministry is under an obligation to provide a detailed substantive justification; that is, it must specify precisely which decision to be taken in which ongoing procedure the requested data of public interest is intended to support, and, in this regard, to what extent the disclosure of the data of public interest would influence the decision-making process, and thus whether it would frustrate the effective implementation of the decision or render impossible the independent, effective work of civil servants free from unauthorised influence. Furthermore, this ground for refusal may only be invoked in relation to a specific decision. With regard to the preparatory data for decisions already taken, the general rule is public access, whilst future decisions must be identifiable decisions to be taken in the near future; the Ministry's general reference to unspecified future decisions cannot be accepted as an obstacle to the disclosure of the data.

In its response to the Authority's request, the Ministry merely listed the purposes for which the answers to the individual consultation questions could be used. It did not refer to any specific decision or measure – whether already taken or planned – in connection with numerous questions in the questionnaire; thus, the link between the data and the decision was not sufficiently direct and specific. The Ministry was unable to establish any reason why the data sought by the petitioner could not be disclosed. The disclosure of data of public interest may only

be refused on the grounds of data used for decision-making if the controller can demonstrate a specific risk[22]. The Ministry's response did not contain any justification that would, under the Fundamental Law, justify the restriction on access – for example, in the interests of upholding another fundamental right or protecting a constitutional value – according to which the restriction is strictly necessary, purpose-limited, proportionate, and respects the essential content of the fundamental right concerned. [NAIH-10695/2025]

The Authority issued a report in the two cases mentioned because neither the Foundation nor the Ministry of the Interior accepted the position clearly set out in the Authority's requests.[23]
A common feature of both previous cases was that the authorities examined the identity of the person requesting the data and the purpose of the request, even though, according to the provisions of the Fundamental Law and the Privacy Act, neither of these may be examined. Pursuant to Article VI(3) of the Fundamental Law of Hungary, the right to access and disseminate data of public interest is a fundamental right to which everyone is entitled. Under the Privacy Act, anyone may exercise this right by submitting a request for access to data of public interest. Ensuring freedom of information is a fundamental obligation of organs performing public tasks. To this end, organs performing public tasks are obliged to fulfil requests for information addressed to them impartially and professionally, without inquiring into the reasons or purpose of such requests. It can generally be stated that the less transparent public organs make their activities and financial management through electronic publication, the more and the more detailed individual data requests they will have to fulfil.

3. Transparency of public interest asset management foundations performing public tasks (KEKVA)

Public interest asset management foundations (hereinafter: KEKVA) are organisations established with public funds, managing public funds and performing public tasks, and are therefore organisations falling within the scope of the Privacy Act, which are obliged to ensure transparency and provide information both by virtue of their performance of public tasks and their management of public funds. Not all of these investigations have yet been concluded, but the following points are worth highlighting from the Authority's calls for investigation.
In its request for information addressed to the Neumann János University Foundation, the complainant sought copies of the detailed minutes of the meet-

22 Kúria Pfv.20.509/2023/4.
23 https://www.naih.hu/jogi-szabalyozassal-kapcsolatos-allasfoglalasok-2026

ings of the Board of Trustees and the Supervisory Board, including the annexes, as well as the names, positions and remuneration of persons employed or contracted for the performance of work within the Foundation's organisation and copies of contracts, certificates of performance and accepted invoices relating to persons entrusted with legal representation.

The Foundation's reply letter contained four grounds for restricting access to data of public interest and data accessible on the grounds of public interest: reference to data serving as the basis for a decision, trade secrets, ongoing proceedings, and the protection of personal data.

Regarding the reference to data used for decision support, the Authority's position was that a reference to Sections 27(5) and (6) of the Privacy Act cannot be used as blanket grounds for refusal. During the investigation, it was established that the Foundation refused to comply with the data request without subjecting the submissions to a substantive review, nor did it fulfil its obligation to provide substantive justification in the case of the minutes; it merely referred formally to the decision-preparatory nature of the data, nor did it refer to a specific procedure or decision, and the link between the data and the decision was thus not direct or specific. With regard to references to data used in the preparation of decisions, the proposals and minutes must be examined individually and on a data-by-data basis to determine whether the legal conditions for referring to data used to substantiate a decision still exist, as it is unlikely that, based on data from proposals and minutes dating back several years, the decision on which the data sought to be disclosed could have been based has not already been taken.

With regard to the invocation of trade secrets, the Authority reiterated that data relating to public funds and public assets cannot constitute a trade secret.

Pursuant to Section 1 (Objectives and Principles) of Act IX of 2021 on public-interest asset management foundations performing public duty (hereinafter: Kekvatv.), the State, as a member, provides the Foundation with the assets and financial resources necessary for the performance of its public duties.

Any data that would otherwise constitute a trade secret of privately owned companies or private individuals in connection with a contract or grant entered into with an organ performing public tasks is classified as data accessible on the grounds of public interest under Section 27(3) of the Privacy Act. Resolving the conflict between trade secrets and freedom of information, Section 27(3) of the Privacy Act – in the interests of transparency in the management of public funds

– classifies data related to the use of the central budget, local government budget and European Union funds, to benefits and allowances involving the budget, to the management, possession, use, utilisation and the disposal and encumbering of state and local government assets, and to the acquisition of any right connected to such assets as data accessible on public interest grounds.
Copies of contracts concluded with persons entrusted with legal representation, invoices and certificates of performance must be made available to the notifying party in such a way that neither the name of the agent (name, company name) nor the agency fee and the amounts of individual payments and invoices can be obscured. The Authority also drew the Foundation's attention to the fact that, in the disclosure section specified in point III.4 of Annex 1 to the Privacy Act, it is not sufficient to state the hourly rate for contracts concluded with law firms for legal advice; rather, the total amount of the consideration calculated on an annual basis must be indicated.

With regard to personal data accessible on the grounds of public interest, the Authority stated: organs performing public tasks act in accordance with the principle of transparency if they inform their contracting partners and employees in an appropriate manner, at the time of concluding the contract or commencing employment, about the processing of their personal data accessible on the grounds of public interest and the possibility of requests for data of public interest.

In the event that such information is not provided at the time of concluding the contract, the provisions of the Fundamental Law in force in Hungary and the Privacy Act shall nevertheless apply with regard to the accessibility of the contract's data. As the provisions of a contract may not conflict with Hungarian legislation, agency or employment contracts may not contain any clause restricting access to information regarding remuneration. The principle of integrity in public life always takes precedence over any perceived competitive disadvantage to the individual.

In accordance with the consistent practice of the Authority and the courts, data relating to the working conditions of persons acting within the scope of the duties and powers of organs performing public tasks – including the value of contracts concluded for the performance of public tasks – are classified as data accessible on public interest grounds under Section 26(2) of the Privacy Act as other personal data related to the performance of public tasks. All employees who assist in the performance of the tasks and powers listed in the legislation act within the scope of the Foundation's tasks and powers. Data concerning the names, posi-

tions and allowances of employees in posts related to the performance of public tasks are, in view of both their performance of public tasks and their remuneration from public funds, data accessible on public interest grounds, i.e. data accessible to petitioners.

In relation to data on ongoing proceedings, the Authority wished to make it clear that Section 27(2)(c) of the Privacy Act (restriction of access to information for the purpose of prosecuting and preventing criminal offences) may be invoked exclusively by the authorities conducting the proceedings, inter alia, in relation to data processed by them in connection with such proceedings. Data accessible on public interest grounds generated by the Foundation do not lose their public accessibility merely because they are used in criminal proceedings. If a petitioner has, for example, received data of public interest concerning the Foundation's financial management or contracts it has concluded prior to the commencement of criminal proceedings, they may lawfully disseminate such data even whilst the criminal proceedings are ongoing.

The Foundation may not invoke the provisions of Act XC of 2017 on the Code of Criminal Procedure in the context of refusing a request for data of public interest; the provisions of this Code may be invoked only by the court, the public prosecutor's office and the investigating authority, exclusively in the cases and for the reasons specified by law, and to the extent and for the duration necessary to achieve or ensure the objectives set out therein. [Section 109(2) of the Code of Criminal Procedure. [Section 109(2) of the Code of Criminal Procedure]

The petitioner did not request information about the criminal proceedings, but rather about the data of public interest and data accessible on the grounds of public interest on which those proceedings are based. Section 109(1) of the Code of Criminal Procedure authorises the court, the public prosecutor's office and the investigating authority to refuse to provide information solely for the purpose of protecting classified data, insofar as this is absolutely necessary.

Furthermore, within the framework of the balancing of interests prescribed in Section 30(5) of the Privacy Act, organs performing public tasks must attach particular weight to the fact that the requested data relate to a significant amount of public funds.

In the course of the investigations – following the Authority's request and summons – the Neumann János University Foundation provided, in a 73-page table, the factual and legal basis for redacting each piece of data in the individual min-

utes. It also informed the Authority that, in relation to a significant proportion of the minutes and proposals of the Board of Trustees and the Supervisory Board concerned in the present case, legal proceedings seeking access to data of public interest are currently pending before the Kecskemét District Court. [NAIH-14084/2025.]

4. Access to waste management concession contracts

During 2025, the petitioner submitted several submissions against companies engaged in waste management activities, as requests for information regarding contracts concluded with MOHU MOL Zrt. in connection with the performance of public waste management duties, specifically concerning public waste management services and institutional sub-activities, as well as the facilities they operate, and contracts concluded with the concessionaire's subcontractors, were rejected. The reason for the rejection in almost all data requests was that, from 1 July 2023, public waste management tasks will be performed by MOHU MOL Hulladékgazdálkodási Zrt. (hereinafter: MOHU) as the concessionaire, and that the company in question participates in the performance of these duties as a concessionaire's subcontractor. In view of this, and in accordance with Sections 53/A(1) and (2) of Act CLXXXV of 2012 on Waste (hereinafter: Waste Act) , the petitioner must submit the request for data of public interest to MOHU, as the business in question is not subject to a data reporting obligation, does not perform a public function, and the requested data are not data accessible on public interest grounds. During the investigation, in two cases the business undertaking carrying out waste management activities disclosed the data. In the other cases, the Authority called upon the relevant business undertaking to comply with the request for data of public interest and data accessible on the grounds of public interest. In its reasoning, the Authority pointed out that state waste management is a public service that must be used; where relevant, it identified municipal ownership from the ownership structure, and thus the management of national assets, and set out its position on trade secrets as a restriction on the disclosure of data of public interest. Typically, the business entities which invoked trade secrets as a restriction on the disclosure of data did not specify any interest to be protected, but merely referred to trade secrets in general terms; they did not substantiate any substantive restriction on disclosure, nor did they demonstrate that the legal conditions for trade secrets were met. [NAIH/12068/2025., NAIH/12069/2025., NAIH-12073/2025., NAIH-13450/2025., NAIH-12067/2025.]

In another case relating to a waste management concession, the notifier approached the Authority alleging that MOHU had failed to comply adequately with

a request for information of public interest, as it had redacted a significant portion of the documents sent and had not provided any justification for the non-disclosure of this information.
MOHU argued that the notifier's request for information was limited exclusively to contracts providing capacity for the sub-activity of public waste management services, the definition of which is set out in Section 2(26c) of the Waste Act , and stated that it had anonymised the data relating to the institutional waste management sub-activity in the documents issued to the notifier. MOHU referred to the fact that, based on the definitions in Section 2(26c) and 26b of the Waste Management Act, the public service sub-activity of waste management and the institutional sub-activity of waste management cover different activities, and the data request did not concern data relating to the institutional sub-activity of waste management; therefore, MOHU redacted the relevant data from the document. The Authority ruled that MOHU had complied with the data request and terminated the investigation. [NAIH/8388/2025.]

5. A publicly owned company's invocation of trade secrets

In their submission, the complainant alleged that MVM Főgáz Földgázhálózati Kft. (hereinafter the Company) had not properly complied with their request for data of public interest, as the total amounts had been redacted from the concession agreement sent to them. During the investigation, the Authority established that the Company is indirectly state-owned and, accordingly, manages and disposes of state assets and administers public funds. Pursuant to Article 39 of the Fundamental Law of Hungary, data relating to public funds and national assets constitute data of public interest. The Authority referred to Section 5(2) of Act CVI of 2007 on State Assets (hereinafter: Act on State Assets), which provides that any organ or person managing or disposing of state assets shall be deemed to be an organ or person performing a public function. During the investigation, the Authority established that, pursuant to Section 27(3) of the Privacy Act, access to the details of a contract may only be restricted on the grounds of business secrecy if this does not prevent the disclosure of data of public interest, and furthermore, the contractual amount cannot be the subject of business secrecy.
The Authority also pointed out that, whilst the Company had invoked the business secrets of the licensee as a contracting party in justifying the restriction on the disclosure of the data, it had failed to demonstrate what legal measures the licensee, as the holder of those secrets, had taken to safeguard its business secrets.
Furthermore, the Company failed to demonstrate that the disclosure of data of public interest would cause disproportionate harm, nor did it demonstrate what

kind of irreparable disadvantage it would suffer in relation to its competitors. The Authority ordered the Company to comply with the data request. Following the order, the Company complied with the data request. [NAIH/695-9/2025., https://naih.hu/dontesek-infoszab-allasfoglalasok

6. Access to data relating to the operation of the appointed and substitute defence counsel system

In May 2025, the petitioner civil society organisation submitted a request for data of public interest via the KiMitTud system to five police organisations regarding the operation of the appointed and substitute defence counsel system. The petitioner requested the following data, broken down by year for the period 2019–2024:

- the number of cases in which a decision was made to appoint a defence counsel,
- in how many cases a substitute defence counsel was appointed,
- information on the names of the appointed substitute defence counsels and, broken down by individual solicitors, the number of appointments as substitute defence counsel,
- statistical data, broken down by year, on the reasons for the appointment of substitute defence counsel.
-

In their data requests, the petitioner specifically referred to the judgment[24] of the European Court of Human Rights in the case of the Hungarian Helsinki Committee v. Hungary, delivered on 8 November 2016 , in which the **ECtHR held that the police stations' refusal to provide data on the number of appointments, broken down by the names of the appointed defence lawyers and by individual lawyers, was contrary to Article 10 of the European Convention on Human Rights**.

In their data requests, the petitioner also highlighted Articles 3, 4, 6 and 10 of Directive (EU) 2016/1919 on legal aid for suspects and accused persons in criminal proceedings and for requested persons in European arrest warrant proceedings.

Citing Section 30(2a)(b) of the Privacy Act (no obligation to produce new data) and the fact that "the Police do not collect data in the requested breakdown", the Police rejected the data requests.

At the request of the petitioner, an investigation was initiated against the Police, during which the controllers explained in detail how the appointment of defence

24 https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-167828%22]}

counsel and substitute defence counsel operates within the police document management system (Robotzsaru system), and

- *"with regard to the issues raised, it is possible to identify the assignments of substitute defence counsels in the Robotzsaru system by conducting a search based on file identifiers, followed by the collection of the names of the defence counsels and the legal basis for their assignment, and a detailed review of the files",*
- *"it would be possible to retrieve the data from the Robotzsaru system's database by entering complex search criteria,"*
- *but: „Querying data at database level regarding the assignment of defence counsel and substitute defence counsel would require specialist programming skills, meaning that police staff cannot directly retrieve data from the database.*"

Furthermore, the Police's position is that "*the obligation to provide data to the Commission set out in Directive 2016/1919 (Article 10 of the Directive) generally falls on the Member State in connection with the implementation of the Directive", and "the collection and provision of the detailed statistical data requested by the petitioner in relation to the appointment of defence counsel and the appointment of substitute defence counsel are not required.*"

The NAIH called upon the Police to respond to the petitioner's requests for data of public interest and to send the listed data to the petitioner.

In its reply dated early December 2025, the Police informed the Authority that it maintained its position regarding the data provision obligation set out in the Directive. However, following the Authority's request, "after technical adjustments", the Police provided the petitioner with the requested data in response to the query regarding the number of cases in which a decision was made to appoint a defence counsel.

According to the Police's argument, regarding data on substitute defence counsel, "*the existing problem is that, when drafting the decision to appoint a substitute defence counsel, the legal basis for the appointment selected on screen is stored by Robotzsaru until the document is authenticated; this information cannot be retrieved from the database*", and "*the data on screenings is distorted by the fact that the relevant amendment to Section 49(5) of Act XC of 2017 on the Code of Criminal Procedure*[25]*, has been in force since 18 June 2020; prior to that, substitute defence counsels were appointed in procedural acts*."

Pursuant to Section 30(2a)(b) of the Privacy Act, "*the organ performing public duties shall not be obliged to comply with the data request if complying with the*

25 The appointment of a substitute defence counsel remains in effect until the conclusion of the procedural act conducted in the defence counsel's absence. In the case of Section 47(1), the substitute defence counsel may act in procedural acts held in immediate succession until the appointed defence counsel appears or contacts the prosecuting authority or investigating authority.

request would necessitate (…) 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."
The Authority accepted the Police's position that, in view of the distorting factors and IT constraints, complying with the request would require a case-by-case review of a total of 54,463 cases[26] relating to assignments involving the Police (the five police units contacted), and a comparison of the data, which would place a disproportionate burden on the Police. [NAIH-13165/2025., NAIH-13166/2025., NAIH-13167/2025., NAIH-13168/2025., NAIH-14009/2025.]

26 Csongrád-Csanád VMRFK: 1809 cases; Szeged Police HQ: 5573 cases; Debrecen Police HQ: 3503 cases, Hajdú-Bihar VMRFK: 771 cases, BRFK: 42.807 cases.

IV. Cooperation with partner authorities in the European Union and international affairs

The most significant event for the NAIH in 2025 was the international conference[27] organised on 17 September 2025 to mark the 30th anniversary of the institution responsible for overseeing the enforcement of information rights, which was directly preceded by a meeting held behind closed doors, attended by supervisory authorities from Central and Eastern Europe. Last year, on the initiative of the Austrian data protection authority, the Czech, Slovenian, Slovak, Austrian and Hungarian data protection authorities held an informal meeting in Vienna, at which the heads of the data protection authorities exchanged information on the most common data protection, procedural and cooperation issues that pose daily challenges. In view of the success of the meeting, the Authority hosted the Central European meeting in 2025 and expanded the circle of participants by inviting the Croatian data protection authority. The event offered a unique opportunity to share our experiences and views on common challenges as well as new responsibilities and tasks relating to EU digital legislation.

Perhaps the most significant event of 2025 in the field of EU cooperation on criminal matters and justice is that, following many years of preparatory work, the European Union Entry-Exit System (Entry-Exit System, EES), established by Regulation (EU) 2017/2226, began operations on 12 October 2025, with a phased roll-out. In Hungary, live operations commenced on 12 October 2025 at Beregsurány on the Ukrainian–Hungarian border, followed later by the Serbian–Hungarian border sections; at airports, operations began slightly later: at Budapest Liszt Ferenc International Airport on 18 November and at Debrecen International Airport, and Hévíz-Balaton Airport in Sármellék between 18 and 20 November, respectively.

In addition to our regular participation in working groups run by the European Commission, we also took part in 2025, on behalf of the Hungarian supervisory authority, in the evaluation of Member States using the SIS, this year in Austria and Switzerland.

As the national supervisory authority for SIS, the NAIH conducted a comprehensive inspection at the Sirene Bureau and the BRFK 2nd District Police Station in 2025, which concluded with reassuring results.

27 https://naih.hu/30-evfordulos-nemzetkozi-konferencia/beszamolo-az-esemenyrol

An important organisational change within the Authority is the establishment, on 1 January 2026, of the new Digital Data Strategy Department, which primarily addresses tasks arising from EU digital legislation that affect the NAIH.

In 2025, the Authority established the AI Lab, which is currently being set up. As part of this, six colleagues with legal qualifications and expertise in data protection took part in several months of intensive junior data scientist training. The retraining and further training of staff continued beyond the scope of the data scientist training; consequently, in the second half of the year, internal training sessions on data science and artificial intelligence became a regular feature, with a primary focus on familiarising staff with classical machine learning methods and large language models. For the work of the AI Lab, the Authority is, among other things, drawing on the assistance of the European Data Protection Board through the 'support pool of experts' programme[28]. The AI Lab will perform a dual role: on the one hand, it will assist legal colleagues in the Authority's proceedings in understanding and analysing new technologies; on the other hand, it will explore the possibility of making the Authority's internal operations more efficient through the use of artificial intelligence and other new technologies, in a secure manner and without the involvement of third parties. The first step in this process is a project aimed at anonymising the Authority's decisions.

IV.1. Thematic review of the Hungarian banking sector with regard to AI

As AI systems are spreading at a significant rate as data processing tools, and the banking sector processes the personal data of millions of data subjects, the Authority wishes to obtain an overview of the purposes for which AI systems are used in the Hungarian banking sector, what personal data are processed, and how compliance with data protection law is ensured. In this context, the Authority first approached the Magyar Nemzeti Bank in 2024 for the purposes of consultation and information sharing. Following the consultation, the Authority sent a questionnaire to the selected banks as part of the thematic review, with the aim of assessing the use of AI systems and their legal compliance.

On 22 December 2025, the Authority published a report on the main findings of the review[29] and highlighted, among other things, the importance of proper documentation; when using a third-party solution, it is essential to ascertain and

28 https://www.edpb.europa.eu/support-pool-experts-spe-programme_hu
29 https://www.naih.hu/hirek/802-jelentes-magyarorszagi-bankok-mi-hasznalatarol

record which data from which sources were used during the training of the AI model that converts images into data, and how the accuracy of the AI model was measured. The knowledge of AI models is determined not primarily by the algorithm, but by the data used for training. For this reason, the quality of the data used for training is not irrelevant, nor is the question of whether it is necessary for the data to be linkable to a specific natural person. In this context, the report highlights the importance of pseudonymisation and anonymisation in reducing risks, noting that the technical implementation of this must be adapted to the changing technical environment. The report also draws attention to the phenomenon of 'shadow AI', a collective term covering all instances where, within a given organisation, users utilise the organisation's IT infrastructure to use individual AI systems – whether for work purposes or for personal use – in a manner that is, from the organisation's perspective, unregulated, non-transparent and uncoordinated. This can entail numerous data protection and business risks, which is why it is of paramount importance for the controller to manage this through preventive technical and organisational measures. From the perspective of data protection obligations, due to the technology-neutral nature of the GDPR, it is irrelevant whether a given data processing tool qualifies as AI or is merely a similar analytical model; the fundamental principles apply equally to all data processing tools, and appropriate safeguards must be applied to them based on all the circumstances of the data processing. With regard to the classification of AI systems, the report draws on the European Commission's 2025 guidelines[30] on the definition of artificial intelligence systems.

30 https://ec.europa.eu/newsroom/dae/redirection/document/118630

IV.2. Cooperation with foreign supervisory authorities under the GDPR

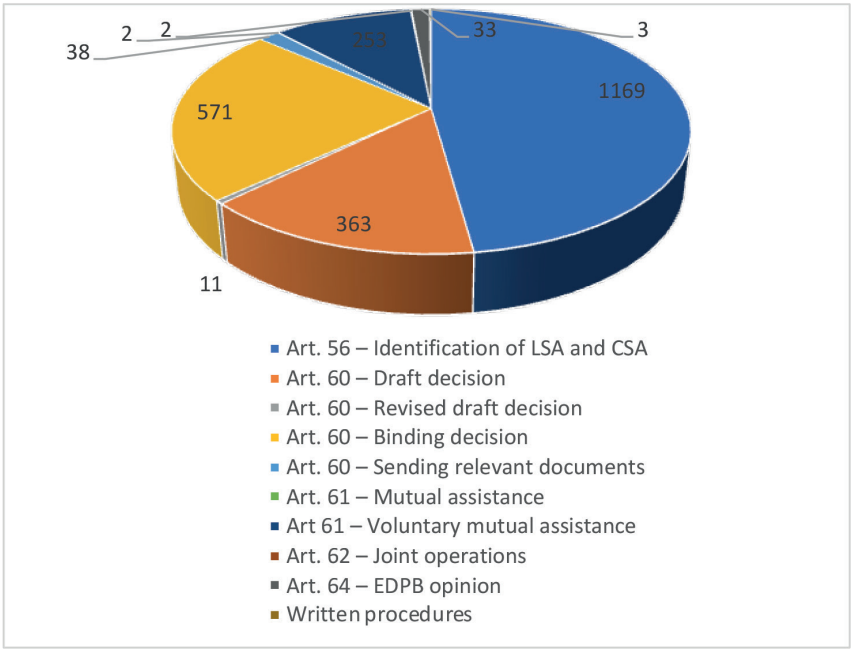


Figure 1: Procedures received by the NAIH

Since the GDPR came into force in 2018, the Authority has been actively participating in cooperation procedures with EEA Member States under the so-called one-stop-shop mechanism (Article 60 of the GDPR), which serves to investigate cases initiated on the basis of complaints or ex officio regarding cross-border data processing. Communication between authorities takes place via the interface of the Internal Market Information System (hereinafter: IMI), which has been specifically adapted for these procedures. The details of the procedures have already been outlined in previous reports (for example, the 2023 report). Based on statistics compiled since the GDPR came into force in May 2018, it can be stated that the trend continues whereby, in proceedings between Member State authorities, the focus is shifting from the identification of lead supervisory authorities towards cooperation and communication. In addition to the frequently recurring topics in the review of draft decisions and during voluntary mutual assistance procedures (camera-based data processing, insurance companies and

issues concerning data processing by messaging applications), it is worth noting that the GDPR-compliant verification of identity by controllers remains a challenge for them.

In 2025, the Authority received 1,169 cases under Article 56 from other Member State authorities via the IMI system. In more than 350 of these cases, the Authority found itself to be the concerned supervisory authority, and it acted as the lead supervisory authority in 8 proceedings; furthermore, in 2025, the Authority initiated 4 proceedings under Article 56.
The number of Article 60 proceedings received by the Authority also increased in 2025. The total number of draft decisions, revised draft decisions, final decisions and relevant documents also increased by more than 200 compared to the previous figure for 2024, rising from 766 to 983.
The Authority received a similar number of Article 61 proceedings as in the previous year, totalling 255, and we also received a higher number of EDPB opinions under Article 64 than in 2024, totalling 33. In parallel with this, we received 3 written procedures this year, and in 2025 the Authority initiated a total of 18 Article 61 procedures, of which 15 were voluntary and 3 were mutual assistance procedures.

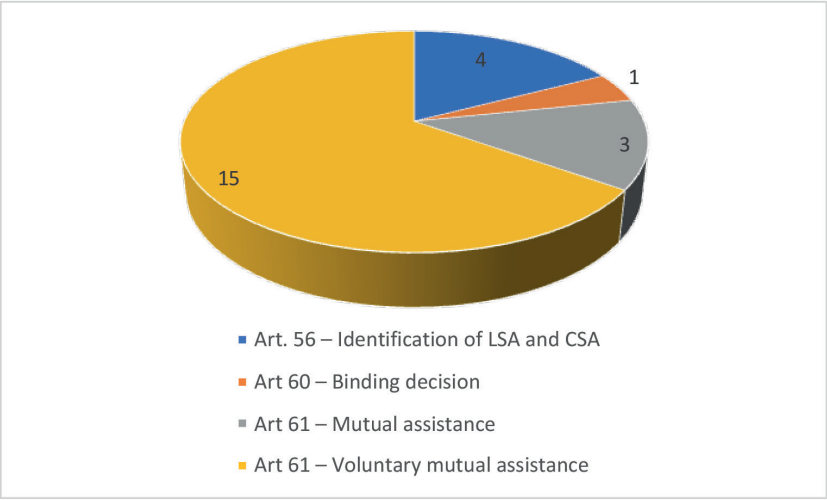


Figure 2: Procedures initiated by the NAIH

A steady increase in the number of cases can also be observed in 2025; a total of 2,445 cases were received by the Authority, and the Authority referred 23 cases to partner authorities. Compared to 2024, the number of cases received increased by 507, whilst compared to 2018, this represents an increase of 1,853 cases. No dispute resolution procedure has yet been initiated against any of the Authority's draft decisions.

IV.2.1. Joint operation under Article 62 of the GDPR concerning the processing of personal data by smart TVs

The widespread adoption of so-called smart TVs with internet connectivity raises a number of data protection risks, as these devices continuously collect large volumes of personal data involving multiple parties during their operation. The complexity of data processing and the lack of transparency of data processing procedures for data subjects have led the EDPB, within the scope of its tasks under Article 70(1)(e) of the GDPR, to designate the data processing of smart TVs as a strategic investigation topic for 2022, and the Dutch data protection authority (NL SA) published a call to launch a joint operation under Article 62 of the GDPR to examine data processing by smart TVs, which was joined by the Italian (IT SA), Liechtenstein (LI SA) and Hungarian supervisory authorities, i.e. the NAIH. The aim of the joint operation was to determine the extent to which data processing carried out by smart TVs complies with the principles set forth in Article 5 of the GDPR, in particular the requirements of transparency, data minimisation and purpose limitation, and to examine the lawfulness of any data transfers to third countries.
During the investigation, the participating supervisory authorities analysed the network data traffic of products from a total of three major manufacturers using a standardised IT expert methodology, while the devices were being installed, in standby mode, during normal use and when switched off. The authorities examined the telemetry data generated by the device using technical tools, including network traffic analysis. It was established in the course of the investigation that the device transmitted information constituting personal data to the manufacturer, its affiliated companies and certain advertising partners, in particular IP addresses, device identification data and data linked to user accounts. According to the results of technical analyses, significant data flows were observed in all devices examined, which were not limited to operations involving active user interaction. Although most of the data transfers remained within the European Union, a smaller proportion was directed to third countries outside the Union, such as Japan, South Korea and the United States, which also necessitated an examination of the safeguards under Chapter V of the GDPR. According to the

findings of the investigation, the devices transmitted personal data to manufacturers, operating system providers, streaming platforms and several third parties, often in an automated manner and in a form that was rather difficult for data subjects to follow.

As an authority participating in the joint operation, the NAIH conducted an investigation pursuant to Article 57(1)(a) and (h) of the GDPR and Section 38(2) of the Privacy Act in connection with the data processing practices of one of the selected smart TV manufacturers and, in the specific case, it found that the roles of the controllers could be distinguished, the legal basis and safeguards for data transfers complied with data protection regulations and therefore no breach of the GDPR could be established. Accordingly, the investigation was closed without the issuance of a formal notice, pursuant to Section 55(1)(b) of the Privacy Act.

The joint report on the case, issued by the participating authorities and available on the NAIH website in both Hungarian and English[31], highlighted that the data processing ecosystem surrounding smart TVs is extremely complex, involving the simultaneous presence of multiple controllers and data processors. This circumstance poses a particular challenge in terms of fulfilling the information obligations set forth in Articles 12–14 of the GDPR, as well as clearly defining the roles (joint controllers and data processors) under Articles 26 and 28 of the GDPR. According to the report, compliance with the data minimisation principle set forth in Article 5(1)(c) of the GDPR may also be questionable in the case of pre-installed applications that cannot be removed by the user. Although no specific data protection infringements were identified among the manufacturers examined, the findings may serve as a useful starting point for other EU data protection authorities in relation to future investigations of such devices. In summary, it can be concluded that data processing practices relating to smart TVs require particular attention at both European and international levels. Technological developments, multi-party data processing models and data transfers to third countries collectively pose risks that justify the consistent enforcement of the GDPR and, accordingly, regulatory action, as well as the further strengthening of cooperation among supervisory authorities.

31 English version: https://naih.hu/tajekoztatok-kozlemenyek?download=1293:a-holland-a-magyar-az-olasz-es-a-liechtensteini-adatvedelmi-felugyeleti-hatosagok-kozos-jelentese-az-okos-tv-k-adattovabbitasaival-osszefuggo-a-gdpr-62-cikke-szerinti-kozos-muveletrol-angol-nyelvu-valtozat

IV.2.2. Coordinated enforcement by supervisory authorities ('Coordinated Enforcement Framework' CEF)

In 2025, the European Data Protection Board decided to conduct a joint investigation into practices relating to the right to erasure ('the right to be forgotten'). As part of the coordinated action, the Authority sought to assess the practices of banks operating in Hungary regarding the implementation of the right to erasure under the GDPR, and to this end contacted 13 controllers. From a statistical perspective, it is significant that the volume of requests received by banks was largely determined by their size. Typically, smaller banks received far fewer erasure requests, and this also significantly determined their procedures. Regardless of this, it can be stated that, proportionally, every contacted controller received a large number of erasure requests, and fulfilling these put a significant burden on them. Based on the responses, these difficulties can be attributed primarily to the fact that personal data are often processed for different purposes, on different legal grounds, and with different retention periods.

In general, it can be observed that controllers – where possible – carry out erasure physically, i.e. at database level. This, which the Authority considers to be best practice, also posed a serious challenge to the respondents, as data structures often date back decades and were not designed in accordance with the 'privacy by design' principle. Consequently, complete erasure would also remove internal references within the database, leading to inconsistencies. In such cases, anonymisation may be an appropriate solution, and many banks also reported using this method when completing the questionnaire. A further difficulty is that some data processors charge an additional fee for cooperation in responding to requests addressed to data subjects.

Based on the responses collected during the coordinated operation, the Authority has drawn up proposals regarding the issuance of guidelines on the right to erasure, taking into account the above experiences.

IV.3. AWARE Project – the NAIH's data protection project to assess GDPR awareness among micro-enterprises

AWARE, the NAIH's latest EU data protection project, was launched on 1 February 2025, whose aim was to assess and enhance awareness of the GDPR's requirements among micro-enterprises, with a particular focus on the beauty industry and the private healthcare sector. SMEs play a significant role

from both an economic and an employment perspective, as in 2023, 66% of the workforce in Hungary was employed by a micro, small or medium-sized enterprise, and they accounted for approximately 41% of domestic value added. Thus, the starting point for the project was that many SMEs – despite playing a prominent economic role – still lack the expertise and resources necessary to comply with the GDPR.

The AWARE project specifically targets micro-enterprises operating in the beauty industry and the private healthcare sector, in collaboration with Hungarian and EU SME organisations and chambers of commerce. The selection of the target group was based on the NAIH's most recent data protection investigations and consultations with the Hungarian Chamber of Commerce and Industry, taking into account that both the cosmetics industry and private healthcare are continuously expanding sectors. The beauty industry is also an important sector from the perspective of gender equality, as the overwhelming majority of those employed in this sector are women.

The project focuses on areas requiring particular attention from SMEs and are significant from a data protection perspective: video surveillance; mapping and identifying data processing activities, with particular regard to special categories of personal data, such as the processing of health and biometric data; the presence or absence of a privacy notice; requests relating to the exercise of data subjects' rights; the processing of personal data of minors and women; employment-related issues; as well as the operation of websites or social media accounts, the sending of newsletters, the use of online payment and appointment-booking platforms, and knowledge of artificial intelligence.

Under the leadership of the NAIH, the project is being implemented in partnership with Trilateral Research Ltd., an Irish consultancy and R&D firm specialising in new technologies and data protection. The partners aim to achieve the set objectives through innovative, micro-SME-focused online tools and direct support offered to the target groups. The project will produce a number of deliverables: interviews with representatives of the Hungarian beauty and healthcare sectors, as well as EU and Hungarian SME organisations and chambers of commerce in order to map GDPR awareness and assess needs; an information website with resources in Hungarian and English[32]; a repository of previous project documents and other useful links in Hungarian and English, as well as the production of slideshows and brochures, and the organisation of webinars and training days

32 https://www.naih.hu/aware/aware-attekintes; https://www.naih.hu/aware-project/aware-general-information

for the target groups. To ensure the widespread dissemination of knowledge and experience, the partners plan to present the project's main results at international conferences as well as at meetings of the European Data Protection Board and its sub-groups.

Among the results already achieved are an analytical report on the target groups, a repository of 100 EU resources containing useful links and online tools for SMEs and interviews conducted by the consortium partners. NAIH, in cooperation with the MKIK, conducted a survey among Hungarian micro-SMEs operating in the beauty industry and private healthcare, while Trilateral Research Ltd. carried out interviews with EU SME organisations and chambers of commerce, partly through direct contact and partly via the EUSurvey. The information gathered during the interviews will be used to produce slideshows and brochures and to organise webinars and training days.

Other key details of the project:
Identification number: 101193182
Total budget: EUR 277,779
Contracted grant amount: EUR 250,000
EU funding rate: 90%
Planned completion date: 31 January 2027.

Further information on the project is available on the website https://www.naih.hu/aware/aware-attekintes.

V. Cases of litigation for the Authority

In 2025, the Authority had altogether 25 closed cases of litigation at the BudapestCapital Regional Court or the Curia.

Of this, the Authority won 14 cases in full, partially won one case, the court rejected even the petition in four lawsuits, the court terminated one lawsuit, and lost litigation in five cases only.

In 2025, the Authority imposed fines of HUF 98,235,000, of which HUF 67,195,000 was for data protection, HUF 27,965,000 was procedural fine and HUF 3,075,000 was enforcement fine. Of the fines imposed in 2025 and in previous years, including the late payment penalty, HUF 120,876,610 was paid voluntarily by the obligors, while enforcement action by NAV was taken in connection with fines of HUF 6,939,319. In 2025, the Authority initiated enforcement proceedings with the tax authority regarding fines totalling HUF 79,575,000, of which HUF 75,200,000 were data protection fines and HUF 4,375,000 were procedural fines.

Based on the Authority's litigation experience, it can still be concluded that the focus of court proceedings lies on administrative lawsuits following data protection authority procedures initiated upon petition; however, 24% of the cases concluded in 2025 were related to decisions issued in ex officio authority procedures. In 2025, 12 administrative lawsuits were brought against the Authority. Of the cases closed with final judgment, 15 were initiated by natural persons and 10 by legal entities.

Some of the more interesting and notable court cases are highlighted below.

V.1. Unlawful collection and storage of document copies under a LED replacement programme

Facts of the case

The controller, an energy trader, was classified as being subject to energy-saving obligations under the Energy Efficiency Obligation Scheme (hereinafter: EKR) from 1 January 2021, pursuant to Section 15(1) of Act LVII of 2015 on Energy Efficiency. The controller met its EKR obligation through lighting modernisation; on this basis, under the '[…] Residential LED Programme" (hereinafter: Programme), residential users were able to obtain new, state-of-the-art LED light

sources free of charge by entering into an energy efficiency agreement following online registration and the relevant procedure. The Programme was launched on 10 December 2021, and 132,546 registrations were made by 30 June 2024 via the web application set up for this purpose (hereinafter: Database).

During registration, in addition to providing certain mandatory personal data to apply for the Programme, applicants were required to upload a file containing both sides of their identity card and both sides of their official proof of address (hereinafter: copies of documents), as well as an image of the electricity bill in the consumer's name and certain additional details appearing on it.

The Authority found that, in respect of data processing carried out via the Database during the period from 10 December 2021 to 30 November 2023, the privacy notice available did not contain any details whatsoever regarding the registration process associated with the Programme, or the handling of identity documents, and official documents verifying the address and personal identification number. The eight-year retention period specified in connection with data processing relating to contracts and requests for quotations differed both from the actual data processing period established by the Authority and from the mandatory data retention period specified in general but not elaborated upon in the "General Terms of Contract" (hereinafter: ÁSZF) available to contracting consumers and the option of using the data for the purposes of similar energy-saving programmes.

The unverified digital copies of documents uploaded to the Database during registration are not suitable for achieving the purpose specified by the controller ("identification of the person"), as that requires the presentation of the original document. The principle of data minimisation is also breached by the fact that the copies of documents and the copy of the electricity bill contain not only the data strictly necessary for the request for quotations or the conclusion and maintenance of a contract, but list also other personal data (such as the photograph or signature on the relevant document, or the actual current account balance indicated on the electricity bill). The controller was unable to establish an appropriate legal basis for the processing of document copies carried out via the Database, and the data subjects were unable to give their voluntary consent to the processing of their personal data, given that they could not apply for the Programme without providing copies of their documents; therefore, the controller's data processing activities in relation to the copies of documents failed to comply with the provisions of Sections 7(2) and 35 of Act XX of 1996 on identification methods replacing personal identification numbers and the use of iden-

tification codes. The privacy notice was not readily accessible to data subjects; Chapter III.5 of the ESZF was not easily comprehensible to a person without legal knowledge, despite the fact that broad public interest in the Programme could have been anticipated. The provisions relating to data processing were not separated from the contractual provisions. The Frequently Asked Questions (hereinafter: GYIK), which were also available, stated that the data subject could not object to the data processing, contrary to the rights to withdraw consent, object and seek legal remedy under the General Data Protection Regulation.

The controller failed to take appropriate measures to provide data subjects with all the information and details referred to in Articles 13 and 14 of the General Data Protection Regulation in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Neither the ESZF nor the privacy notice available until 30 November 2023 specified, explicitly and, in accordance with the facts, the exact purpose of the intended processing of the data, nor the legal basis for the processing; the recipients of the personal data, the categories of recipients; the duration of storage of the personal data; or the categories of personal data concerned.

From 1 December 2023, the controller introduced a new privacy notice in which it incorrectly specified the legal basis for the intended processing of the data and the duration of storage of the personal data; the information provided was not comprehensive, and it did not explain the mandatory data processing required of the controller by law. According to the new privacy notice, in the case of data processing for the purposes of retaining, verifying and, where necessary, auditing documents, or conducting legal proceedings and providing evidence in the course of such proceedings, the controller processes the data for a period of ten years; however, the specific provision of the relevant legislation was not indicated. The information provided was not in accordance with Section 14(4) of Government Decree 122/2015. (V. 26.) on the implementation of the Energy Efficiency Act.

The controller did not implement technical measures to prevent unauthorised data saving by users, which would prevent staff from saving data or copies of documents from the Database from the browser to a computer, or from taking screenshots of them. Access rights to the Database administration interface were not revoked for persons who were not actually performing contributor tasks during the relevant period. The deletion of document copies was not automated or regular; it generally took place on a monthly basis. According to the findings of the on-site inspection, the documents were stored for too long, as their deletion

had not taken place, as established during the on-site inspection and according to the results of the internal investigation conducted by the controller; furthermore, the deleted email addresses were stored for an indefinite period, thereby breaching the principle of limited storage. The cooperation agreement concluded with the cooperating local authority cannot be regarded as a data processing agreement, as it did not contain the safeguards set forth in Article 28(3)(b) and (f) of the General Data Protection Regulation. In addition to this substantive deficiency in the cooperation agreement, the Authority found that the controller had committed an infringement because the contract for data processing was not put in writing.

The Authority's decision as respondent

In its decision No. NAIH-19-18/2024 dated 10 September 2024, the respondent found that the petitioner had negligently breached for the period from 10 December 2021 to 30 November 2023 the principle of transparency set forth in Article 5(1)(a) of the GDPR, Article 5(1)(c) of the GDPR, Article 6(1), Article 12(1), Article 13(1)(c), (e) and (2)(a), Article 14(1)(c), (d) and (e) and (2)(a), and Article 32(4) (points (a) to (i) of Section 1.1); for the period from 10 December 2021 to 2 November 2023, Article 5(1)(e) of the GDPR (Section 1.2); for the period from 16 May 2023 to 15 June 2023, Article 28(3) and (9) of the GDPR (Section 1.3); during the period from 1 December 2023 until the conclusion of the evidentiary proceedings, Article 13(1)(c) and (2)(a) of the GDPR, as well as Article 14(1)(c) and (2)(a) [points (a) to (d) of Section 2]. Due to the infringements established in Section 2, the Authority ordered the petitioner to bring its data processing practices into line with the provisions of the GDPR and to amend its relevant privacy notice (Section 3). Due to the infringements established in Sections 1 and 2, the court ordered the petitioner to pay a data protection fine of 75,000,000 forints.

The court's decision and its legal justification

According to the Budapest-Capital Regional Court, the petition brought by the petitioner was unfounded.

On the merits of the case, the court found that the petitioner had merely asserted that the data processing it carried out was transparent, but had not put forward any arguments to refute the respondent's findings in this regard. It was unfounded to argue that adequate information was available in the ESZF and the old privacy notice, because information provided in connection with the Programme in the manner and with the content required by the GDPR, and a detailed explana-

tion of the fundamental characteristics of the data processing, was not available in any of these documents. The information provided by the petitioner was fragmented, incomplete and, in places, inconsistent, and it was also contrary to the GDPR. In addition to the fact that certain elements of the information were missing, the information was not sufficiently clear, comprehensible or readily accessible at the start of the registration process. The information had to be transparent to data subjects and fully compliant with the requirements set forth in the GDPR, irrespective of the petitioner's assumption as to what information the data subjects possessed or whether they were able to interpret the differences between the various legal bases under the GDPR. The provision of information that does not meet the requirements of the GDPR and is not transparent is not justified by the fact that anyone could participate in the Programme. The transparency and adequacy of the information for all data subjects is also essential because, due to the different legal bases, data subjects are entitled to different rights; for example, in the case of the legal basis under Article 6(1)(b) of the GDPR, the data subject is not entitled to the right to withdraw consent. It must therefore be clear to data subjects what rights they can exercise in relation to a given data processing operation. If the petitioner uses the term 'consent' in the privacy notice, this cannot lead to the conclusion that the legal basis for the data processing is not consent under Article 6(1)(a) of the GDPR.

The petitioner also made an unfounded assertion that no complaint had been received regarding the transparency of its data processing, since the complaint set forth in paragraph (51) of the decision specifically drew attention to the shortcomings, inaccuracies and potential opportunities for abuse in the Programme's data processing notice. Based on all this, contrary to the petitioner's position, the information provided by it was not transparent, comprehensible, clear and accessible.

With regard to the processing of personal documents via the Database, the data subjects were unable to give their voluntary, informed and explicit consent: it was mandatory to upload copies of documents to the Database in order to apply for the Programme; without doing so, they could not participate in the Programme; they did not receive adequate information on a number of fundamental circumstances relating to data processing; and the text displayed next to the tick box on Website1 did not meet these requirements either.

The processing of copies of documents was not necessary for the conclusion of the contract; therefore, the legal basis under Article 6(1)(b) of the GDPR was also

inapplicable. For all these reasons, the petitioner's arguments challenging the findings of the decision regarding the lack of a legal basis were also unfounded.

In relation to the infringement of the principle of data minimisation, the court noted that the GYIK itself had specified the verification of the person named on the electricity bill as the reason for uploading the identity documents. Making copies of the documents in their entirety and viewing the documents – which the respondent cited as an appropriate method in this context – cannot be regarded as entirely identical data processing operations, given that the former, as it concerns all personal data appearing on the document copies, is not limited to the extent necessary to achieve the purposes of data processing. In contrast, the inspection of documents may be limited solely to those personal data that are relevant to the purpose of data processing and necessary for achieving that purpose. The data processing in question, relating to the Programme, falls outside the scope of the Anti-Money Laundering and Counter-Terrorism Act (Pmt.) and is not covered by its provisions; therefore, the Anti-Money Laundering and Counter-Terrorism Act is not relevant to the present case and cannot be taken into account, and the petitioner's reliance on its provisions was unfounded. In the case under consideration, proof of identity could have been established not by collecting copies of documents but by presenting the original documents; in view of this, the request for copies of documents was unnecessary, as they were not suitable for achieving the purpose indicated by the petitioner. However, the respondent found a breach of the principle of data minimisation not only because the copies of the documents were unsuitable for verifying identity, but also because they contained data – such as a personal identification number and a photograph – which were undoubtedly unnecessary for data processing. Consequently, the principle of data minimisation was clearly breached, as certain personal data processed by the petitioner were not relevant to the purposes of the data processing and were not limited to the necessary scope. By changing its practice, the petitioner introduced, with effect from 1 December 2023, the presentation of documents upon the physical handover of the LEDs for the purpose of document verification, instead of requesting copies of documents, which also demonstrates that a method existed that was suitable for achieving the objective whilst protecting the personal data of the data subjects. The finding that there has been a breach of Article 5(1)(c) of the GDPR is not affected by the petitioner's assertion that no incident occurred in relation to the data.

With regard to the limited storage period, the petitioner stated that data was generally deleted on a monthly basis; however, this cannot be regarded as systematic. The petitioner did not dispute that, at the time of the on-site inspection, it was

still processing copies of documents in the Database in relation to 374 individuals registered prior to 1 September 2023, that is, it had not deleted 374 records, and as regards the infringement of the principle of limited storage, it is irrelevant what percentage of participants in the Programme this figure represents. The petitioner was required, in accordance with the principle of limited storage, to store personal data in a form that allows the identification of data subjects only for as long as is necessary to achieve the purposes of the processing of personal data. The petitioner could have met this requirement by regularly and automatically deleting copies of documents, but failed to do so, as – undisputedly – 374 records had not been deleted at the time of the on-site inspection. The continued processing of the names and email addresses of the 84 data subjects requesting erasure, referred to in paragraph (254) of the decision, and the maintenance of a separate register containing this personal data was unnecessary and also contrary to the requirement that the storage of personal data should enable the identification of data subjects only for as long as is necessary to achieve the purposes of the processing of personal data.
The respondent did not arbitrarily identify data security deficiencies in the petitioner's practices relating to the measures required by Article 32(4) of the GDPR. In paragraphs (217) to (241) of the decision, the respondent set forth the circumstances in exhaustive detail which resulted in a breach of Article 32(4) of the GDPR, in that the measures taken by the petitioner were not sufficient to ensure that natural persons acting under its control who had access to personal data relating to the Programme could process such data only in accordance with its instructions.

In view of the foregoing, the respondent's decision was not unlawful in the respect contested by the petition; and the court therefore dismissed the petition pursuant to Section 88(1)(a) of the Code of Administrative Court Procedure (Fővárosi Törvényszék 105.K.703.714/2024/17).

The petitioner lodged a petition for judicial review against the judgment. The Curia refused to accept the petition for judicial review. According to the reasoning of the order, the fact that accepting the position of the party submitting the petition for judicial review might result in a decision more favourable to that party does not establish either the particular gravity or the social significance of the legal issue raised (Kúria Kfv.IV.37.804/2025/2).

V.2. Ordering the enforcement of a judgment

Facts of the case

The first petitioner operates as a religious association forming part of an international church, whilst the second petitioner operates as an organisational unit of the first petitioner that has legal personality.

On 5 December 2016, the respondent, acting ex officio, initiated a data protection authority procedure under Section 60(4) of Act CXII of 2011 on the Right to Informational SelfDetermination and Freedom of Information (Privacy Act) to examine the petitioners' data processing activities. In its decision NAIH/2017/148/98/H of 13 October 2017 (the "Decision"), points 1 and 2 of the operative part established that the petitioners had carried out unlawful data processing activities, as – according to the reasoning – they had breached their obligation to provide prior information, the principle of purpose limitation, the principle of fair data processing, the requirements of data security and they had processed data without a legal basis. The Decision prohibited the petitioners from continuing their unlawful data processing and called upon them to, within 30 days from the communication of the Decision, amend their data processing information practices in compliance with the Privacy Act due to the breach of their obligation to provide prior information, ensuring that in the future they give adequate information on the purposes of data collection and processing, the identity of the controller, and the further circumstances of the processing to data subjects at the time their personal data are collected on consent forms and other forms; they were instructed to inform their staff, service users and followers of how the data processing had been modified, and to request the consent or reconfirmation of consent from all affected persons, presenting the amended privacy notice to the respondent in advance; in the absence of consent confirmed for each purpose, they were required to ensure the documented deletion of the affected data; personal data collected about third parties who were neither employees, nor applicants, nor followers, and for whom there was no appropriate purpose or legal basis, had to be deleted or destroyed by ensuring irreversibility; for the future, they were required to cease data collection concerning third parties; to terminate transfers of data abroad; and to fulfil data security requirements concerning any transfer of personal data abroad.

The petitioners were instructed to inform the Authority of the measures taken within 30 days from the expiry of the deadline for bringing an action, attaching

records fully documenting the fact and circumstances of the deletions, along with a declaration confirming that all copies and versions of the specified data had been deleted.

In its judgment 13.K.700.014/2018/60 dated 22 March 2019, the Budapest-Capital Regional Court dismissed the petitioners' petition. The Curia, as the court of legal review, by its judgment Kfv.II.37.743/2019/21 (hereinafter: the Curia's judgment), set aside the judgment of the Budapest-Capital Regional Court 13.K.700.014/2018/60, as well as paragraphs 159–170 of the justification for the Decision, and otherwise dismissed the petitioners' petition.

By its order NAIH-731-7/2021 of 28 April 2021, the respondent ordered the implementation of the obligations set forth in points 1 and 2 of the operative part of the Decision, as well as the provision of evidence of such implementation, together with supporting documents, within 15 days of receipt, given that the petitioners had failed to fulfil the obligations set forth in the Decision in full and within the prescribed time limit.

The action brought against the order for enforcement was dismissed by the Budapest-Capital Regional Court in its judgment 104.K.704.400/2021/19 (judgment of the Budapest-Capital Regional Court [Fővárosi Törvényszék]).

The Authority's decision on enforcement

In its order of 22 March 2024, under case number NAIH-4797-10/2024, the respondent decided on the enforcement of the obligations set forth in points (a) to (f) of paragraph 1 and points (a) and (b) of paragraph 2 of the operative part of the decision in the enforcement proceedings ordered, and on the manner of such enforcement. It ordered that, within 45 days of receipt of the order, the documents and records listed item by item in the minutes NAIH-731-12/2021 and NAIH-731-13/2021 and seized during the on-site inspection held on 29 and 30 April 2021 at the respondent's registered office, specifically the personal data obtained by the petitioners without legal basis and the personal data of third persons stored in the PC and Ethics files, to be deleted by destroying the PC and Ethics files. In the operative part, it listed the files in the minutes by serial number. It further ordered the petitioners jointly and severally to destroy, at their own expense and risk, those PC and Ethics files not seized or impounded by the respondent or any other authority, within 45 days of receipt of this order, in which the controllers recorded the personal data of the data subject on the legal basis of consent.

The court's decision and legal justification

With regard to the breach of the obligation to clarify the facts of the case, the petitioners argued that the respondent had failed to carry out an item-by-item and comprehensive examination of the seized documents. In this regard, the court established that the respondent is obliged to clarify the facts of the case to the extent necessary for reaching a decision. In its order, the respondent described in detail the method used to conduct an item-by-item examination of the extremely large volume of seized documents and also set forth the results thereof. The court found the respondent's method of examination to be appropriate, having regard to the quantity and quality of the documents – namely, that they were largely unsystematised paper-based documents – since the findings could be made in respect of the entire volume of the documents seized on the basis of the results of the examination. In view of this, the respondent did not breach the obligation to clarify the facts set forth in Section 62 of the Code of General Administrative Procedure. Nor could a breach of the obligation to state reasons under Section 81 of the Code of General Administrative Procedure be established, as no further description of the content of the documentation – beyond what was set forth in the order – was necessary for the decision to be made. The respondent provided an extremely detailed statement of reasons for its decision, which was supported by the facts and evidence discovered, and its legal justification was also exhaustive.

The procedural objection that the respondent provided no assistance whatsoever to the petitioners in drafting the consent forms for data processing was entirely unfounded, despite the fact that they had expressly requested such assistance and had sent the statements they had drafted to the respondent. No breach of the principle of fair procedure could be established, and given that the petitioners were unable to identify any specific legal provision under which the respondent would have been obliged to take the measure they alleged was lacking, due to a failure to perform a procedural act which does not arise from either procedural or substantive law, no violation of fundamental principles by the Authority can be established. The respondent is not responsible for the legality of the petitioner's proceedings; indeed, it falls within the respondent's remit to monitor the implementation of the Decision and, where necessary, to conduct enforcement proceedings, as it occurred in the present case. The assumption that the respondent is obliged to draft forms for the petitioners in order to obtain consent in accordance with the law, or even to correct or comment on them, is entirely unfounded.

In the present case, the court found, with regard to the enforcement of the Decision, that the General Data Protection Regulation does not contain any provision that would render the obligations set forth in the Decision legally unenforceable; the rules of the General Data Protection Regulation are consistent with the relevant provisions of the earlier Directive in force at the time the Decision was adopted, indeed, in the areas of the validity criteria for consent and the justification of the lawful basis for the processing of personal data, it requires the application of even stricter principles and conditions than those set forth in the Directive.

The court emphasised that the Act on Judicial Enforcement stipulates that the Authority is obliged to order the method of enforcement that most effectively promotes compliance with the obligation.

Consequently, the sole purpose of the enforcement proceedings was to ensure compliance with the obligation set forth in the Decision; to this end, the respondent was required to prescribe the method that would most effectively facilitate compliance. This was not merely an option for the respondent, but a statutory obligation; in other words, the respondent was required, above all, to bear in mind the effectiveness of the enforcement and compliance. The Act on Judicial Enforcement does not require the party obliged to manage enforcement to order the least onerous method, but rather the most effective method for the purposes of compliance. The respondent's decision complied with this statutory obligation; for want of voluntary compliance, it was required to order the most effective method of compliance, which is undoubtedly the complete destruction of the documents seized.

The respondent substantiated with facts and calculations that the obligation ordered in the Decision – the erasure or destruction of third parties' personal data – could only be fulfilled by the destruction of the entire documentation seized.

The petitioners' assertion that the respondent prescribed an act not contained in the Decision was unfounded. The operative part of the Decision cited above obliged the petitioners to erase or destroy the personal data of third parties that had been processed unlawfully. The documentation seized – as established in previous proceedings – contains the personal data of third parties processed in breach of the law. According to Section 3(16) of the Privacy Act, in force at the time the Decision was issued, data destruction means the complete physical destruction of the data medium containing the data; the complete destruction of documents. In the present case, the data medium consists of the documents,

records and data carriers seized; thus, by ordering the destruction of the data, the Decision effectively prescribed the complete physical destruction of the documents. Physical destruction naturally applies to the document as a whole. The Decision ordered the erasure or destruction of the data, which means that any method of enforcement may be applied and may thus be ordered in the enforcement proceedings. The respondent provided detailed reasons as to why, in view of all the circumstances of the case, erasure would not be feasible or would entail a disproportionately heavy workload; therefore, the destruction of the data is the most effective method of enforcement applicable under the Decision and Section 174 of the Act on Judicial Enforcement.

When ordering the method of enforcement, the respondent was not required to consider the petitioners' followers' freedom of religion and right to freely practise their religion, particularly given that the infringements and obligations established in the Decision were fixed and could not be reviewed on the basis of any new arguments. The sole purpose of the order at issue in the proceedings was to determine the method of enforcement; the obligation to be enforced cannot be the subject of review, and thus the infringement of the believers' rights caused by the enforcement cannot be considered in this regard.

Taking the above into account, the court found that the respondent's conduct and order were not in breach of the law for the reasons set forth in the petition; the respondent, on the basis of facts that had been properly established and clarified, and through a lawful and correct interpretation of the law, reached a well-founded decision, on the basis of which it dismissed the petitioners' unfounded claim (Fővárosi Törvényszék 103.K.701.522/2024/65.).

By its order Kfv.VII.37.166/2026/3 of 20 March 2026, the Curia refused to accept the application for review filed by the first and second petitioners. (Kfv. VII.37.166/2026/3.).

V.3. "Listing" at a local authority

Facts of the case

On 16 May 2023, the mayor of a municipality (hereinafter: the mayor) held a press conference at which a list containing personal data (hereinafter: the list) was distributed in paper form to the journalists present. This list, in tabular for-

mat, contained the names of natural persons, their job titles, the starting date of their employment, the end date of their employment, and the gross monthly salaries paid upon termination of their employment. At the press conference, the mayor claimed that all the individuals on the list were relatives or family members of former local government leaders. Following the press conference, on the very same day, an online report on the events of the press conference appeared on a website operated by a company wholly owned by the first petitioner local authority, under the title "(…) listed the corruption cases that occurred during the time of its predecessors", which published the data contained in the list in anonymised form.

The Authority's decision as respondent

In its decision NAIH-519-13/2024 of 14 June 2024, the Authority, as respondent, – inter alia – partially upheld the applicant's request, finding that the first petitioner ordered the collection of personal data without a proper legal basis and, by means of data transfer during a public press conference, had made the applicant's personal data relating to his employment as a former employee accessible. In doing so, it intentionally infringed Article 6(1) of the GDPR. Furthermore, in the case of the first petitioner, it found ex officio a breach of the principle of fair processing under Article 5(1)(a) of the GDPR, as well as an intentional breach of the principle of processing for specified purposes under Article 5(1)(b) of the GDPR. In the case of the second petitioner, it found ex officio that the petitioner extracted and transferred personal data and data of the public interest to the first petitioner without an appropriate legal basis, thereby intentionally breaching Article 6(1) of the GDPR. As a result of the infringements, the first petitioner was ordered to pay a data protection fine of 2,500,000 forints, whilst the second petitioner was ordered to pay a data protection fine of 500,000 forints.

The court's decision and its legal justification

The court primarily ruled on the legal basis for data processing and data transfer – as the main issues in the proceedings. In the case in question, personal data were collected, transferred and disclosed to the public via the press. Recitals (39) and (41) of the GDPR also indicate that data processing is lawful only if the specific purposes of the processing are determined prior to the commencement of processing, and these must be explicitly defined and lawful. The legal basis for the data processing carried out by the first petitioner was Article 38(1) and Article 39(2) of the Fundamental Law, and the legal basis for the data transfer was Article 6(1)(e) of the GDPR, whilst the legal basis for the data processing of

the second petitioner was founded on press enquiries from the media and the volume of data requests. The court noted that, in the case of data processing based on Article 6(1)(e) of the GDPR, the controller's balancing of interests is not relevant. In this context, the respondent correctly referred to Section 26(2) of the Privacy Act, stating that the balancing of interests had been carried out by the legislator itself in that provision, and therefore the controller was not entitled to re-evaluate it. In relation to the data processing purposes identified by the petitioners, the court further points out that the decision explained in detail and with due reasoning that the legislation and case law – having regard to the fact that his legal relationship did not exist under the Act on Public Service Officials – why it does not classify the applicant, employed as an IT specialist, as a person performing a public function, and further supported, with reference to Constitutional Court guidelines and case law, the degree of balancing of interests required of controllers by the legislator when disclosing the data of persons performing public functions. The court found that neither the first nor the second petitioner complied with these legislative and judicial requirements in their data processing. The balancing of interests prior to disclosure was one-sided, as the first petitioner disregarded the private interests of the persons appearing on the list.

In the case of the first petitioner, in addition to the unlawful processing of data, breaches of the principles of fair processing and purpose limitation were also established. The principles of lawfulness, fairness and transparency under Article 5(1)(a) of the GDPR must be met from the perspective of the data subjects; in other words, data processing must be carried out in a manner that is transparent not to just anyone, but specifically to the data subject. As for the principle of purpose limitation under Article 5(1)(b) of the GDPR, it is a necessary condition that data processing be carried out for a clear and legitimate purpose.

The court established that the data requests referred to by the petitioners and found in the petitioners' records in the previous proceedings did not demonstrate a high level of public interest in relation to the persons on the list, and could not substantiate the alleged significant media interest with data from the first petitioner's records. Consequently, the publication of the list did not serve the purpose of transparency in the use of public funds by the municipality, which had been cited as the purpose of the data processing. The breach of the fundamental principles was also supported by the fact that the second petitioner acted contrary to its previous practice when it forwarded the applicant's data to the first petitioner without the applicant's consent. Irrespective of the first petitioner's objective, the publication resulted in a negative value judgement regarding the persons named on the list, a consequence which was already foreseeable during

the data collection process. In view of the above, the court found that the data processing by the first and second petitioners did not comply with the fundamental requirements expected by the legislator, and thus the respondent correctly established that those requirements had been breached.

The Authority, as respondent, classified the petitioners' data processing activities as intentional, given the nature of the infringement. In this regard, it is important to note that 'intentionality' does not refer to a conceptual category in the sense of criminal law, but rather to a higher degree of culpability, which the respondent took into account as an aggravating circumstance when adopting the decision, pursuant to Article 83(2)(b) of the GDPR. The court was satisfied, on the basis of the procedural documents arising from the preceding proceedings, that the respondent had sufficient evidence to establish both the fact of the adverse assessment of the data subjects resulting from the listing and the mayor's abuse of public authority and to assess them as aggravating circumstances in its decision. These findings could be correctly inferred from the circumstances and the manner of the data processing, the lack of a balancing of interests, and the context of the disclosure to the public.

On other issues, the court found that the first petitioner merely asserted, without providing any justification, that it would have been necessary to disclose the relatives' data in view of the former managers' identities. In the absence of a legal basis, it is also irrelevant that the mayor requested the collection of data on specific individuals or a category of relatives. In its decision, the respondent did not state that the second petitioner maintains a register of relatives. Although the petitioner referred to the fact that the names of the former leaders' relatives are matters of public knowledge, it was unable to substantiate this assertion; thus, the respondent's assessment was also appropriate in this respect.

To summarise the above, the petitioners did not have a valid legal basis for the processing of the data, and the documents they submitted did not prove its existence. They did not substantively refute either the alleged breach of fundamental principles, the lack of a legal basis, or the respondent's findings regarding the rights of the data subjects.

On the basis of the above, the respondent's decision did not contravene the law within the scope asserted by the petition; therefore, the court dismissed the petition pursuant to Section 88(1)(a) of the Code of Administrative Court Procedure (Fővárosi Törvényszék 105.K.703.121/2024/10.)

V.4.Legality of a decision adopted in a transparency administrative procedure

Facts of the case

On 3 March 2023, the State Secretary for Sport of the budgetary authority, acting as the petitioner, made a funding decision in favour of the Utánpótlás Neveléséért Alapítvány (Foundation for the Education of Young Athletes; hereinafter: the Foundation) entitled 'Support for the 2023 sports academy tasks of state-recognised sports academies, methodological centres and priority regional sub-centres', amounting to 5,613,000,000 forints in budgetary support (hereinafter: the Grant). The petitioner entered into an administration agreement (hereinafter: Administration Agreement) with the (…) Sportügynökség Zrt (hereinafter: SÜ) on 23 March 2023 for the payment of the Grant and grants to other supported organisations not affected by this legal dispute, amounting altogether to 39,176,000,000. Pursuant to the Administration Agreement, SÜ, acting on behalf of and in the name of the petitioner, entered into a grant agreement (hereinafter: Grant Agreement) with the Foundation on 11 April 2023. The petitioner made the budgetary funds available to SÜ for the payment of the Grant (and grants awarded to other organisations), on the condition that SÜ may not manage these funds but may transfer them exclusively to the Foundation. The Implementation Agreement and the Grant Agreement primarily provided for the application of the provisions of Act V of 2013 on the Civil Code (hereinafter: Civil Code).
In relation to the Support, the petitioner fulfilled its disclosure obligation under Section 37/C of Act CXII of 2011 on the Right to Informational SelfDetermination and Freedom of Information (Privacy Act) by indicating, in row 19 of its data submission of 17 April 2023 on the Central Public Information Register platform (the "Platform"), the SÜ as the beneficiary and the amount of the support as 39,176,000,000 forints.

According to data from the Treasury Monitoring System (hereinafter: OTR) available on the website of the Hungarian State Treasury, the grant agreement relating to the Grant came into effect on 11 April 2023, with the Foundation as the applicant for the Grant, the grantor as the petitioner, and the grantor recording the claim for the grant is SÜ.

The Authority's decision

The respondent, in its decision NAIH-3786-10/2024 of 24 October 2024, found that the petitioner breached Section 37/C(1) of the Privacy Act and paragraphs (2) and (3) of Section 5 of Government Decree 499/2022 (XII. 8.) on the detailed rules of the Central Public Information Register (hereinafter: the Decree) by fulfilling its data reporting and disclosure obligations with information that did not reflect reality; it was required to fulfil its data reporting and disclosure obligations on the Platform on an urgent basis, but within a maximum of fifteen days, by supplementing the data with the details of the actual beneficiary in accordance with the facts, in respect of the data of the Subsidy specified in Section 37/C(3)(a) of the Privacy Act, indicating which line of data in its previous data report is affected by the correction and in what manner; it further ordered, ex officio, that the decision be published on the respondent's website.

The court's decision and its legal justification

Pursuant to Section 37/C(1) of the Privacy Act, in the interests of transparency regarding the use of public funds, legal persons registered in the Register under the Act on Public Finances – with the exception of national security services – shall make the data specified in paragraph (2) accessible to anyone via a website operated by the organ designated by Government Decree and in accordance with the requirements set forth in Section 33(1) via the platform of the Central Public Information Register, which enables machine readability, bulk downloading, grouping, searchability, extraction and comparability of data, at two-monthly intervals, in a manner accessible for at least ten years following publication, broken down in accordance with paragraph (3). Those required to publish shall, on the occasion of data submissions made every two months, publish the data generated up to the 30th day preceding the deadline for the next data submission.

The petitioner is undisputedly a legal person registered in the Register under the Act on Public Finances, and is therefore obliged to publish on the Platform pursuant to Section 37/C(1) of the Privacy Act. The obligor cannot fulfil its obligation under Section 37/C of the Privacy Act on a public platform other than the Platform; it is therefore unfounded to claim that disclosure and transparency are not compromised in itself due to publication on the SÜ's own website. The SÜ cannot fulfil the obligation prescribed in Section 37/C of the Privacy Act on behalf of the petitioner, because the SÜ is not a legal entity registered in the Register of legal entities and therefore it is not among those obliged to publish on the

Platform. As regards the merits of the infringement established by the respondent, it is irrelevant whether the SÜ published the details of the Grant on its own website with content that reflects reality. The Platform serves the purpose of making data of public interest or data accessible on public interest grounds available from a single location; therefore, the principle of transparency is breached if the publication is not 'carried out' by the person obliged to do so, in the appropriate place, and with the appropriate data.

Pursuant to Section 37/C(2) of the Privacy Act, those obliged to publish on the Platform must publish data on payments on the Platform made for [….] a) any budgetary support exceeding five million forints, provided from domestic or European Union sources, namely budgetary support provided in accordance with the Act on Public Finances – unless the budgetary support is withdrawn or the beneficiary waives it prior to publication. Paragraph (3)(a)(aa) stipulates that those required to publish the data referred to in paragraph (2) on the platform shall publish them in the following breakdown, indicating the proportion of domestic and European Union funds used:

a) in the cases under points a) and c) of paragraph (2): aa) the designation (type) of the contract, the name of the beneficiary – in the case of a nonnatural person, its name and registered address – its tax number, the subject of the support, the place of implementation of the support programme, the start and end dates, and, where applicable, the date of payment, as well as the amount and currency of the support, […]

In accordance with Clauses 1.1 and 1.2 of the Grant Agreement, the Ministry of Human Resources has, with effect from 1 January 2020, provided central sports funding to state-recognised sports academies, methodological centres and priority regional sub-centres, a task which, following legislative changes, was taken over by the petitioner from 24 May 2022. It is an undisputed fact that the decision to provide the Grant to the Foundation was taken by the petitioner's State Secretary, a fact clearly supported by the OTR data and the Implementation Agreement. Since, without the State Secretary's decision, it cannot even be considered that the Foundation is the beneficiary of the Grant, the respondent correctly and reasonably established that the Grant was provided by the petitioner, and consequently, pursuant to Section 37/C(2)(a) of the Privacy Act, the petitioner was also required to publish the payment details on the Platform.

The court made the following findings regarding the role of the SÜ. Both Clause 1.3 of the Grant Agreement and Clause I.1 of the Implementation Agreement stipulate that the petitioner entrusted the SÜ with the performance of the implementing tasks pursuant to Section 49 of the Act on Public Finances. The use of an administrator was undoubtedly permitted under Section 9(3) of the Grant Decree. The Grant Agreement – in accordance with the common meaning of the term 'administrator' and Clause I.1 of the Administration Agreement – nevertheless stipulates that SÜ acts on behalf of and in the name of the petitioner, which clearly constitutes legal representation under Section 6:11 of the Civil Code. Furthermore, Clause 10.2 on page 17 of the Grant Agreement also primarily stipulates the primacy of the provisions of the Civil Code, which is not inconsistent with the Act on Public Finances and the Decree on the Implementation of Public Finances referred to by the petitioner without citing specific legal provisions. The Grant Agreement thus concluded on behalf of the petitioner gives rise to rights and obligations directly between the petitioner and the Foundation pursuant to the relevant provisions of the Civil Code; therefore, from the perspective of legal effects, it must be regarded as if the petitioner had concluded the Grant Agreement with the Foundation.

It is undisputed that the petitioner transferred the budgetary grants allocated to the sports academies, including the Grant, to the SÜ's account; however, pursuant to Clause III.1 of the Implementation Agreement, SÜ may not manage the amounts thus transferred; its sole task is to transfer the specified grant amounts to the sports academies, methodological centres and priority regional sub-centres designated in the petitioner's grant decision. For this reason, the SÜ clearly cannot be the beneficiary of the Grant, since the beneficiary – even in the general sense of the term – is the person who may use the grant provided. Due to the incorrect identification of the beneficiary – given that the Grant is only part of the grants covered by the Implementation Agreement – the amount of the Grant did not reflect reality in the data published on the Platform, and thus the part of the decision aimed at rectifying this is also lawful.

The arguments regarding the double publication were also unfounded, because the respondent clearly and unambiguously stipulated the obligation to provide supplementary data and publish them in the operative part of its decision, which means that the correction of the actual beneficiary data must be carried out as a follow-up act by the petitioner in a new document, since the previously published data cannot be subsequently amended in the system; the petitioner must indicate in that document how the data in line 19 of the data disclosure published on 17 April 2023 have changed. The court notes that the previous proceedings did

not concern the identification of the full range of beneficiaries; however, the petitioner's data disclosure and publication can only be considered complete when it includes payments made to beneficiaries other than the Foundation, which the petitioner may also fulfil within the framework of voluntary compliance.

The secondary claim was also unfounded, as the respondent has the legal right to publish its decision pursuant to Section 63/B(5) of the Privacy Act. The respondent decides on this within its discretionary powers, taking into account whether the gravity of the infringement of rights justifies publication. The gravity of the infringement is not only based on the fact that the provision of data not corresponding to reality is linked to a contract obliging the payment of several billion forints – although this in itself satisfies the requirement of reasonableness – but also on the fact that the infringement was committed by a key player in public administration. The gravity of the infringement at issue in the proceedings is not reasonably affected by how the respondent might provisionally assess it, nor by whether the breach of the substantive legal provision can be traced back to an interpretation of the law.

In view of the above, the respondent lawfully established the infringement against the petitioner by correctly interpreting the Privacy Act and reasonably assessing the evidence. The petitioner, who is obliged to publish the information, did not publish the Grant on the Platform with the data content specified in Section 37/C(3)(a)(aa) of the Privacy Act, as neither the amount of the grant nor the identification of the beneficiary corresponded to the actual facts. The court therefore dismissed the claim pursuant to Section 88(1)(a) of the Code of Administrative Court Procedure [Fővárosi Törvényszék 105.K.704.156/2024/12].

VI. The Authority's legislation-related activities

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	2025
Act	77	68	89	70	77
Government decree	74	56	56	55	58
Ministerial decree	15	16	53	36	33
Government decision	14	4	18	4	5
Other (Parliament decision, instruction, etc.)	16	19	17	11	9
Total	196	163	233	176	182

VI.2. Priority cases

VI.2.1. Amendment to the Act on National Security Services

The amendment to Act CXXV of 1995 on National Security Services (hereinafter: National Security Services Act), which entered into force on 1 January 2026, transformed the system of national security vetting primarily with the aim of reducing the number of more than ten thousand vetting procedures carried out annually on average by the Constitution Protection Office and thereby achieving cost savings. According to the amendment, the positions subject to national security vetting are defined exclusively by the National Security Services Act. The amendment does not affect judges who are subject to national security vetting; in their case, the positions requiring such vetting continue to be determined by the act on the legal status and remuneration of judges.

The amendment introduced the concept of simplified national security vetting, which is based on exposure to unlawful attempts at influence, covert attacks, or threats. Under the amendment, national security vetting continues to apply to those handling classified information and to persons holding key positions who are highly exposed to unlawful influence, covert attacks or threats. In addition, for those working in sensitive positions who are exposed – though not to an increased extent – to unlawful influence, covert attacks or threats, and who are employed by an authority or organisation handling classified information, national security protection is ensured through simplified national security vetting. As a result of the amendment, bodies handling classified information were required to review the positions subject to national security vetting, and the amendment itself also removed several positions from the list of those requiring mandatory vetting (e.g. ministerial commissioners, generals, employees of the Hungarian Atomic Energy Authority). If the information and data obtained during the simplified national security vetting do not reveal any circumstance that could affect employment from a national security perspective, the national security service issues a certificate instead of a security opinion. The certificate is valid for three years (whereas the security opinion is valid for five years).

The range of persons subject to national security vetting is designated by the initiating authority, within the quota determined by the minister supervising the national security service in an individual decision. For bodies under governmental control, the minister exercising direction or supervision proposes the size of the quota – together with justification – to the minister supervising the national security service. For employers not under governmental direction, the head of the employing organisation submits the justified proposal.
Under the amendment, the security questionnaire must be completed electronically.

VI.2.2. Amendments to the Act on the Protection of Classified Information and the Privacy Act

With effect from 21 February 2026, the Act on the Protection of Classified Information (Protection of Classified Information Act) was amended. The legislator repealed the rule that had previously required the mandatory fiveyear review of the classification of classified information. Pursuant to the amended Section 8 of the Protection of Classified Information Act, instead of the mandatory fiveyear review, a review becomes obligatory in the following cases: when there is a change in the conditions of classification; when a request is submitted to exercise the right of access under Section 17 of the Privacy Act; and when a request

is submitted to access data of public interest and data accessible on public interest grounds relating to the classified information. In these cases, the classifier shall review the national classified information created by them, their legal predecessor or another classifier, provided that the information falls within their responsibilities and powers at the time of the review. The classifier may involve an expert in the review.
In connection with this, Section 17 of the Privacy Act has been supplemented with a new paragraph (2a), which provides that if the data subject wishes to exercise their right of access and their personal data represent national classified information, and the classifier is not the controller or the processor acting on behalf of, or under the instructions of the controller, then the controller shall contact the classifier to carry out the review of the national classified information in accordance with the rules of the Protection of Classified Information Act and to inform the controller of the result. [NAIH-11843/2025., NAIH-12708/2025.]

VI.2.3. The Act on Govóernment Information

During the public consultation phase, the Authority received for review a single consolidated draft bill whose aim was to grant certain bodies under the control of the Government a legal basis to contact citizens directly and provide them with direct information about certain state measures or events affecting a broad range of the population.

Ultimately, the proposal was not submitted to Parliament as a single bill but was divided into several amendmenttype bills. The Act CXXII of 2010 on the National Tax and Customs Administration was supplemented with a new Section 80/A, under which NAV, at the request of a member of the Government and on the instruction of the minister responsible for tax policy, provides information to taxpayers affected by tax allowances, tax base reductions or tax exemptions defined by law, as well as to persons subject to optional preferential taxation rules, and processes their personal data to the extent necessary for this purpose. Processing personal data is required not only to determine the mode of contact but also to ensure that information is provided to the person to whom it pertains. The data subject may opt out of receiving such information by submitting a written declaration addressed to the NAV.

In addition to the provision concerning NAV, Act CXCV of 2011 on Public Finances was supplemented with a new Section 106/F, which assigns to the Hungarian State Treasury the task of providing information – on the instruction of the minister responsible for public finances – regarding support, benefits, allowances or

concessions granted to natural persons under conditions defined by law and falling within its remit, and to process the personal data necessary for this purpose. If the Treasury does not possess the personal data required for identifying the affected individuals, it may request such data from another state body or from the storage service provider connected to the governmental electronic identification service. The body or service provider thus contacted is required to provide the data without delay, and no later than within eight days.

Act CXXIII of 2020 on Family Farms was also supplemented with a new Section 13/A, which provides that the agricultural administration body may process the personal data of agricultural primary producers registered in the primary producer register for the purpose of providing information, and it must provide such information on the instruction of the minister responsible for agricultural policy. [NAIH-14543/2025.]

VII. Annexes

VII.1. The financial management of the Authority in 2025

We have passed the 14th 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 estimates and the data of its performance in 2025

The Authority accounted for operational-purpose funds received from an international organisation as prefinancing for the priority EU project titled “RAISING GDPR AWARENESS for microenterprises”.
Among the revenue data, the Authority’s operating income showed no significant change either in composition or in value compared to previous years. Most of the surplus revenue resulted from reimbursements related to business trips.
The 2024 budgetary carryover, when appropriated, increased the original revenue estimate by HUF 136.3 million.
In addition to the original budgetary support, the Authority received HUF 6 million during the year from the central budget to support the 2025 salary increases of elected officials and senior executives.

VII.1.2. Expenditure estimates and the data of its performance in 2025

Overall, it can be stated this year as well that, based on the experience of previous years, particular attention was paid to the costoptimisation of all concluded contracts; where necessary, negotiations were held to recalculate prices; nevertheless, financing the costs of work increased by the rate of inflation posed a significant challenge from a management perspective. Due to the expansion of the Authority’s tasks and the continuously rising number of cases each year, as well as the further growth of administrative and increasingly complex regulatory support activities, it was necessary to ensure adequate human resources to carry out the new tasks (an almost 16% increase in staff within a year).
The total expenditure on personnel allowances and related employer contributions exceeded last year’s figures by 15.6%. This increase was influenced by the continuous midyear rise in staffing levels noted above, taking into account optimised, balanced and responsible wage management.

With regard to operational and capital expenditures, the tasks at hand included creating a suitable work environment for new employees and upgrading the outdated financial management systems (a comprehensive upgrade and the introduction of electronic signatures), and purchasing office furniture for the newly hired staff. As EUlevel data protection and freedomofinformation tasks increasingly prompt state actors (partner authorities) to introduce new technological tools, the Authority took further steps to expand its existing artificial intelligence laboratory as well.

The Authority conducted a public procurement procedure for a construction project at its headquarters in Falk Miksa Street, in order to modernise the building's heating system, with a total value of HUF 269.5 million, including VAT. This amount was allocated proportionally to the Office of the Commissioner for Fundamental Rights, which also has its headquarters in the same building.

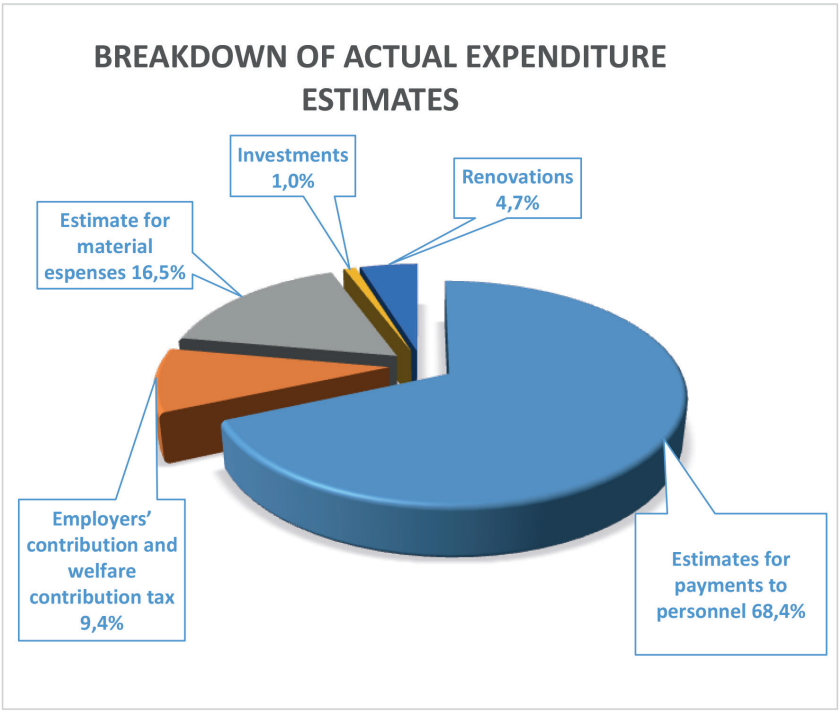
The Authority's 2025 carryover resulting from its core activities amounts to HUF 34.8 million, all of which constitutes committed appropriations.

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

Description	Original estimate	Amended estimate	Performance	2025 remainder from basic activity
Mediated services		1 432	1 432	
Exchange rate gain		21	21	
Other operational revenues		2 221	2 221	
Cost recovery		6 618	6 618	
Sale of tangible assets		3	3	
Funds received from an international body for other operational purposes		32 777	32 777	
Recovery of a loan for investment purposes		1 004	1 004	
Funds remaining from the 2024 budget		136 322	136 322	
Grant from central budget from Managing Authority	2 282 500	2 288 469	2 288 469	
Revenue estimates total:	***2 282 500***	***2 468 867***	***2 468 867***	-

Estimates for payments to personnel	1 666 500	1 680 911	1 665 515	15 396
Employers' contribution and welfare contribution tax	221 600	231 108	229 107	2 001
Estimate for material expenses	304 400	417 898	400 543	17 355
Investments		23 566	23 566	-
Renovations	90 000	115 384	115 384	-
Expenditure estimates total:	***2 282 500***	***2 468 867***	***2 434 115***	***34 752***

The following chart shows the actual expenditures for the revised estimates, broken down by percentage:



VII.1.3. Changes in the headcount of the Authority

As of 31 December 2025, the Authority's headcount according to labour law was 139.

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. This year, the Authority managed to keep staff turnover within an acceptable range, which required offering competitive salaries to employees. During the year, 14 employees left, and 20 new colleagues arrived. In 2025, 9 employees were on long-term leave, and 3 returned from long-term leave during the year.

VII.1.4. Changes in fine revenues

In 2025, the annual turnover of the Authority's fine account amounted to HUF 70.9 million. It remains important to note that the fines do not constitute revenue for the Authority but for the central budget.

VII.2. Recipients of the NAIH Commemorative Medal

Pursuant to NAIH Regulation No 19/2012 on the award of the "National Authority for Data Protection and Freedom of Information Commemorative Medal", the Medal may be awarded to individuals who have achieved outstanding, exemplary results of a particularly high standard in the field of data protection and the right to informational self-determination and freedom of information, or who have made a significant contribution to the attainment of such results. The commemorative medal, made of silver, is the work of master goldsmith Tamás Szabó. It is awarded annually on the occasion of Data Protection and Freedom of Information Day.

In 2025, the silver commemorative medal was awarded to Pál Könyves-Tóth in recognition of his contribution to the preparation of the first Hungarian draft law on information rights, as well as for his active role in shaping the rules on data protection and freedom of information in Hungary.

Pál Könyves-Tóth obtained a degree in electrical engineering from the Budapest University of Technology in 1964, followed by a degree in economics from the University of Economic Sciences in 1972. From 1964, he served as national manager at IBM; subsequently, he worked at the Computer Technology Training Centre and later held the position of head of department and subsequently deputy director, at the Computer Applications Company. In the early 1970s, he worked as a scholarship-funded development engineer in the United States, where his interest was drawn to the federal data protection legislation adopted in 1974. Following his return to Hungary, he joined the Hungarian Central Statistical Office, where he was engaged in matters relating to data protection and freedom of information. It was during this period that – through the active contribution of Pál Könyves-Tóth and László Sólyom – the first Hungarian draft act on information rights was prepared, which later served as the basis for the bill submitted to the Parliament. From 1989, he was a member of the Telecommunications Data Protection Working Party (the so-called "Berlin Group"), as well as of the Council of European Professional Informatics Societies, and from 1992, of the Telecommunications Interest Reconciliation Forum. He became an internationally recognised authority in the field of data protection. In recognition of his work, he was awarded the Neumann Prize by the John von Neumann Computer Society in 1986. He authored numerous publications in the field of information rights. In addition to his work in data protection, he also served as responsible editor of several prominent professional journals in the field of information technology. Pál Könyves-Tóth undeniably laid the foundations of data protection in Hungary; it is no exaggeration to describe him as one of the founding figures of data protection in Hungary. At the award ceremony held in December, we were honoured by the presence of the family of Pál Könyves-Tóth.

VII.3. Highlights from the Authority's Daily Activities

The 30th anniversary of the institutional system of information rights in Hungary was commemorated within the framework of an international conference.

33rd Children's Day in Városliget – Safer Internet Awareness Tent

Joint ceremonial reception held in Brussels on the occasion of the 45th anniversary of the establishment of the Austrian Data Protection Authority and the 30th anniversary of the institutional system of information rights in Hungary.

Dr. Kovács Tamás Iván, Ambassador, Dr. Júlia Sziklay, Deputy president for international affairs, Dr. Franz Wirtenberger, Ambassador, Dr. Matthias Schmidl and Dr. Attila Péterfalvi, President

The Spring Conference of European Data Protection Authorities – Batumi, Georgia

A cooperation agreement was signed between NAIH and the Turkish Data Protection Authority.

Mr. Muhammed Serdar Cafoğlu, Prof. Faruk Bilir, Dr. Attila Péterfalvi, President, Dr. Júlia Sziklay, Deputy president for international affairs and Ms. İrem Arık

NAIH was represented by Dr. Júlia Sziklay, Deputy president for international affairs at the 15th Media and Internet Conference

Table of content

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)