National Authority
for Data Protection
and Freedom of Information

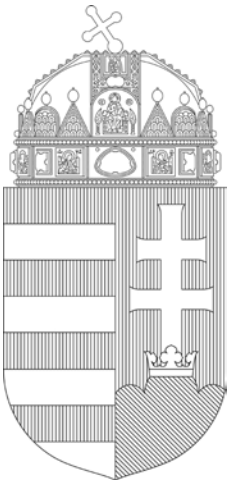
ANNUAL REPORT OF THE HUNGARIAN NATIONAL AUTHORITY FOR DATA PROTECTION AND FREEDOM OF INFORMATION (NAIH) 2023

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

on its activities in 2023

B/7156

Nemzeti Adatvédelmi és Információszabadság Hatóság
(Hungarian National Authority for Data Protection and Freedom of Information)
Budapest, 2024.



Introduction

Greetings Dear Reader,

In recent years, due to the challenges of the 21st century, a comprehensive renewal of the digital space landed in the focus of data protection regulation. In 2023, there were significant advances to adopt the EU digital regulation package, as a result of which the responsibilities of NAIH also expanded.

One of the elements of outstanding importance of the new regulations is the Data Governance Act or DGA for short. DGA aims for data--centred innovation, i.e. to facilitate data sharing among strategic areas and branches (such as healthcare, environment protection, energy, finances, public administration, etc.) and EU Member States with a view to exploiting the opportunities in data for the benefit of European citizens and undertakings. As of 1 January 2024, NAIH acts as the "competent authority" according to DGA. (More detailed information on the new EU digital regulations is available in the chapter "*EU digital regulations (current affairs)*".)

Changes can be reported also in national regulation: at its session on 13 December 2023, Parliament adopted the Act on the System of the Use of National Data Assets and Certain Services, whose amendments affecting Act CXII of 2011 on the Right to Informational Self-Determination and the Freedom of Information entered into force on 1 January 2024. Inter alia, the amendment assigned responsibilities and powers for the regular supervision of the implementation of the requirements concerning the transparency and accessibility of data of public interest and data accessible on the grounds of public interest and the related reporting obligation to NAIH. The amendment introduces a new reporting obligation, expanded relative to the former scheme, with regard to organs performing public duties, municipalities and business organisations in public ownership to be met by 31 January of each year by providing data on the preceding year (see in greater detail in the chapter on *Freedom of information*).

The expansion of responsibilities implied changes in personnel: as of the second half of 2023, two vice presidents assist the president in his work: a general vice president in charge of general affairs and an international vice president acting in relation to EU and international affairs.

For the third time since NAIH's establishment, the spring conference of the European data protection authorities was organised again in Budapest in May 2023, receiving visitors from 39 countries. The goal of the conference convened each year is to promote cooperation and the exchange of good practices among the members of the conference (accredited EU and non-EU data protection supervisory organisations) with a view to the promotion and maintenance of the protection of personal data and privacy in Europe. Based on an idea of Giovanni Buttarelli, a former European Data Protection Supervisor, the novelty of the May conference was that in addition to the close sessions organised for accredited members an open day was also included accessible to the interested public, whose subject matter was the presentation of the role and functions of the data protection officer.

Another important event in 2023 was the ratification of the Data Protection Convention of the Council of Europe (the so-called Convention 108+) by Hungary as the 30th country. The two objectives of modernisation – while continuing to respect the principles – were to reflect on the challenges of the digital age and to reinforce the monitoring mechanism of the Convention. The merit of the 1981 Convention was that this was the first internationally binding document to include the right to the protection of personal data derived from but independent of the right to the protection of privacy and to this date, this is the international data protection legal norm with the broadest territorial scope.

Budapest, 20 February 2024

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

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

I.1. Statistical characteristics of our cases

In accordance with the objectives of the National Digitalisation Strategy (2021-2030), and in line with the Authority's IT strategy, the Authority strives to support the implementation of digital, organised, consistent and transparent institutional operation expected from the organs of state administration with the least possible administrative burden at the level of an administrative authority.

The reduction in the administrative burden is a complex task, which at front office level means an option to launch and conduct cases online in a customer-friendly and rapid manner on the one hand, and the maintenance of electronic contact through the use of regulated electronic administrative services, on the other hand. At back office level, it means streamlining and digitising file management and administrative processes, as well as reducing the lead times of processes.

Our strategic objective continues to include the widest possible implementation of e-administration through the introduction of new e-administration services and the necessary development of related internal systems. The implementation of e-administration services requires the digitalisation of the processes and the implementation of a paper-free, fully electronic back-office, meaning an improvement in the specialised electronic systems, the development of the processes and, if possible, their automation in administration, in customer relations, as well as in back-office processes. More widely automated processes save on time, resulting in cost reductions; further digitalisation increases the accessibility of the results of the authorities' work and requires substantially less assets.

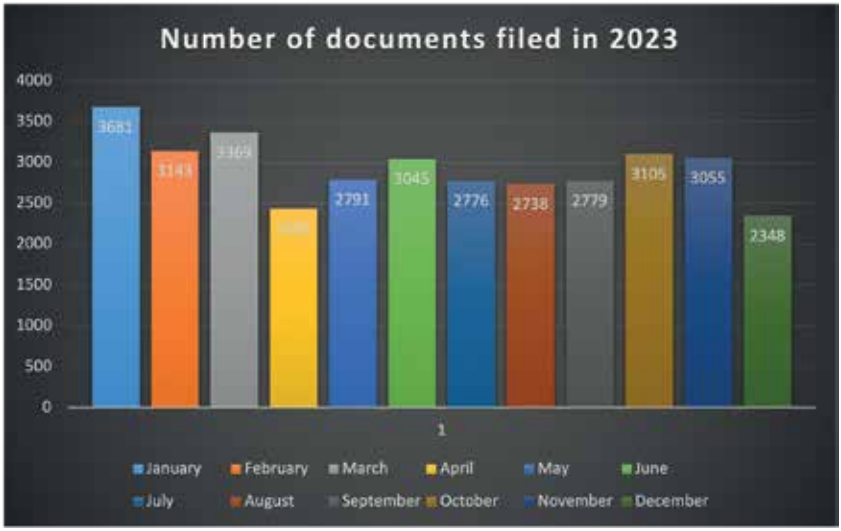
We are continually searching for solutions, which facilitate more efficient management of internal processes, information flows and available resources. The goal is to align the internal and external processes of the organisations, by improving in-house communication, a more efficient use of the authority's resources and the accessibility of real time data for decision makers.

As a result of the expansion of tasks in the various professional areas and on the basis of the number of cases showing an increasing tendency year-after-year, the Authority expects a further expansion in administrative tasks and the tasks

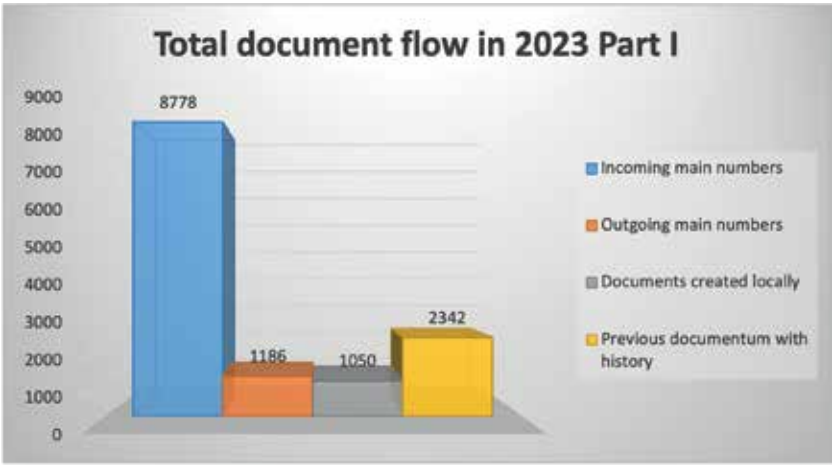
supporting its increasingly complex operation. The file management system currently employed by the Authority no longer provides full support for the secure discharge of these tasks, which necessitates and warrants the implementation of a new file and document management system in the near future.

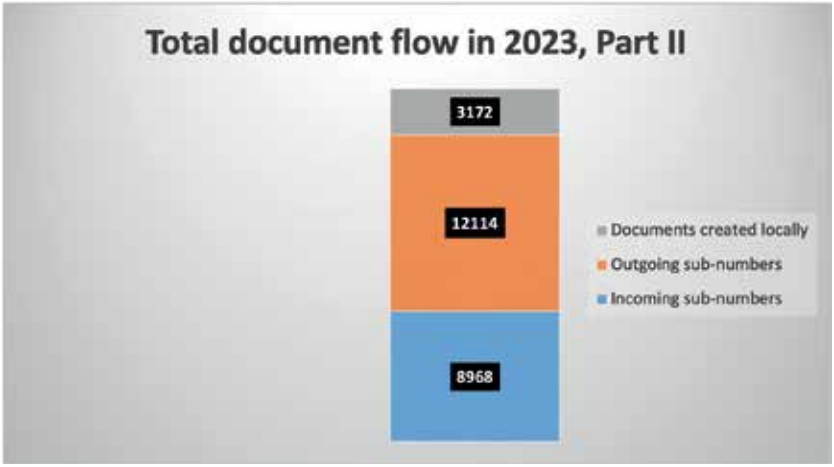
Such a new system may enable the use of modules dealing with specialised tasks, working in an integrated manner with the file management system. Its elements will be available to the Authority and its clients in a uniform, organised and transparent structure. The flexibility and scalability of the new system may provide the foundations for expanding both current and future requirements ensuring data integrity and data security through the application of the appropriate processing procedures and security measures.

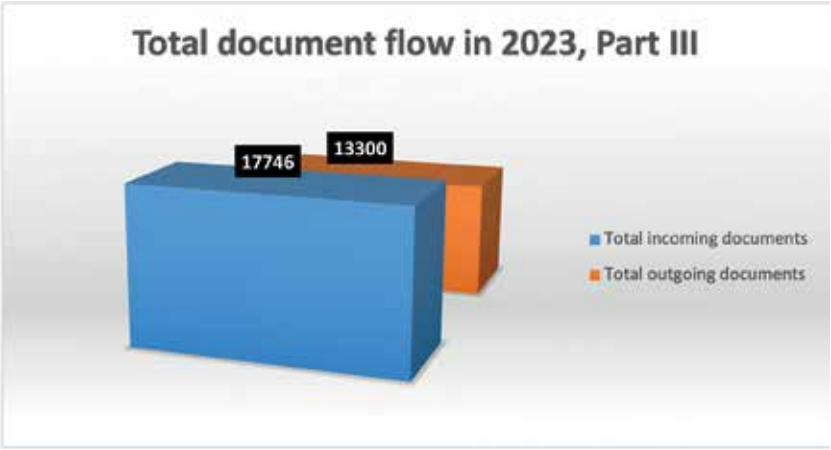
The Authority has already begun preparing for the tasks related to the planned implementation of the new system, data migration, setting the parameters of the system, system integration and the development of the new file management processes, which arise in parallel with the simultaneous and continuous discharge of the daily tasks of case management, administrative engineering, coordination and administration.



Document statistics of the Authority in 2023







In 2023, 8,672 new cases were filed in the Authority's specialised internal case administration system. Together with cases from earlier years (2,342), altogether 11,014 cases were in progress. The number of cases substantially rose relative to last year's numbers exceeding them by close to 1,300.

A comparison of the data series reveals that the number of authority cases increased by almost fifty percent (from 708 to 1,040) relative to the preceding year; a similarly steep rise was seen in the number of cases related to GDPR cooperation (IMI) (from 1,489 to 1,846). In addition, the number of investigations and submissions for consultation also exceeded the number of cases in the preceding year.

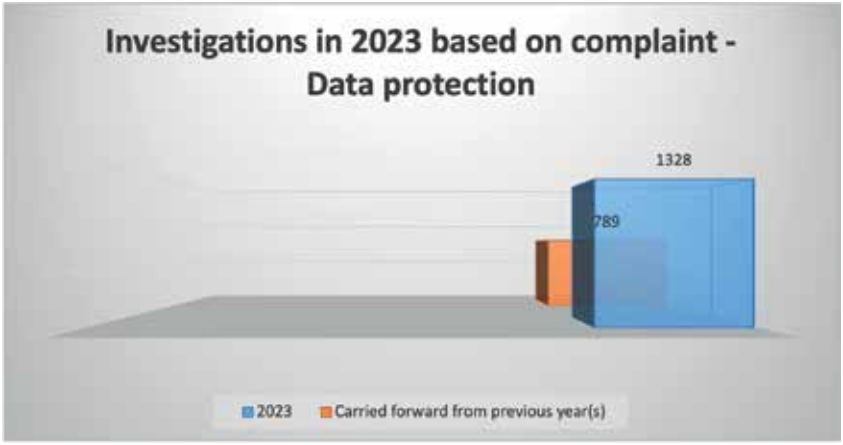
The Authority's case types with the most significant case numbers in 2023

Investigative procedures	**2,894**
Consultative procedure	**1,410**
Authority investigations	**715**
Providing opinion on legal regulations	**206**
GDPR cooperation (IMI)	**1,846**

Investigative procedures in 2023 – Data protection

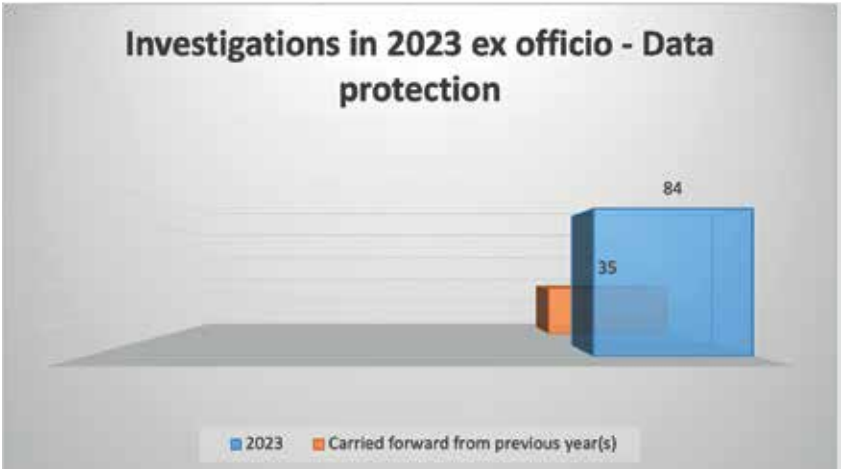
Investigated cases based on complaint in 2023

2023	**1,328**
Carried over from previous year(s)	**789**



Investigated cases ex officio in 2023:

2023	**84**
Carried over from previous year(s)	**35**



Data protection investigative procedures in 2023 per case type

Case type	*Total*	*Carried over from previous years*	*New cases*
Investigative procedure ex officio	**119**	**35**	**84**
Investigative procedure ex officio in data protection case - Law Enforcement Directive	8	5	3
Investigative procedure ex officio in data protection case - GDPR and other	110	30	80
Investigative procedure ex officio in data protection case - GDPR and other - data breach	1	-	1
Investigative procedure based on complaint	**2,117**	**789**	**1,328**
Investigative procedure based on complaint in data protection case - data breach	220	57	163
Investigative procedure based on complaint in data protection case - Law Enforcement data breach	5	5	-
Investigative procedure based on complaint in data protection case - Law Enforcement Directive	72	37	35
Investigative procedure based on complaint in data protection case - GDPR and other	1820	690	1130

Investigative procedures in 2023 – Freedom of information

Investigated cases based on complaint in 2023

2023	**503**
Carried over from previous year(s)	**150**

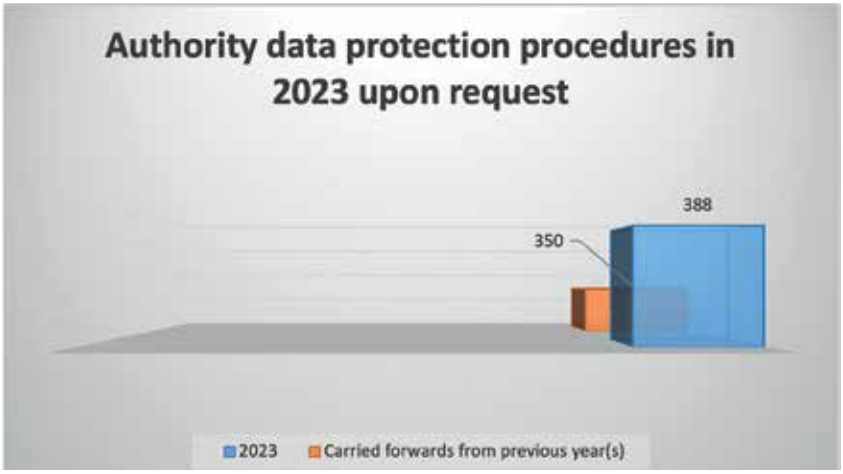
Investigated cases ex officio in 2023

2023	**4**
Carried over from previous year(s)	**1**

Number of Authority procedures for data protection in 2023

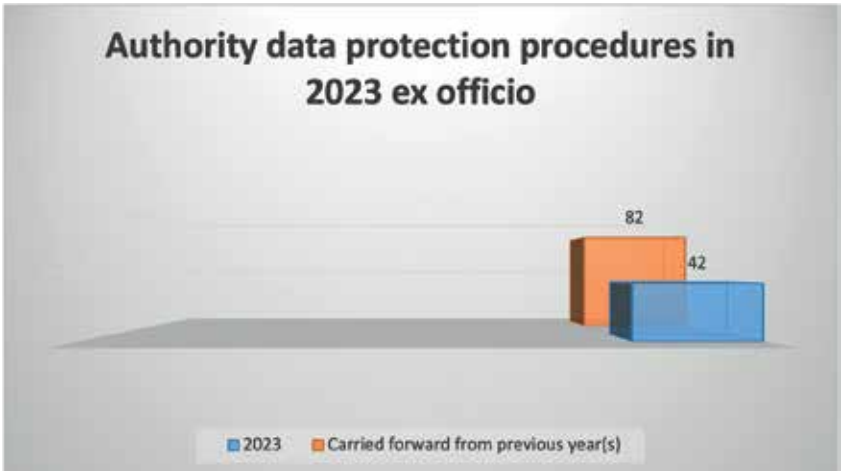
Number of Authority procedures for data protection based on petition in 2023

2023	**388**
Carried over from previous year(s)	**350**



Number of Authority procedures for data protection ex officio in 2023

2023	**42**
Carried over from previous year(s)	**82**

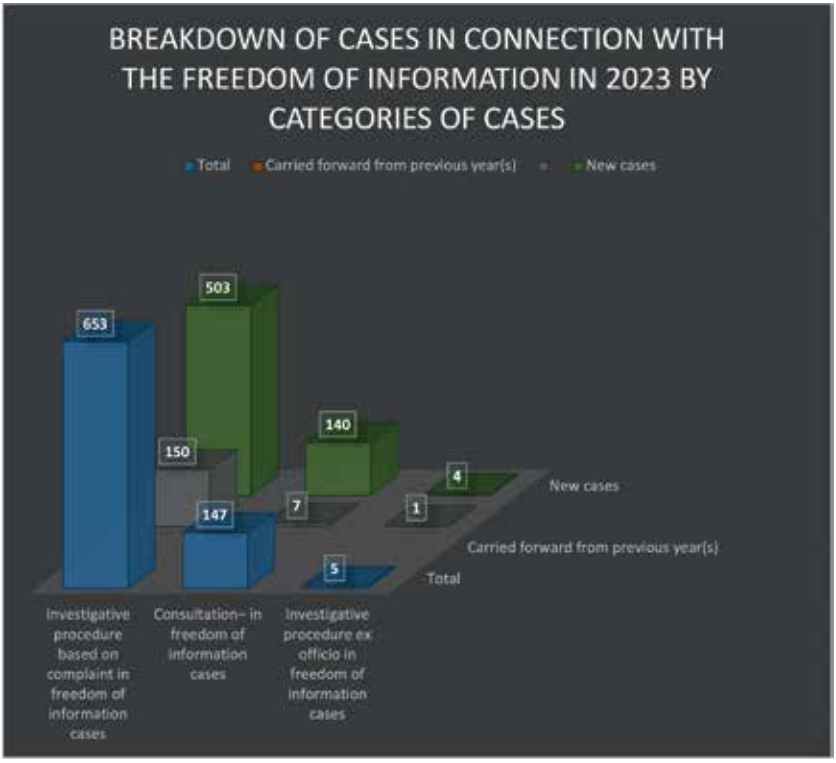


Authority procedures for data protection per case type in 2022

Case type	*Total*	*Carried over from previous years*	*New cases*
Authority procedures for data protection ex officio	**124**	**82**	**42**
Authority procedures for data protection ex officio - Law Enforcement Directive	5	4	1
Authority procedures for data protection ex officio - Law Enforcement Directive - data breach	3	1	2
Authority procedures for data protection ex officio - GDPR and other	83	55	28
Authority procedures for data protection ex officio - GDPR and other - data breach	33	22	11
Authority procedures for data protection ex officio - GDPR and other - freedom of the press and expression	-	-	-
Authority procedures for data protection based on petition	**738**	**350**	**388**
Authority procedure for data protection based on petition - Law Enforcement Directive	24	16	8
Authority procedure for data protection based on petition - Law Enforcement Directive - data breach	2	2	-
Authority procedure for data protection based on petition - GDPR and other	666	313	353
Authority procedure for data protection based on petition - GDPR and other - data breach	44	19	25
Authority procedure for data protection based on petition - GDPR and other - freedom of the press and expression	2	-	2-

Distribution of freedom of information cases in 2023 by case type

Case type	*Total*	*Carried over from previous years*	*New cases*
Investigative procedure based on complaint concerning freedom of information	653	150	503
Consultation - freedom of information	147	7	140
Investigative procedure ex officio - freedom of information	5	1	4



Changes in the number of Authority procedures for transparency in 2023

Ex officio Authority procedure for transparency launched upon notification	13
Ex officio Authority procedures for transparency	149

Changes in Authority investigations in 2023

Investigations in 2023	**715**
Carried over from previous year(s)	**151**

Case type	***Total***	***Carried over from previous years***	***New cases***
Authority investigation for data protection - Law Enforcement Directive	-	-	-
Authority investigation for data protection - Law Enforcement Directive - data breach	33	17	16
Authority investigation for data protection - GDPR and other	25	10	15
Authority investigation for data protection - GDPR and other - data breach	657	124	533

Number of opinions on legal regulations in 2023

2023	**200**
Carried over from previous year	**6**

Case type	***Total***	***Carried over from previous years***	***New cases***
Opinions on regulations upon request (opinions and consultation on draft legal regulations)	**202**	**6**	**196**
Recommendation for legislation (draft regulation, opinion, own, initiated by those applying the law)	**4**	**-**	**4**

Important areas of international cooperation in 2023 (GDPR, IMI)

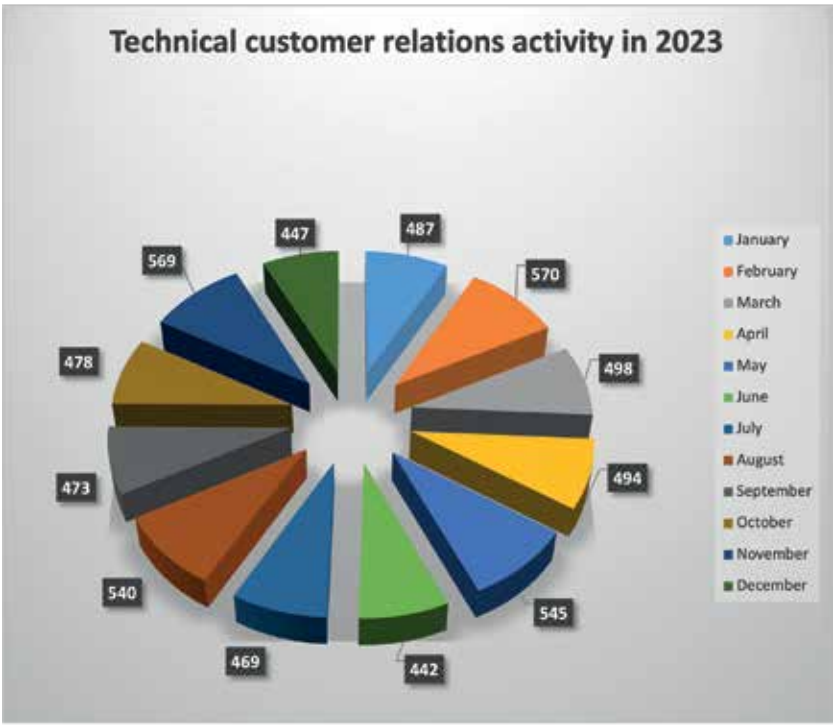
2023	**1,390**
Carried over from previous year	**456**

Case type	***Total***	***Carried over from previous years***	***New cases***
Cooperation with other EEA supervisory authority as authority concerned - data breach	**13**	**5**	**8**
Cooperation with other EEA supervisory authority as authority concerned, GDPR 56,60,61,62,64,65	**1,828**	**451**	**1,377**
Cooperation with other EEA supervisory authority as authority concerned - freedom of the press and expression	**5**	**-**	**5**

In 2023, the Authority's customer service received 6,012 phone calls. The number of face-to-face client receptions increased slightly (78), while there was no change of merit in the number of in-person inspections, which can be requested in administrative authority procedures (55).

Beyond the issues highlighted in our earlier reports, our clients primarily requested information on the mode of lodging submissions in relation to Act XXV of 2023 on Complaints, Whistleblowing and the Rules of Reporting Abuses (new Complaints Act).

In addition to providing specific assistance, the Authority's customer service staff called attention to the Guidelines published on NAIH's website (link: https://naih.hu/panasz-vagy-kozerdeku-bejelentes-a-panasztorveny-szerint#_ftn7), which sets out in detail the notions of complaint and whistleblowing and the various modes of reporting them.



In 2023, our customer service staff provided general information in writing in response to requests for appointments related to the submission of complaints in 9 cases, and they also provided assistance in informing clients about the ways in which data subjects can turn to the Authority in relation to their cases concerning the protection of personal data or access to data of public interestor data accessible on the grounds of public interest.

I.2. Annual conference of data protection officers

In November 2023, the President of the Authority sent out invitations to the conference of data protection officers to the 4,461 data protection officers notified to it through the electronic data protection officer notification system used by over 12 thousand controllers and processors, in view of the provisions of Section 25/N of the Privacy Act and he surveyed the general preparedness and the needs of data protection officers through the EU survey system, and provided an opportunity for them to shape the content of the presentations at the conference and to submit proposals for subjects.
The primary objective of the conference is to develop a uniform practice in the course of the application of legal regulations concerning the protection of personal data and access to data of public interest, and to provide regular professional contact between the Authority and the data protection officers. In view of the large number of the data protection officers notified to the Authority and the right of participation due to all of them, and to promote a high degree of utilising the professional information developed, the conference was again organised exclusively in electronic format in 2023.

Similarly to the conference videos of earlier years, the presentations compiled on the basis of the results of the survey and the questions posed are accessible in the Authority's website thanks to MTVA's Médiaklikk service.

In his welcome address, **Dr. habil Attila Péterfalvi** first reviewed the most recent EU regulatory changes affecting the powers of the Authority focusing in particular on the Digital Services Act aimed at reforming the world of online platforms and the Data Governance Act that also affects the Authority's powers.

He also assessed the annual statistical data of the Authority's operation highlighting the positive experiences of the transparency procedures regarded as a novelty of 2023 and the cases also concerning the Authority received through the IMI system. In addition, he referred to several decisions in which the Authority took a stand concerning issues with long-term effects, including the resolution containing statements related to the use of artificial intelligence, and the decision concerning paparazzi activities affecting former public figures.

Júlia Sziklay PhD, vice president for international affairs, expounded the 2023 EU data protection developments in greater detail in her presentation. In the field of uniform data protection cooperation, the role of the European Data Protection

Board and its most important documents adopted during the year and the one-stop-shop trans-border cooperation of supervisory authorities were discussed.

Among the opinions adopted by the EDPB, the opinion concerning the US Data Privacy Framework (opinion 5/2023) and the EDPB-EDPS joint opinion on the proposal for a regulation laying down additional procedural rules relating to the enforcement of GDPR (joint opinion 01/2023) were presented in detail in view of their particular significance.

Following a review of the most important dispute settlement procedures of the Board, Dr. Júlia Sziklay presented EDPB's most important guidelines, focusing on the main elements of content of Guideline 01/2022; then she summarised the most important data protection related decisions of the Court of Justice of the European Union highlighting Ruling C-307/22 on the release of a copy of medical records.

Dr. Norbert Vass, head of division, was the first to provide information on the novelties of the Digital Package of the European Union as several of its elements have an impact on the protection of personal data. Following a review of various aspects of digital sovereignty, he reviewed the legislative acts included in the Digital Package.

On account of the Digital Services Act (DSA), applicable to those providing intermediary services in the internal market from February 2024, its risk-based approach was highlighted among other things, which specifies stricter requirements for the large online platforms in its regulatory structure and contains other procedural guarantees as well. The Data Governance Act (DGA) regulates access to publicly held databases, technically through the establishment of a central one-stop-shop agent, and it also regulates the operation and supervision of data intermediation undertakings and data altruism organisations.

In addition, participants were able to receive information on the detailed rules of the Data Act regulating data sharing between undertakings (B2B) and the uniform regulatory challenges of a new processing tool arising in relation to the Artificial Intelligence Act (AI Act) and the listing of prohibited and high-risk AIs. The expert delivered a separate presentation on the relevant related experiences of the Authority demonstrating the serious technical and social difficulties in defining artificial intelligence through the cases of Budapest Bank and ChatGPT.

In addition, he addressed the main elements of the amendments to the Regulation on Electronic Identification and Trust Services (eIDAS), including the aspects of

establishing a European digital identifier, which counts as a major novelty, as well as the developments related to digital citizenship. The Interoperable Europe Act primarily addresses the regulation of the online procedures in the public sphere and their transborder interoperability; in the event of the implementation of new electronic public administration systems, which also process personal data, the Authority will be mandated to perform the supervision of test operation and of legal compliance in a mandatory test environment prior to commissioning according to the current draft.

Dr. Gergely Barabás, head of department, summarised the novelties in EDPB Guidelines 4/2022 on the calculation of administrative fines under the GDPR adopted as a result of several years of preparatory work and public consultation in the spring of 2023. The goal of the Guidelines is to harmonise the methodology used by supervisory authorities to calculate fines to be levied on controllers and processors regarded as undertakings. However, the Guidelines also underline that it is also possible to levy fines on natural persons – provided that they are otherwise controllers – based on the General Data Protection Regulation as the practice of Hungarian and other EU supervisory authorities show in levying fines on natural person controllers in many cases.
In his introduction, he focused at first on recalling the essential content of Article 83 of the GDPR, then he pointed out the EU principles, which justify the adoption of separate guidelines in addition to the GDPR provisions, which determine the calculation of the data protection fine in detail. With respect to the content of the Guidelines, he called attention to the fact that the calculation of the amount of the fine continues to be at the discretion of the supervisory authorities, what is expected in the course of calculating the fine is not a mathematical demonstration, but giving due regard to the explored circumstances of a specific case subject to the rules provided for in the GDPR. The supervisory authorities of the Member States still have to justify the calculation of the amount of the fine based on their own national procedural rules.
The Guidelines developed a “five-step method” to determine the amount of the administrative fine, whereby a radically new viewpoint rooted in criminal law appeared in data protection law; the presentation addresses these in detail.

Dr. Dániel Eszteri PhD, head of division, presented the main decisions of the Authority in related to data breaches from 2023. He mentioned, inter alia, NAIH’s statement concerning the issue of transferability of obligations related to data security to the data subject. After this, he shared the lessons of a procedure launched in relation to a data breach, which took place because of a vulnerability of an obsolete content management system, with the participants of the confer-

ence, and then he addressed the data breach affecting processing related to the administration of a primary election. He closed the list of the most important data breach cases of the year by assessing the non-compliant data breach practices by a district heating supplier.

The presentation of **dr. Éva Tóth** dealt with the new disclosure obligations of budgetary organs; then she provided insights into the experiences of the Authority procedures for transparency. Underlining the significance of the new disclosure obligation, she emphasised that organs discharging public tasks and using public money often failed to meet their general disclosure obligations appropriately according to the Privacy Act, the Authority's statements concerning disclosure were not enforceable to this day and citizens could not turn to the courts in the event of a failure to disclose. So, one of the most important results of the new regulation was putting an end to the "lack of consequences" in the field of publishing financial management data as the Authority's decisions made in authority procedures for transparency are enforceable with the expansion of the sanctioning powers of the Authority. In the remaining part of her presentation, she addressed the detailed rules of the new obligation as set forth in the Privacy Act, as well as the possibilities for the further improvement of the regulation.

Dr. Attila Kiss, head of department, presented the 2023 results of surveys concerning data protection officers. Since 2020, the European Data Protection Board has launched coordinated surveys focusing on various areas of data protection and NAIH also joined the coordinated enforcement framework in 2023. Currently, the role and legal status of data protection officers was investigated; in relation to this, the Authority focused on the officers of the Hungarian public sector.

Based on a direct questionnaire methodology, he summarised the preliminary results and main statements and identified several factors involving serious risks. He also compared the results of the coordinated survey related expressly to data protection officers in the public sector with the results of the survey covering all data protection officers notified to the Authority which was carried out prior to the conference.

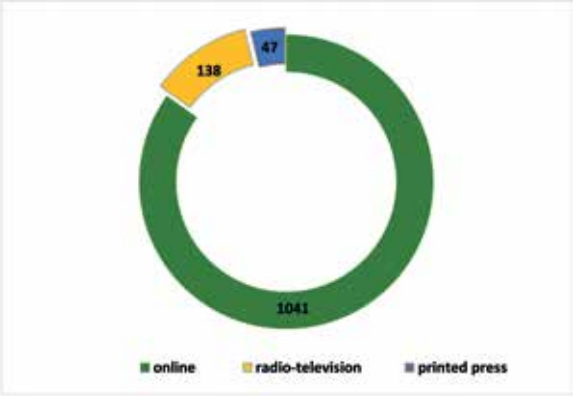
Finally, he answered groups of questions received from data protection officers in relation to the conference including questions on the conditions of using cloud services outside the European Union, interest in the content of data protection obligations of organs discharging public duties, measures expected because of the differences in the notion of consent according to the Civil Code and

the GDPR, and questions related to the possible legal basis for processing implemented through recording images.

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

Between 1 January and 31 December 2023, members of the media published altogether 1,227 news items about the Hungarian National Authority for Data Protection and Freedom of Information. As to the types of media, most of the time news on the activities of the Authority were broadcast by the online media, altogether on 1041 occasions. NAIH was presented in the printed press in 47 cases and 138 times in the electronic media.

Share of NAIH's appearances in the various media in 2023



Source: Observer Budapest Médiafigyelő Kft.

II. Data protection cases

II.1. Application of the General Data Protection Regulation

II.1.1. Data processing by forensic experts

In its 2022 annual report, the Authority demonstrated the identification of several problems with the interpretation of the law in relation to processing operations carried out by forensic experts. As a continuation of this theme, and based on the experiences of additional investigations into processing operations by forensic experts, the Authority pursued professional reconciliation with the representatives of the Hungarian Chamber of Forensic Experts in the summer of 2023, in the course of which a number of theoretical and practical issues were discussed. According to the common standpoint of the Chamber and the Authority, there is a need for the amendment of legal regulations in this field. The Authority sent its recommendations concerning legislation in family law affecting Act XXIX of 2016 on Forensic Experts (hereinafter: Forensic Experts Act) to the Ministry in charge of the preparation of legislation.

Particularly with respect to the exercise of data subject's rights concerning personal data generated in the course of investigations by forensic psychologists assigned in family law litigations, the Authority found that the assigning orders of the courts did not include instructions concerning the restriction or granting of access. At the same time, the assigned expert is subject to confidentiality obligations and a situation may arise when whatever a minor tells the expert in the course of the investigation contains information, which when accessed by the legal representative, may have detrimental consequences for the child. According to the procedural experiences of the Authority, in such cases the assigning court issues an order on rejecting the right of access subsequently upon the initiative of the expert; however, there have been examples when the court – instead of bringing a decision – found that it had no competence. In the case of authority procedures for data protection initiated before the Authority by parents or legal representatives on account of the infringement of the right to access, the decision requested by the expert from the assigning court is a preliminary question, which results in the suspension of authority procedures for data protection initiated by petition. In view of the above and bearing the interests of children in mind, the Authority believes it is justified that the assigning court brings a decision concerning this in every case. To ensure this, it is necessary to amend the

relevant provisions of the Forensic Expert Act and the Civil Procedures Act, so that the assigning authority or court makes the decision on the right to access not in advance, but taking into account the experiences of the expert examination. [NAIH-6627-1/2023]

The next question arising among these problems was the legal basis of processing by a private expert. Section 53(1) of the Forensic Expert Act restricts the legal basis of processing to the data subject's consent, while according to the GDPR, processing can be pursued according to any one of the legal bases listed in Article 6, hence this section of the Forensic Expert Act should also be reviewed with a view to compliance with the GDPR.

Practical problems arose also in relation to sound recordings made by the expert, which is based on the rule, according to which "*the expert may make voice recordings in the course of the examination, if the person under examination, or their legal representative, give their written consent*". For the expert, the purpose of making and using the voice recording is to reconstruct whatever was said in the course of the examination and to provide a reasoned professional opinion based on that. However, in practice, it is not always clear for the experts how long is keeping the recording justified and lawful and up to what point of processing a data subject may exercise the right to withdraw their consent. According to a grammatical interpretation of the provision of the relevant Ministry of Justice and Policing Decree[1], the data subject's consent can be regarded as granted only to making the recording and the scope of the consent does not extend to the use of the recording – while the purpose of making and using the recording is identical in accordance with what was said above. So, the expert makes and uses the recording pursuant to Section 40(1) of the Forensic Experts Act on the legal basis of meeting a legal obligation; however, when the purpose is achieved – which may be the completion of the transcript or access to it by the data subject, the recording may not be erased because Section 42 of the Forensic Experts Act stipulates a mandatory retention time. The possibility of withdrawing consent is a fundamental condition of applying the legal basis of consent. In the case referred to, however, consent cannot be regarded as a valid legal basis even for making the voice recordings, because of the questionability of the withdrawal of consent. In view of this, the Authority recommended to the Ministry of Justice to annul Section 20/A(3) of the Ministry of Justice and Policing Decree and the clarification of the provisions on making and using voice recordings. The provision referred to was annulled. Further, according to the response of the Ministry of

1 Ministry of Justice and Policing Decree 31/2008. (XII. 31.) on the operation of forensic experts

Justice, the problem may be fully settled during the conceptional review of legal regulations affecting expert activities. [NAIH-4665/2023].

II.1.2. Cases concerning health-related documentation

Another area often affected by the right of access exercised by legal representatives representing their children is the processing of health-related documentation.

Currently, the right to a copy of health-related documentation as a patient's right is not separately named in the sectoral regulation; it can be enforced through the exercise of data subject's rights arising from the rules of data protection: the right to access is declared by the Act on Healthcare, while its enforcement, i.e. the request for copies may be pursued according to rules of the GDPR. Because of this regulation, the Authority disagreed with the position taken by the Ministry and the ombudsman, according to which "*the service provider meets their obligation to provide information by providing it to any of the parents in case of parents living separately, but exercising parental supervision jointly*". The patient – in the given case, the child – is the data subject of the processing of data in the documentation and the rules of the GDPR apply with regard to the data subject and while ensuring the data subject's right of access exercised by the legal representative. Both parents of the data subject child, who live separately but exercise parental supervision jointly, have the right to legally represent the child, hence they are also individually entitled to enforce data subject's rights on behalf of the child acting within the framework of exercising data subject's rights as set forth in the GDPR. Because of this, the controller healthcare provider may not refuse to grant the right of access to either legal representative because they have already issued the documents to the other parent under the cooperation according to the Civil Code. At most, the service provider may consider other conditions of enforcing rights, such as multiple requests for copies by the data subject, disproportionate or excessive request, etc., but they cannot refuse the right to access by the data subject with reference to the parents' obligation to cooperate because the GDPR does not include such a criterion of restricting access. Because of this, such a practice is contrary to the GDPR rules, i.e. to ensuring the enforcement of data subject's rights.

An investigation before the Authority essentially related to the enforcement of this right when a complainant weekly requested the full health-related documentation of his three children from the family physician and the family physician handed over the documentation by blocking some parts. A family law dispute

has been in progress between the complainant and his wife for several years, the main issue of which is the custody and right to supervise their three children. To improve their situation in the litigation, both parents have been trying to collect evidence against the other parent and data to improve their respective positions in the litigation, even exploiting the care of the children. The physician blocked the parts in the copies handed over, which in his view, contained stories told by the other parent and communications containing secrets in correspondence and private information subject to the protection of personality rights (for instance, one parent defames the other, or the other parent details the threats she had already received in the family lawsuit), or contained details of a procedure by the government office in progress. The Authority's investigation found that a number of data were recorded in the medical system, which conceptually exceed the data content to be recorded in health-related documentation, some of the examined entries were not related to the examination and treatment of children according to Section 136 of Act CLIV on Healthcare (hereinafter: Healthcare Act) and they were not at all related to the healthcare of the children. The information provided by one of the parents were recorded in the service provider's system as comments unrelated to the child and these qualify as the personal data of the given parent and the other parent is not entitled to access them by exercising the right of access on behalf of the child. At the same time, the parts which relate to the children (such as the clothing of the children and eventual sicknesses that may arise from that, or the fact that the children regularly attend other physicians, etc.) cannot be regarded as parental comments not at all related to the care of the children, nor can it be stated that these parts constitute content that are not related to the children, irrespective of the fact whether their recording was justified as part of the documentation, hence the Authority ordered that they should be issued without blocking. The Authority called the attention of the family physician to the fact that he should record relevant data in the Complaint-Diagnosis-Opinion columns of the children's care only, because these are forwarded to Healthcare Service Space (hereinafter: EESZT) while other information should be stored in a different way.

The case also shed light on the unfortunate situation indicated by many similar complaints submitted to the Authority that following separation, parents are unwilling to cooperate with one another in many cases, although their cooperation in the interest of the children would be their obligation required under the Civil Code and parents tend to use the agency or person looking after the child to verify their perceived or real truth. In this case, it did not serve the children's interest that the children were forced to change physicians in the course of their paediatric care, which fundamentally functions as a relationship of trust, because the family physician was faced with a disproportionate burden when ensuring the

enforcement of parental rights, which could be traced back to the absence of parental cooperation. [NAIH-3606/2023]

A complaint of a different nature, but still concerning health-related documentation, was that the healthcare provider requested copies of the entire ID and social security card of the data subject in order to let the data subject have electronic access to their health documentation. The service provider indicated the enforcement of the principle of accuracy as the justification for requesting the copies, as this could do away with any eventual mistyping of names and numbers in the request. According to their statement, this also decreases the possibility of misusing the data of the petitioner (personality theft), which also decreases the risk of issuing by the university as controller the data subject's data to a person, who is not authorised to receive them. As this was a matter of processing special category data, unauthorised access to which could cause severe damage to the data subject, increased precautions are taken to check the authorisation; compliance with the requirement of accountability requires verification of who the documentation was issued to, when and based on what authorisation. According to the Authority's position, in addition to ensuring data subject's rights, the controller has an equal obligation in warranting data security and taking all measures whereby the unauthorized transfer of the data can be avoided. Health-related data as special category data enjoy particular protection, so it is not only a fair demand on the part of the controller, but also a legal obligation, to ensure prior to its issuance that the health-related documentation has been indeed requested by the authorised individual, and it is delivered to him,.

According to the consistent practice of the Authority, a copy of an ID card is not suitable *for checking personal identity*, it may however, be suitable for making a presumption about the person of the petitioner and *his authorisation*. If the petitioner has copies of the ID cards, there is a lower chance of abusing health-related documents and request them in the name of somebody else. However, the controller is authorised to process the data content of the ID copy only within the range, in which it processes the personal data of the data subjects in any case. The range of personal data included in the full copies of the ID card – photo and document identifier – is wider than the range of data, which the healthcare provider otherwise lawfully processes with a view to providing healthcare, and it is wider than what is necessary for the achievement of the above objectives as indicated by the university. All in all, this means that the copy of the document is not suitable for identifying the data subject submitting the petition; however, the Authority believes that the healthcare provider has a legitimate interest in making a presumption about the person and the authorisation of the petitioner re-

questing copies of health-related documents and to request supplementary data appropriate to the objective from the data subject to this end. According to the Authority's position, this purpose can be achieved by requesting a form of copy from the data subject, in which the data not otherwise processed by the service provider can be blocked. If the data subject sends the copy of the document by blocking his photo and the document identifier, he renders it probable with the copy of the document he possesses that he is the petitioner. The consistency of the data can also be established based on the blocked copy. If, however, in spite of this, the data subject sends a full copy, it is the obligation of the university to block the photo and the document identifier and to continue to process the copy in this format. [NAIH-10199/2023]

In another case, the Authority levied a data protection fine of 10 million forints on a private healthcare provider for refusing to issue a copy of the health-related documentation. The service provider not only failed to ensure the exercise of the data subject's rights, but fully disregarded the data subject's request for the copy failing to react to them in any way whatsoever. The institution also failed to co-operate with the Authority and except for a single answer, it made no statement in the course of the procedure, it ignored the orders of the Authority and failed to give a satisfactory answer in its only statement. This behaviour rendered the exploration of the facts of the case very difficult. Had it been cooperative, it would have been easy to discover that the service provider misspelled the surname of the data subject in its own system. It arrived at the conclusion that it did not process documentation on the data subject based on the misspelled surname, although the other natural person identifiers of the data subject were correctly shown in its system. Thus, had it been willing to grant the request, it would have been able to identify the petitioner. [NAIH-5267/2023]

A complaint submitted against a company providing healthcare services threw light on an important problem with regard to access to documentation. In some settlements, a healthcare services company provides on-duty medical services under a contract for such services concluded with the municipality. The company complained against provides such healthcare services in several settlements at predetermined venues and times. The diseased husband of the petitioner received care in one of the surgeries of the petitionee company, but according to the petitioner's statement, neither she, nor her diseased husband received any document on the care provided. Because of this, the petitioner requested the issue of the documentation generated while healthcare services were provided to her diseased husband by mail sent to the address of the surgery; however, all her letters were returned marked as "unclaimed" because the company provid-

ed care in a different surgery when the letters arrived, hence none of their staff received the letters. The company argued that the medical on-duty service is a non-existent entity, hence it has no liability as controller. In the course of its procedure, the Authority also examined in what way the company facilitated the submission and receipt of requests from data subjects in its general procedure. In its decision, the Authority established that medical on-duty service is the name of a service, it is a widely used phrase and it does not qualify as controller; the services provided and the processing is carried out by a legal entity, i.e. the company, which uses this name, hence it has to bear the consequences arising from providing the service and using its name, including their responsibility as controller. The Authority also found that the company failed to provide transparent information to the data subjects on the possibility of submitting data subject request, it did not facilitate the exercise of data subject's rights and as patients receiving care in the surgery they had good reason to assume that they should send their access requests to that address. The Authority ordered the company to take measures to appropriately receive data subject requests and to provide appropriate information on the mode of exercising data subject's rights. [NAIH-4656/2023]

In another case before the Authority, the notifier complained that the dentist who had earlier treated her child failed to answer her letters, in which she requested the issue of the health-related documentation generated in the course of treatment. In addition, she also objected to the fact that there was ongoing surveillance by cameras in the waiting room to the surgery and the live stream was visible in the treatment room. Following the examination of the camera system, the Authority found that a camera was aimed also at the door of the toilet, whereby the processing infringed the principle of fair processing and the data subject's right to human dignity. In the course of the procedure, the controller stated that he had already informed the notifier in the course of a meeting in person that she can obtain the requested documents in person in the surgery. The Authority called the attention of the controller to the fact that if it fails to take action on the request, it has to inform the data subject of the reasons for failing to take action without delay, but at the latest within a month from receipt of the request, or if it refuses to take action on the request, because of clearly unfounded or excessive nature of the request, it has to bear the burden of proving that the request was clearly unfounded or excessive. At the same time, the controller did not substantiate in any way that it did not respond to the notifier's letter because it personally informed her of the possibility of obtaining the documents in the surgery. In addition, the Authority established that the controller's Privacy Statement did not include any provision concerning the mode of submitting data subject request.

The notifier submitted her request for the issue of a copy by e-mail and expressly requested that the documents be sent by e-mail. The controller did not regard it right to send health-related documentation containing special category personal data in an e-mail to an ordinary Gmail account. The Authority deems that the controller's general intent related to the appropriate identification of data subjects, i.e. to make personal data accessible only once it has assured itself of the identity of the data subject is fundamentally correct, however, this has to be assured by lawful, appropriate and efficient procedures, while providing information to the data subjects. Consideration should be given to the procedures, organisational and technical measures, which could best serve this purpose. Several relevant solutions are known in practice: forms, password protected attachments, two-factor authentication, password sent by text message, proprietary IT interfaces, password protected online accounts, e-mail address authentication through clicking on a URL sent by e-mail, regularly repeated reconciliation of data, etc. It is important that in such a situation, the recording and reconciliation of the data served the purpose of ensuring the establishment of the identity of the petitioner and the formerly treated data subject; hence the procedures applied have to be adequate to such a purpose. If, when such measures are taken, doubt arises with regard to the identity of a data subject, it is easier to objectively assess whether there is any channel, which would seem adequate from the viewpoint of data security, or the identity of the given petitioner may have become questionable to the extent that the request cannot be granted through any channel until the appropriate reconciliation of data. In this case, the controller did not refer to any circumstance for the Authority, which would have questioned that the petitioner was identical with the notifier; hence it failed to render the need for data reconciliation probable.

In the course of the procedure, the controller also referred to the fact that the patient documentation was not taken over either by the notifier, or a relative in person, while the controller had uploaded it also to the EESZT interface, which it deemed to be secure. According to the Authority's position, any healthcare provider may refer to informing the data subject that the requested documents are accessible for the data subject in EESZT when granting access. At the same time, the Authority deems that this possibility is available only when the service provider is assured that the data subject has access to EESZT, the documents he requested are fully accessible there and the data subject does not object to access via EESZT after being informed of it. If following such information, the data subject still requests a hard copy, his request cannot be denied as the data subject is entitled to ask for something other than granting his request in the electronic way.

When examining the controller's Privacy Statement, the Authority found that the provision saying that "*the patient is entitled to inspect his health-related documentation and to make abstracts or copies of it, or to receive a copy at his own cost*" is unlawful as the data subject may request the first copy free of charge. [NAIH-9878/2023]

II.1.3. Data of the deceased

Within the case group of health-related data processing, access to data and documents related to deceased persons represents a special group of cases.
Based on a petition, the Authority conducted an investigation in a case where the brother of the deceased person wished to have access to certain medical documentation related to the diseased. The diseased person had a heart condition, he visited his family physician two weeks before his death; then, a few days later he was admitted to hospital where he died. The family physician refused to issue the documentation requested pursuant to Section 7(7) of Act XLVII of 1997 on the Processing and Protection of Health and Related Personal Data (hereinafter: Health Data Act) with the reason that the treatment he provided was not related to the subsequent death of the patient in an institution. The Authority had to develop its position on the meaning of the legal concepts of "treatment *related to or likely be related to the cause of death*" and "*treatment preceding death*". In this case, particularly the latter concept was relevant because according to the professional statement of the family physician, the cause of death could not be related to the treatment provided by him, so the question was whether the documentation should be issued under the other grounds referred to. As the legislator did not define the period, which should be taken into account when interpreting treatment preceding death, the Authority analysed the data subject's right to self-determination, the confidentiality obligation of the physician, which exists even after death, the deceased person's right to respect and the justification by the legislator and came to the conclusion that *data related to treatment preceding death should be taken stricto sensu* and treatment preceding death should in some way be relevant from the viewpoint of the causal process leading to death even if it could not be established as a cause of death. Otherwise, ultimately all treatment provided since birth should be regarded as treatment preceding death, but obviously the legislator did not wish to interpret the concept this way. It also follows that a general statement can be made as to the meaning of the phrase "treatment preceding death" and generally no period can be defined, instead the issue has to be assessed case by case considering all the circumstances of the specific case. [NAIH-3831/2023]

In parallel with the case under investigation, the Ministry of the Interior sent a request for opinion asking for the Authority's position in interpreting the concept of "*treatment preceding death*", while the interpretation of the provisions of Section 24(14) of the Healthcare Act was also an issue. The latter provision enables the exercise of the right to access a copy of health-related documentation through EESZT. It is an interesting point that the justification of the provision expressly refers to ensuring the surviving relatives' rights set forth with the same content also in the Healthcare Act, while the text of the legislation can be interpreted for the entire section, i.e. to any data subject's right, which can be enforced via EESZT with regard to his own data, not only to data concerning the deceased person. The Authority took the position that under the paragraph referred to, the relative has to be given an opportunity to access the requested data via EESZT; this, however, cannot mean to gain access to the entire EESZT account of the diseased. The Authority also initiated a clarification of the legal regulation. [NAIH-5976-2/2023]

The Authority also received two separate submissions, in which complainants presented that they requested the health-related documents of their diseased relative from the Ministry of the Interior as the operator of EESZT. Their requests were rejected and they were directed to the institutions treating the diseased person prior to their death, saying that the establishment of the cause of death, thus the evaluation of the range of documents that could be issued is a technical medical issue, for which the Ministry does not have competence and that the relevant data are to be issued by the controller entering them in EESZT. The Authority has contacted the Ministry of the Interior in order to learn about the application of the above-mentioned provision of the Healthcare Act and the follow-up to the proposal for the amendment of the legislation. In its answer, the Ministry presented that as they also recognised the problem and in view of the recommendation to amend the regulation, they conducted reconciliations, which resulted in the entry into force of a provision of a government decree, according to which the Ministry shall involve the National Directorate General for Hospitals as controller to evaluate medical issues in the event of requests by relatives of diseased persons to access data as detailed in the regulation and the Directorate General may also involve additional processors. The Ministry also stated that they were preparing the procedures for providing information to relatives of the diseased about their health-related data stored in EESZT. [NAIH-8361/2023, NAIH-8369/2023]

In another submission also affecting the data of diseased persons, the mother of a diseased child requested the issue of the autopsy report from the healthcare provider. The issue of the document was denied stating that what they did was not a post mortem for medical reasons as it applies to persons diseased in hos-

pitals, but a post mortem by a forensic expert in a criminal procedure in progress and the report of such a post mortem should be requested from the body taking action in relation to the case of death and in view of the criminal procedure, the healthcare institution is unable to issue the report. The Authority found that the Healthcare Act and the Health Data Act define the concept of health-related documentation differently and the notion of documentation according to the Health Data Act does not include documents generated in relation to autopsies. This is relevant because relatives' rights concerning the documents of a diseased person exercised under the authorising provision of the Health Data Act are subject to the provisions of the GDPR, but not the Healthcare Act. As the enforcement of relatives' rights under the Health Data Act does not include the full autopsy documentation, the Authority does not have the power to take action with regard to such submissions. Incidentally, the complainant could access the requested document in the criminal procedure. [NAIH-5917/2023]

II.1.4. "Blocking" websites

There was a significant change in the instruments and procedural efficiency of the Authority in that the amendment of the Privacy Act – introduced by Section 66 of Act CXXII of 2021, in force from 1 January 2022 – enabled the blockage of websites in specified cases of serious infringements by the Authority, i.e. rendering them temporarily inaccessible or giving an order to that effect. The Authority has taken the initiative of granting this possibility with the legislator in order to be able to act more efficiently against the operators of internet sites who – without disclosing their identity and exploiting the fact that they are unknown – cause substantial damage in some cases to data subjects by the unlawful processing of data.

For a long time, the Authority has been receiving complaints objecting to the fact that one such internet site published photos of sexual content showing the complainants who could be recognised and even identified by name in intimate situations in a manner accessible to anyone without the complainants being aware of this and without them consenting to it. According to the most recent notification of this kind, compromising photos of the notifier were publicly shared on this website. The notifier's Facebook profile was also published among the photos, on the basis of which they became even more identifiable. Similarly, intimate photos of a number of other private individuals are published on the website. The content published on the website contains special sensitive categories of personal data accessible to anyone without restriction. It has been a practice of the website not to grant erasure requests, moreover they publish data subjects' re-

quests in a taunting way. No information concerning the operator and editors of the website is published, the website does not have publishing information. The Authority contacted the domain registrar of the website registered in the United States in a letter to discover the identity and access data of the controller, and as an interim measure ordered the registrar to temporarily remove all data content published through the electronic communication network of the URL belonging to the website. The registrar received the Authority's letter, but failed to meet its order, so the Authority blocked the publication of personal data by ordering that the website be temporarily made inaccessible and contacted the National Media and Infocommunications Authority to enforce the interim measure.

The Privacy Act enables the Authority to enforce the above interim measure and to enforce the rendering of the electronic data inaccessible in the case of this website. The introduction of this legal instrument has made the action against serious infringements of the right to the protection of personal data more effective, since in cases where the controller cannot be identified by the means available to the Authority, or where the controller obstructs the procedure or does not provide the Authority with the information necessary for the procedure, this does not constitute an absolute barrier to the effective application of the law and to remedying the infringement, but the Authority can take substantive action to remedy the infringement. [NAIH-6288/2023]

II.1.5. Cases related to political campaigns and elections

An outstandingly large number of complaints were received by the Authority concerning data processing for political reasons. In view of this, the Authority conducted ex officio procedures concerning the general practice. Such a procedure was conducted with regard to the text messages and phone calls made during the 2022 parliamentary election campaign and also with regard to the request for opinions referred to as "Budapest residents' meeting" in 2023; the Authority also investigated processing during the 2022 primaries of the opposition.

As to the opposition primaries, the Authority clarified the circumstances of unsolicited text messages sent by the opposition. In the course of the investigation, Datadat Professional Kft., and Datadat GmbH (the new name of the company: Estratos Digital GmbH) indicated themselves as controllers with regard to their role in the processing under investigation; as a result of the investigation, the Authority established that the Kilencvenkilenc Mozgalom Egyesület (hereinafter: Union), Datadat Professional Kft., as well as the Datadat GmbH were controllers as based on the facts of the case, each of these companies played an active role

in determining the means of processing and developing the mode of processing. Based on Article 26 of the GDPR, the Authority also examined whether the controllers qualified as joint or parallel controllers. In doing so, the Authority concluded that the Union determined the purpose of processing, while the means of processing were jointly determined by the Union, Data Professional Kft. and Datadat GmbH, hence they qualify as joint controllers with regard to the processing under investigation.

Furthermore, the Authority found that the information provided in relation to the processing under investigation was inadequate because of which the most important elements of the consent by data subjects to processing were missing. Through this, the Union and Datadat Professional Kft. processed the personal data of the data subjects without a valid legal basis, i.e. they acted unlawfully. Based on these findings, the Authority called upon the Union to erase all the personal data earlier collected of the data subjects through their website in a verifiable manner and provide information to the data subjects on the processing of their personal data on its website, and cooperate with the Authority in the future. The Authority called upon Datadat Kft. to perform its processing operations in accordance with the provisions of the GDPR and conclude its legal transactions in accordance with its factual role played in processing, determine the roles played in the actual processing appropriately and enter into agreements on processing personal data in compliance with Article 26(1) and (2) of the GDPR. The calls by the investigation were published on the Authority's website in the form of a report. [NAIH-6752/2023]

Two major case groups of processing during election campaigns included the sending of unsolicited text messages en masse and making unsolicited phone calls en masse.

As to sending text messages en masse, the Authority received a great many notifications prior to the 2022 parliamentary elections: the complainants objected to receiving unsolicited text messages of political content containing their given names or names associated with the subscriber on their mobile phones in which they were encouraged to vote for the political group indicated in the message. The messages were sent by foreign processors as part of sending bulk messages. It was established that the multi-step use of foreign processors renders compliance with transparency and accountability difficult. The Authority found it difficult or impossible to reach the foreign processors; also, the unnecessary processing abroad of politically sensitive personal data and the prolongation of exploring the facts of the case renders it difficult to establish the likelihood of

compliance. Having reviewed the text of all types of text messages, it was found that they did not contain any specific information concerning the controller or any reference to the location of eventual additional information. The text messages forwarded contained spelling mistakes in many cases, which may indicate some foreign relationship, in terms of their content, however, they were intended for Hungarian citizens and could be regarded as campaign messages excluding any doubt.

Because of the difficulties in exploring the facts of the case as detailed above, the roles played in processing could not be clarified, i.e. the person(s) of the controller(s) could not be established, so the Authority declared in a report without indicating the person of the controller but with regard to the exceedingly wide range of data subjects that the processing failed to comply with the legal requirements. [NAIH-4360/2022]

Many complaints were submitted also concerning the “phone calls en masse”, in which complainants objected to the processing of their phone numbers without their consent which were not included in the public phone directories for the purposes of unsolicited political calls. Similarly to the case of sending text messages en masse, here too, the multi-step use of foreign processors encumbered the procedure and compliance with transparency and accountability. The unnecessary storage of a large number of data abroad and their use for political purposes ab ovo gives rise to legitimate doubts concerning lawfulness. If the review of such processing causes difficulties and takes months even for the Authority, data subjects cannot be expected to have an overview of the processing.
Information under Articles 13 and 14 of the GDPR must be provided prior to the commencement of processing, but at the latest upon first contact. As a minimum, this must contain the identification of the sender of the oral or written message (the customer), the source of the contact data and the legal basis of processing and access to additional information, in addition to other information that may be necessary depending on the circumstances. Providing information in advance does not mean that the accessibility of the information would not be necessary during the period of processing (further processing of the content data), this obligation exists throughout the duration of processing. If the website collecting the data is closed down, but the personal data collected are still processed, it is the responsibility of the controller to provide easy-to-access information for the data subjects and to indicate the accessibility of the new information to the data subjects at the latest upon the next contact.
The Authority arrived at the identification of the persons responsible for processing through retracing contract chains through numerous intermediaries. The bulk

political calls were administered through the phone service providers giving the phone numbers included in the complaints, call centres and intermediary agents. The Datadat group played a similar role also in this group of cases. The published report includes additional detailed information; the Authority continues to explore some of the exposed problems under an ex officio authority procedure. [NAIH-4949/2023]

The Authority received numerous complaint notifications, objecting to processing by the Municipality of the Capital City of Budapest related to letters of notification concerning voting at the "Budapest residents' meeting", as the Municipality of Budapest contacted Budapest residents for the purpose of obtaining their opinions on "discharging their tasks in the public interest" by directly sending letters to the residents. The Authority conducted its investigation, which resulted in recommendations to the Ministry of the Interior and the Municipality of Budapest. In its recommendation, the Authority emphatically addressed the following issues:

- the questions asked, the information on data processing,
- rules concerning the participation in public life by persons below the age of 18,
- the request to the group for providing data and its regulatory environment.

In this respect, the Authority's recommendation detailed that the effective purpose of the controller with regard to three questions of those posed to the residents was not consultation about issues related to transportation as specified in the request to the group for providing data, but to share its own political position with the residents in the form of direct mail, hence the Authority identified this purpose as political marketing.

In the Authority's opinion, the questionnaire, which can be regarded as political marketing, clashed with the prohibition of contact with the purpose of direct marketing as set forth in Recital (38) of the GDPR in the case of minors. To obtain the personal data of minors, the controller should have obtained the prior consent of their legal representatives. The Authority also established that the relevant law does not include rules for the possibility of forbidding data requests for "Budapest residents' meeting" and similar other requests for opinions and political marketing. The Ministry of the Interior did not examine the application for requesting data in merit, or the compliance of the legal basis to support it, instead it regarded the reference to the legal regulations needed for granting it as sufficient, i.e. it formally checked the application, but not its content. Another problem

identified by the Authority was that the statutes of the municipality do not include detailed rules for requesting data and the processing of the personal data obtained, i.e. the municipal decree does not regulate the details of processing to be specified by legal regulation: the types of data, the purpose and conditions of processing, the accessibility of data, the identity of the controller and the duration of processing or the periodic review of its necessity.

In its recommendation to the Ministry of the Interior, the Authority recommended that

- the Ministry initiate an amendment to Act LXVI of 1992 on the Registration of the Personal Data and Addresses of Citizens (hereinafter: Registration Act) / [regulating access to the personal data of persons under 18; developing the data protection rules of activities to express political opinions; with regard to the right to object, providing an opportunity for the data subject (or their legal representative) regardless of their age to block the issue of their personal data in the case of requests for opinion],
- call the attention of government offices to examine compliance with the provisions of Section 5(3) of the Privacy Act when checking the legal compliance of municipal decrees.
-

In its recommendation given to the Municipality of Budapest Capital City, the Authority recommended that the Municipality

- review and amend the relevant rules of its statutes,
- review its processing practices and opt for a solution in the cases affecting a large number of people in the future, which does not require the processing of personal data. [NAIH-6166/2023]

II.1.6. "Borderline" cases

The Authority considers cases to be "borderline" cases where the interplay between the right to the protection of personal data and another fundamental right – in particular, but not limited to – the freedom of expression, and the determination of the constitutional balance to be struck in this area, is a question of law enforcement on the merits of the case. Below the most interesting examples of this case type are presented.

The legal representative of the minor Petitioner contacted the Petitionee (a private healthcare provider) by phone in order to ask for an appointment for taking a blood sample from her 15-year-old child. Having used the service, the legal representative described her negative experiences related to the healthcare service provided by the Petitionee in the evaluation column of Google Maps, also providing her full name and photo. In its reply to the evaluation, the Petitionee explained that minors can only be tested for STD (sexually transmitted diseases) with parental consent. The response clearly suggested that the legal representative wanted to take the Petitioner for testing for a sexually transmitted disease, although this was not the case. The Petitionee published untrue health-related data in its comment, although it was aware that the Petitioner could be clearly identified from it. The legal representative of the Petitioner erased her opinion, which rendered the response to it also inaccessible in order to reassure the minor Petitioner and to protect her interests. According to the Petitionee, its answer contained information of a general nature, hence the comment –"*it was in no way related to any specific person, including the complainant's child*" – was incorrect as described above.

According to Article 9(1) of the General Data Protection Regulation, the processing of health and sex life data is prohibited. Pursuant to Article 9(2)(e), paragraph (1) is not applicable when processing relates to personal data which are manifestly made public by the data subject. The Petitioner and her legal representative did not make the data concerning the STD testing public, it was exclusively done by the Petitionee. The Petitionee did not indicate any other legal basis for publishing the contested health data of the Petitioner; according to its position, data processing did not take place.

In its procedure, the Authority found that *"through its data processing the Petitionee infringed Article 6(1) and Article 9(1) of the General Data Protection Regulation when it made health-related data of an under-age child public. The fact that the legal representative of the Petitioner was forced to remove her opinion on the healthcare service provided by the Petitionee in order to get the data made public by the Petitionee concerning to the under-age Petitioner erased was assessed by the Authority as a particularly aggravating circumstance."* [NAIH-3888/2023.]

A civil servant submitted a complaint, according to which the new elected mayor of a settlement published a Facebook entry about the fact that former employees of the mayor's office of the settlement (hereinafter: office) are subject to psychiatric treatment. The Authority found that personal data were not processed

through the entry as the processing of personal data is carried out when the data subject can be identified through the processing. However, the mayor first informed the residents – without naming the people concerned – that "*... the executive of the office and every one of its employees (with one exception) were on leave or sick leave*", then provided information about the fact that "... *the former employees of the office were on sick leave with psychiatric problems"* in the entry referred to. Therefore, as the entry does not say that not all office employees were on sick leave, the persons on sick leave could not be identified even in the case of an office of small headcount.

According to the position of the Authority, the contested entry in the complaint was within the scope of the freedom of expression, the entry described a personal opinion and value judgement concerning the behaviour of the employees of the office, and the author of the entry did not intend to disclose the health-related personal data of individual office employees as special category personal data. Pursuant to Recital (4) of the General Data Protection Regulation, the right to the protection of personal data is not an absolute right and it must be balanced against other fundamental rights, such as the freedom of expression, in view of which the Authority rejected the complaint without investigating its merits. [NAIH-3709/2023]

In another case, the Authority held the petition for launching an authority procedure for data protection on account of a Facebook entry formulating an opinion related to the leave of the mayor as clearly unfounded and rejected it. The Authority found that the mayor was a person performing public duties and the data concerning his leave – just as any data related to being impeded in performing his public duties for other reasons or his absence from work – are personal data accessible on public interest grounds according to Section 26(2) of the Privacy Act, which can be disclosed while respecting the principle of purpose limitation. The Authority established that the private Facebook group according to the location of the disclosure came into being to discuss issues of public life as its title says, where the members of the group shared their opinions in cases of public interest. In the Authority's position, the fact that the Petitionee, who himself was also a person performing public duties, i.e. a local municipal representative expresses his opinion concerning the workplace presence of the mayor in the social media site meant that the processing was in fact purpose limited. Hence, the mayor's personal data accessible on public interest grounds was disclosed for the purpose of the transparency of public affairs as set forth in Section 1 of the Privacy Act and the provisions of Section 2(2) of the Municipalities Act ensuring wide public access to local public affairs. So, the entry, a copy of which

was enclosed with the Petitioner's submission belonged within the freedom of expression. The Authority also referred to the governing judicial practice, according to which the mayor as a person discharging local public tasks had to reckon with the fact that his activities would be subject to criticism, hence as a public figure he has to suffer the expression of negative opinions concerning his activities, unless it is unjustifiably disparaging or humiliating. In the case of public figures, the boundaries of expression are wider and this also applies to the representative, as well as the mayor of a municipality. (BDT2010. 2215.) [NAIH-3816/2023]

The Authority condemned a press organ and ordered it to pay a high amount of administrative fine and to erase the unlawfully published personal data, which despite the express objection of the petitioner and her requests for erasure failed to delete the article the petitioner contested that contained a one-sided opinion regarding her professional activities and qualifications. The Authority did not accept the individual balancing tests supporting the legitimate interest of the petitionee because it only took the interest of the press organ into account and misinterpreted the notions of a role in public life and public figure with regard to the petitioner. The petitionee wrongly concluded that the petitioner became an active public figure by assisting her politician husband during the campaign period. An issue related to the article – the subject matter of child delivery outside an institution – is of public interest, however, according to the Authority's position, sharing of opinion-forming information cannot be referred to as the purpose of processing when the content and formulation of the article suggests a one-sided position, excluding the possibility of forming one's own opinion. [NAIH-3977-4/2023]

The Authority condemned a press organ controller on the grounds of disregarding data subject's rights as a result of an investigation into a processing, in which the former political role of the petitioner and his university career at the time of carrying out an act concerned in a criminal procedure and at the time of the publication of the article turned the person of the petitioner into a subject of public interest. Through this, the criminal act alleged to be carried out by the petitioner became the subject matter of public discussion as higher moral standards are expected from a former politician and university lecturer, they are subject to more stringent evaluation; therefore, if a person discharging respected public tasks is subject to a criminal procedure generally reflects upon and impacts the moral state of society as a whole. [NAIH-257-13/2023]

The Authority did not find infringement in an investigation when a member of Parliament lodged a complaint against processing by a news platform, which recorded a phone conversation with the complainant and published it online without his consent. As a result of the investigation, the Authority established that the complainant as a person performing public tasks voluntarily accepted the publicity concomitant with his position in Parliament, as well as his obligation to suffer the expressions of opinion and criticism related to his activities, including his position expounded concerning a social issue. The public nature of the information through the online article could be clearly established as the controller complained against published the complainant's position expounded upon the questions posed in relation to a social issue in the public interest commanding the interest of the public to this day. [NAIH-394-2/2023]

II.1.7. Other important cases subject to the General Data Protection Regulation

1. Complaint against processing by a dating agency

The Authority investigated a data protection complaint against a dating agency (hereinafter: Agency) under an authority procedure launched upon request. The company provides dating mediation services to persons entering into a contract of assignment with it; the complainant was one of its clients. The complainant objected to the fact that the Agency forwarded all the personal data recorded on him/her to potential partners without his/her consent as he/she provided the data to the Agency by completing the relevant datasheet. The complainant also objected to forwarding his/her data to persons, who met his/her excluding conditions, and should not have received his/her data at all. In addition, the forwarding of all of his/her data meant that the recipients had access to all the data on the complainant, including those related to his/her religion, enabling his/her unambiguous identification. The dispute between the parties revealed that processing and in particular the process of data forwarding was insufficiently clear.

The Agency operates several websites to advertise its services. No Privacy Statement was available on the websites and the Agency was unable to present any written Privacy Statement, which would have been in force during the contract with the complainant; all that was available was the contract, which did not include any transparent information of appropriate content. The parties disputed the content of the oral information provided upon the conclusion of the contract and the Authority was unable to reconstruct it.

The Privacy Statement and contract form drafted during and as a result of the procedure still did not contain any information of merit on the forwarding of data, neither with regard to the procedures followed, nor on the process of selection or the range of data forwarded. It was not possible to clearly learn the legal basis of the individual processing operations, the retention period, the information concerning the processing of special category data from these documents and several of their elements were contradictory and confusing. The websites of the Agency did not reveal the basic information as to who is their operator and who provides the services. A common feature of the websites in question was that their central element of marketing was the strongly emphasized personal contribution of a person called "A.É." suggesting as if this person would be the dating intermediary; while it was also suggested that the Agency does not employ a person by that name, and the use of the name was no more than a marketing trick to win the trust of those in search of partners. In the course of the procedure, the Agency stated that the person named does not actually participate in mediating partners, s/he does not know the data of the members, and the agency acted as both controller and service provider. Because of this, the Authority established that the contribution of the person indicated on the website and in the documents, their real role in processing could not be transparent for the complainant and the promises made were practically untrue. According to the Authority's position, it is not acceptable if untrue information is provided on the person of the controller based on marketing criteria as this cannot be regarded as true and appropriate information.

So, the Authority established that the Agency did not provide processing information with content compliant with Article 13 of the GDPR, the information provided was neither transparent, nor easy to access, and the Agency was unable to comply with the principle of accountability. With regard to the data, which qualify as special category data (religion), the Agency was unable to verify a lawful legal basis either for the processing or the forwarding of the data. With respect to the infringement of transparency, the Authority underlined in particular that neither the method, nor the legal basis of the forwarding of the data were transparent. The Authority found the problems assessed with regard to transparency to be injurious, particularly because of the nature of the service. Data processing is not an accessory issue for a dating service, rather it is the central element of the very essence of the service. The clients of the Agency are persons who wish to become acquainted with persons they do not know for sensitive reasons and they provided data to the Agency for this purpose because they trusted the service provider. In view of the above, the Authority instructed the company to provide full and transparent information on data processing and to publish the

information in an appropriate manner. As regards sensitive data, it should either provide an adequate legal basis for their processing or cease processing them. [NAIH-4788/2023]

2. Data processing by toll enforcement agents

A notifier objected to the fact that the service provider operating a toll payment system (hereinafter: service provider) makes use of agents to collect the surcharge in the case of vehicles with foreign number plates and to that end transfers the data available on the vehicle to its foreign collaborators. The service provider pursues its collection, checking and surcharging activities with regard to the toll payable for the prorated use of the national public roads based on designation and authorisation by legal regulation, in the course of which it enforces the surcharge to be levied in the case of unauthorized road use against the operator/owner of the vehicle that uses the road without authorisation and to that end, it contracts foreign companies in the event of residents outside Hungary. The relevant legal regulations do not address the position of agencies involved in retrieving the data of vehicles with foreign number plates from a data protection aspect; however, according to the Authority's standpoint, it would be necessary to express this in the legal regulation requiring data processing as that would ensure the transparency of processing. For this reason, the Authority submitted a recommendation to the competent ministry proposing that the legislator regulate the role of agents used for collection played in processing in relation to the enforcement of tolls, so that basic circumstances of processing – the person of the controller, the agents, the role of collaborators in processing – be settled at the level of a legal regulation in line with data protection requirements. The legislator adopted the recommendation. [NAIH-7639/2023]

3. Treatment of decisions authorising adoption in the case of a baby loan contract by credit institutions

The ministry in charge of drafting the regulation gave a favourable answer also in the case when a notifier couple concluded a new baby loan contract with the credit institution after which they adopted a child under a secret adoption arrangement, then notified the credit institution of the fact of the adoption and requested the suspension of repayment. The notifier objected to having to submit the entire final decision permitting adoption to the credit institution, which included personal data and information, which were not needed for the evaluation of the request for the suspension of repayment. Of these, the notifier particularly objected to the processing of the name of the child prior to adoption and of what

was experienced during the mandatory period of care. The decision permitting adoption contains a number of personal data, which are not needed to decide whether the assisted couples are entitled to an interest subsidy until the end of the loan period, or for the suspension of repayment. According to the Authority, the relevant provisions of the government decree on the assistance for the new baby and the processing by credit institutions of the final decisions permitting adoption in full on the basis of that authorisation infringes the principle of data minimisation. With a view to the amendment of the government decree on the new baby subsidy, the Authority recommended that the fact of the adoption be verified with the certificate issued by the competent welfare authority, which should include – in addition to the personal identification data of the assisted persons and the adopted child, and excluding its name prior to adoption – only the fact of adoption, that the adoption has taken place, the number of the decision permitting the adoption and the date of its becoming final. The Authority recommended that the legislator render the use of this certificate mandatory for the verification of the fact of adoption. The underlying reason is that the justification of the decisions permitting adoption includes sensitive information describing the details of the life and circumstances of the family, which qualify as personal data. The processing of these personal data by credit institutions is not justifiable and by far exceeds the range of data needed to achieve the purpose of processing – checking whether the entitlement for the suspension of repayment and the assistance exist – resulting in the credit institutions infringing the principle of data minimisation, while they meet their legal obligations. [NAIH-6491/2023]

4. Exercise of the right to access in the case of a life insurance contract

According to a submission received by the Authority, the father of the notifier entered into a life insurance contract with an insurer, in which the notifier was designated as beneficiary. Following the death of his father, the notifier requested the payment of the insurance amount; however, the insurer rejected his claim. The notifier lodged a complaint against the rejection of his claim, which the insurer rejected based on the opinion of a medical consultant, who was unknown to him and treated as confidential. The notifier repeatedly requested the insurer to make the consultant's opinion available to him on the basis of which the payment of the insurance amount was rejected. The insurer did not grant the notifier's claim with reference to the insurance secret because, according to its position, only the heir according to the grant of probate can be granted access to the requested personal data and not the beneficiary pursuant to the Act on Insurance. In the insurer's view, the authorised person named in the contract must be the person

authorised to exercise data subject's rights, who is not identical with the beneficiary indicated in the contract.

According to the insurer's statement to the Authority, the "authorised person named in the contract" may also exercise data subject's rights who may be a person whom the data subject had designated in writing while alive with respect to whom the insurer was exempted from its confidentiality obligation. In its statement, the insurer acknowledged that the term "authorised person named in the insurance contract" is unclear, its interpretation is disputed, so the insurer issues data related to the insurance contract exclusively to heirs as there is no statement available, which would prove without any doubt that "the authorised person named in the contract" would be identical with the beneficiary. Because of the insurer's interpretation of "authorised person named in the contract", the notifier could not have access to the document on the basis of which the insurer rejected the payment of the insurance amount.

Based on this, the Authority established that the insurer infringed the data subject's right to access when it failed to provide access to the data and documents of the life insurance contract to the notifier designated as beneficiary in the life insurance contract. The Authority also established that the natural persons named in life insurance contracts as beneficiaries in the event of death belong to the category of "authorised person named in the contract", they may exercise the data subject's rights to which the deceased had been entitled during his life. Accordingly, the Authority called upon the insurer to grant access to the notifier as beneficiary in the event of death to the personal data of his father processed in relation to his life insurance contract and the data related to the insurance contract and to review and modify its practice concerning granting access to data which may relate to diseased persons. [NAIH-357/2023]

5. Investigation into data processing related to supporting the career choice of children in child protection care

Based on a notification in the public interest, the Authority conducted an investigative procedure concerning a memo and its lawfulness, entitled "*Request in relation to the career interest of children and young adults in child protection care*" sent on 24 March 2023 by the Ministry of the Interior State Secretariat for Social Affairs (hereinafter: controller) to the operator of every child protection facility.

The request was based on the implementation of the Franciska Apponyi Future Workshop Programme, which was established in order to support the career

choices of children and young adults in child protection care and an improvement of their chances in the labour market. It was under this programme that the controller wished to survey the career interests of children being raised in foster parent networks operated by the recipients and in group homes and children's homes studying in the 5th, 7th and 9th-12th grades, and young adults receiving aftercare services and their ideas in finding a place in the world of work.
The controller requested the individual care facilities to provide the data by completing open online forms through its processor, the Margit Schlachta National Social Policy Institute (hereinafter: NSZI) for this purpose. The social security number of the child had to be entered in the form; the data collection extended to the school performance of the children, their special needs, as well as the BNO codes related to the children's health condition. The accessibility of a Privacy Statement was not included either in the form or in the letter inviting their assistance.
The controller indicated the development of a personalised career programme as the purpose of processing; however, according to their statement made to the Authority in the course of the procedure, the development of the actual career plans and models would in fact have been the task of the specific care facility.

The investigation found that the controller infringed the principles of lawfulness, fair procedure and transparency according to Article 5(1)(a) of the GDPR; the principle of purpose limitation according its point b); the principle of data minimisation according to its point c), the principles of integrity and confidentiality according to its point f); the principle of accountability according to Article 5(2) of the GDPR; and Article 6(1) of the GDPR as it failed to substantiate an appropriate legal basis for the processing; the requirement of providing information according to Articles 12, 13, 14 of the GDPR and, furthermore, it failed to meet the tasks of the controller according to Article 24(1) of the GDPR. In addition, the controller breached the requirement of data protection by design and by default arising from Article 25 of the GDPR; its obligations concerning processors arising from Article 28(1)-(3) of the GDPR; its obligation to cooperate according to Article 31 of the GDPR; its obligations concerning risk evaluation and data protection impact assessment arising from Articles 32 and 35 of the GDPR; its obligation arising from Article 38(1) of the GDPR with regard to cooperation with the data protection officer; and its obligation to cooperate with the Authority in accordance with Section 54(2) of the Privacy Act.

In view of the severity and large number of the infringements found, the Authority called upon the controller, inter alia, to erase permanently and irrecoverably the

personal data collected via the questionnaire form, which was fully met by the controller. [NAIH-495/2024, antecedent case number: NAIH-4511/2023]

6. Investigation into changing the names made public of children from unknown parents placed in the baby rescue incubators of hospitals

The press reported several times that newborns were found in the baby rescue incubators of various hospitals (for instance in Miskolc, Békéscsaba and Hatvan). These reports disclose, in addition to the name of the settlement and the hospital, the sex of the children found in the incubators, as well as the names given to them by those who found them, and at times even the weight or the length of the body of the children.

Based on Section 38(3)(a) of the Privacy Act, the Authority conducted an ex officio investigation whether the names of the children found in the incubators disclosed to the public (such as Marcell Hajnal, Ferenc Réthy, Martin Szombati) were subsequently changed, or the fact of their discovery and its circumstances would remain identifiable for anyone for their entire lifetime because their names were made public.

Pursuant to Section 4:151(1)(b) of the Civil Code, the welfare departments (guardianship authority) determine the child's name if both parents of the child are unknown (name given by the guardianship authority), with the powers being exercised by the municipal executive in relation to the processing under investigation. Under Government Decree 149/1997. (IX. 10.) on the guardianship authorities and child protection and guardianship procedures, the data required for entry into the registry of births and deaths are determined by the municipal executive in agreement with the child's guardian, so as not to violate the legitimate interests of others with the provision that reference to the circumstances of finding the child must not be made. If the real data of the child and the data of the child's parents by blood subsequently become known, the municipal executive initiates a renewed registration of the child's birth.
In this case, the Authority contacted the municipal executives of the above three settlements and requested submission of the documents generated in the course of name determinations by the guardianship authority. On the basis of these documents it was established that the names of children from unknown parents, placed in the baby rescue incubators of the hospitals of the cities under investigation which had been made public were indeed changed, so there was no infringement in any of these cases. [NAIH-3885/2023]

7. Investigation of the lawfulness of surveillance by a camera set up by an individual beside the shrine of a relative in a (public) cemetery

The Authority received a complaint in relation to the lawfulness of surveillance with a camera complete with a solar panel and mobile internet connection set up by an individual on a pole beside the shrine of a relative in a public cemetery.

According to the consistent practice of the Authority going back to years [see: NAIH/2020/5589; NAIH/2017/2155/2/V; NAIH/2015/1090/5/V], not even the operator of a (public) cemetery may monitor the persons in the public cemetery during opening hours. Outside opening hours [therefore in a closed (public) cemetery], surveillance with cameras may in principle be possible from a data protection point of view, but the cameras may not be directed at individual tombs or shrines, they may be set up along the borders of the (public) cemetery (along the fence) and along the main junctions of the cemetery.

Based on the notification, the Authority launched an investigation and pursuant to Section 56(1) of the Privacy Act called upon the controller to decommission the camera set up beside the shrine of his relative in the territory of the public cemetery and to terminate the camera surveillance, in view of the fact that the processing under investigation cannot be made lawful, even by modifying the camera angle or using additional masking, distorting or digital blocking.

The controller did not dispute the content of the Authority's call. In his answer to the call, he attached the modified image made by the camera under investigation on the basis of which the controller applied additional digital blocking (masking), but did not decommission the camera under investigation and did not terminate the camera surveillance.

In view of the above, pursuant to Section 56(1) of the Privacy Act, the Authority repeatedly called upon the controller to decommission the camera and to terminate the camera surveillance; the controller finally complied. He decommissioned the camera under investigation and supported his claim by screenshots.

In view of the fact that the controller took the necessary measures indicated in the Authority's repeated call and provided written information to the Authority on the measures taken and the evidence thereof within the time period indicated in the call, the Authority closed the investigation. [NAIH-1644/2023 (antecedent case number: NAIH-9385/2022)]

II.1.8. Procedures as lead authority

With regard to trans-border processing operations, the Authority dealt with 28 cases last year as lead authority.

Of these, 12 data subject complaints were submitted to the Austrian Authority through the mediation of a human rights organisation called NOYB, in which the Authority acted as lead authority. In these cases, the Authority established that the one-stop-shop system of administering cases cannot be applied based on the report of 17 January 2023 of the "Cookie Banner Taskforce" of the European Data Protection Board as the alleged infringements belong under the scope of the ePrivacy Directive. In its negative decisions, the Authority stated that even if the GDPR were to apply, these cases would still not qualify as trans-border processing operations because the contested websites were Hungarian, and based on all the circumstances of the case, the processing carried out did not involve the processing of personal data of data subjects outside Hungary.

Among the lead authority cases, the submissions against the processing operations of Wizz Air Hungary Légiközlekedési Zrt. (hereinafter: Obligee) represent an outstanding group of cases, because these were lodged in the largest number since the GDPR has become applicable. Of these, several cases have been in progress for some time and are subject to reconciliation among the Member State authorities; last year one case was closed with a decision, two other procedures are just before decision-making, while in another case the next step is to provide opinions on the draft decision, so these too will soon be closed.

In the above-mentioned case closed with a decision, the authorities consulted on an important issue of law interpretation. At first there was no agreement between the Polish, the French and the Dutch authorities and the lead authority, however, an appropriate solution and interpretation of the law was found. The case was about a Polish citizen lodging a complaint with the Polish data protection authority; then it was found that the Hungarian Data Protection Authority was entitled to conduct the procedure in this complaint. Following an investigative procedure, the Authority launched an authority procedure ex officio. According to the complaint, the complainant contacted the Obligee with a request to terminate their account; in response to which the Obligee informed the complainant of the extension of the period open for the procedure on account of the large number of requests. Ultimately, the Obligee met the termination request within the period open for it, of which it failed to inform the complainant. While significantly exceeding the due date, the Obligee informed the complainant of the fact

of termination only because the complainant repeatedly asked whether it was performed. The information then provided, however, did not extend to the fact that the termination did not mean that the entire processing was terminated, the Obligee continued to retain certain personal data of the complainant for additional processing purposes.

In view of all this, the Authority – finally with the agreement of the other concerned authorities – established that the Obligee extended the period available for the exercise of data subject's rights without a sound reason because, under the GDPR, the large number of requests does not mean what the Obligee referred to, that the controller receives a large number of requests in general from data subjects whose personal data it processes, but that the given data subject submitted a larger number of requests to the controller, whose request is subject to an extension of the deadline. In addition, the Authority found that Article 12(3) of the GDPR requires the controller not only to take action based on the data subject's request, but also to notify the data subject of the actions taken.

The Authority also found important deficiencies of content in the subsequent information provided on the erasure as the notification on the actions taken must extend to everything, i.e. in this particular case not only to the fact of the erasure of the account, but also to exactly what additional personal data were processed by the Obligee on the data subject based on its legal obligation or its legitimate interests, and what is the purpose and planned period of the processing of these data.

The complaint also addressed the lawfulness of the processing of the data. In relation to this, the Obligee referred to certain legal obligations (under consumer protection, taxation and accounting law), with regard to which the obligation to retain the data was present in the specific case according to the Authority's position. Furthermore, according to the Obligee, it is entitled to process the complainant's data also for the purpose of documenting the measures it has taken based on the data subject's request and to furnish evidence in the course of the data protection procedure. According to the Obligee, the legal basis for processing to document the measures taken based on the data subject's request is the performance of legal obligation which as pointed out by the Obligee was the principle of accountability according to Article 5(2) of the GDPR, i.e. it regarded the documentation of its procedures carried out on the basis of the data subject's request as its legal obligation arising from the principle of accountability. Emphatically with regard to the circumstances of the specific case, the Authority did not share this position. Although GDPR itself does not determine the mode

of verifying compliance, the principle of accountability in itself cannot be regarded as a provision requiring mandatory processing of data in general; moreover, it should also be highlighted at this point that according to the second half of Article 11(1) of the GDPR, the controller is not obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this regulation. As the legal obligation was not appropriate legal basis in the specific case and the Obligee failed to verify any other legal basis, in this case the Obligee should not have retained the personal data exclusively for the purpose of being able to respond to eventual subsequent requests. In the given case, the Authority did not regard the legal basis of legitimate interest as supportable either – that would have prevailed, had the legitimate interest of the Obligee been real and existed upon the commencement of processing, or the fact that its legitimate interest obtained could have been verified by way of a balancing test – because if the controller grants data subject request, then there is a low probability of having to verify compliance in an eventual legal procedure on the grounds of not granting the requests in a manner that would involve the processing of personal data. In this case, although the controller may have a legitimate interest in processing personal data related to granting the request, it cannot be regarded as present and effective at the time of commencing the processing. It may suffice to demonstrate the measures taken with log files or in the case of an erasure request by showing that the record keeping system does not contain data on the data subject. If, however, the data subject disputes the appropriateness of performance or abusing his right regularly turns to the controller with data subject's requests in order to take revenge for an earlier alleged or real grievance, or if a problem arises in the course of fulfilling the request, such as the controller is unable to grant the data subject's request or could not do so for any reason whatsoever in accordance with the GDPR requirements, or there is a genuine risk for any other reason whatsoever that the data subject will seek legal remedy from the Authority or the court, then considering in each case with the appropriate balancing of interest, the Authority regards the processing of personal data related to the data subject's request acceptable based on the controller's legitimate interest.

With regard to data processed to furnish evidence in the course of an authority procedure for data protection, the Obligee referred to its legitimate interest as legal basis. The Authority arrived at the conclusion that the legal basis was not appropriately determined, i.e. it was not legitimate interest but the performance of a legal obligation, which laid the foundation for the processing. When submitting the evidence in the investigative and then in the authority procedures, the

Obligee met its obligations of making a statement, documentation and cooperation under the GDPR, the Privacy Act and the Administrative Procedures Act.

II.1.9. Recommendations, statements issued by the Authority

1. Recording phone calls to the on-duty primary care service (1830)

The Office of the Commissioner for Fundamental Rights of Hungary (hereinafter: AJBH) informed the Authority that in the course of its investigation into a complaint concerning the recording of phone calls to an on-duty primary care service, it concluded that the procedures and practice of the service provider providing on-duty primary care subject to the complaint give rise to the suspicion of anomalies related to the right to informational self-determination of persons requesting help. In view of this report, based on Section 36 of Act CXI of 2011 on the Commissioner for Fundamental Rights (hereinafter: Ombudsman Act) AJBH notified the Authority concerning the practice of recording images and sound by the on-duty primary care service.

The Authority launched an investigation into the sound recording practice of the on-duty primary care service[2], in the course of which it requested information from the National Ambulance Service concerning the calls to the on-duty primary care service and arrived at the conclusion that the legal requirements for processing the recording of phone calls as personal data were deficient or unclear.

In view of this, pursuant to Sections 38(4)(a) and 57 of the Privacy Act, the Authority *made a recommendation to the Ministry of the Interior (BM) as the organ in charge of healthcare and empowered to legislate in relation to healthcare and to issue regulatory instruments for public law organisations* with a view to avoiding the infringement of rights or the direct threat thereof, to settle the issues related to the processing in question by legal regulation,

- formulate clear data processing requirements with regard to the dispatching system (MIR) at an appropriate legal level , for example, similar to the rules for the 112 uniform emergency call system (ESR), and
- put forward clear provisions on when the recording of a phone call to the on-duty primary care service should be regarded as health data, and for

2 The National Ambulance Service operates the uniform on-duty call number (1830) of the system of on-duty primary care service, which according to the plans would be gradually implemented in the entire country with the exception of Budapest by the spring of 2024.

how long the voice recording should be retained by the controller, taking into account the applicable conditions.

The Ministry of the Interior informed the Authority of its agreement with the recommendation and that the relevant amendment of the law will be addressed in the course of the legislative cycle in the autumn of 2024.

It should be underlined that the investigation of the Authority extended *only to the recording of calls received by the on-duty primary care service, the processing of the recording as personal data and the issue of the exercise of the related data subject's rights,* while the recording of images and the related processing did not constitute the subject matter of the investigation as the Authority could investigate this only on the basis of complaints received in relation to specific locations and not in general. [NAIH-450/2024 (NAIH-7897/2023)]

2. Processing related to the organisation of a class reunion

The Authority was requested to take a stand whether an educational institution can lawfully issue the personal data of its alumni to an organizer of a class reunion who does not have the contact data or identification data of his former classmates for the purpose of organising a class reunion, so as to enable him to notify the members of his class.

The Authority had already published its recommendation concerning this issue in 2015; however, in view of the fact that the legal environment changed substantially after the General Data Protection Regulation became applicable, that recommendation now has only some significance in legal history, so the Authority issued a new statement, which it also published on its website.

In its statement, the Authority explained that it did not identify an appropriate legal basis for the educational institution to forward the personal data of the former classmates to the organizer to let him contact them, because the educational institution does not have such a public task, obtaining the consent of the former classmates is impossible and the educational institution is unable to carry out a balancing test of the legitimate interest of the organizer as a third party. [NAIH-5830/2023].

3. The data protection limitations of using body cameras in relation to supervision by a parking attendant

The Authority received several notifications concerning the fact that certain municipalities carry out the parking supervision tasks and public service tasks related to waiting times in the administrative territories of certain settlements not by employing public area supervisors, but parking attendants who do not qualify as public area supervisors, or through business organisations set up by the municipalities for this purpose. Based on the notifications, parking attendants have recently experienced atrocities on the part of persons involved in the procedures with increasing frequency, resulting in a marked decrease in the parking attendants' sense of security. To improve the security of parking attendants and to efficiently investigate notifications, they wished to equip parking attendants with body cameras recording both images and sound.

The Authority emphatically called attention to the fact that surveillance of public areas is possible only within a narrow range; neither the parking attendant, nor the business organisation set up to supervise parking can be a controller pursuing processing for law enforcement purposes and they cannot process camera data for the purposes of law enforcement in view of Section 3(10)(a) of the Privacy Act (in contrast to public area supervisors). Over and above this, it is not a negligible aspect that equipping parking attendants with body cameras may in the given case qualify as processing for the purpose of workplace supervision, which may also give rise to a number of questions and problems.

Based on the available information, the Authority currently holds the view that equipping parking attendants with body cameras for the sole purpose of improving their security and to ease the collection of evidence (efficient investigation of notifications) is not acceptable; currently, no legal basis can be identified for equipping parking attendants with body cameras, in view of the restrictions in Article 5 of the GDPR.

To achieve the purposes referred to in the notification (improvement of the security of parking attendants and the efficient investigation of notifications), the Authority recommends to work out other solutions, which would not involve the processing of personal data or only to a lesser extent, such as employing parking attendants working in pairs, or the involvement of public area supervisors, who as persons authorised to process data for law enforcement purposes may also use body cameras in view of Section 7(2) of Act LXIII of 1999 on the Supervision of Public Areas (Public Area Supervision Act).
[NAIH-8330/2023; NAIH-8821/2023]

II.1.10. Involvement in the work of other authorities

In its orders, the Hungarian Competition Authority (hereinafter: GVH) asked for the Authority's position several times concerning the compliance of undertakings with data protection requirements in the competition supervisory procedures against Viber Media S.á.r.l., and TikTok Inc. as well as TikTok Technology Limited launched because of the alleged infringement of the prohibition of unfair commercial practices vis-a-vis consumers.

GVH asked for the position of the Authority, inter alia, concerning the commitment statements and proposals of the undertaking subject to the procedure submitted in the competition supervisory procedure, in particular, whether the measures according to the commitment statements can be regarded as compliant with the data protection regulations in force, particularly with regard, for instance, to the substantial involvement of minors among the users of the TikTok platform; and if they are potentially non-compliant, what modifications the Authority would regard to be justified and why.

Beyond the above, GVH asked for the Authority's opinion concerning the collection of statistical data and the personalisation of the service content (particularly with regard to the legal basis of these processing operations); and concerning the data processing standard Interactive Advertising Bureau Europe (IAB).

Each time, the Authority issued opinions according to Articles 57(1)(c) and 58(3)(b) of the GDPR. [NAIH-1086/2024 (antecedent case numbers: NAIH-3240/2023, NAIH-8159/2022); NAIH-2003/2023]

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

II.2.1. Responding to requests for the exercise of data subject's rights based on the Privacy Act

Upon request of the notifier, the Authority launched an investigation pursuant to Section 38(3)(a) of the Privacy Act against the controller concerning the lawfulness of the evaluation of the notifier's request to exercise data subject's rights.

Pursuant to Section 14(b) of the Privacy Act, the data subject shall have the right with respect to his personal data to obtain from the controller, upon request, in accordance with the conditions laid down in this Act, access to his personal data and information relating to the processing of personal data processed by the controller and by a processor acting on its behalf or under its instructions (right of access).

Under Section 17(1) of the Privacy Act, in order to give effect to the right of access, the controller shall, at the request of the data subject, inform the data subject whether his personal data are processed by the controller itself or by a processor acting on behalf or under the instructions of the controller. In his request submitted to the controller, the notifier requested information not only about the processing of his personal data and the related information, but also with regard to the investigation conducted against him, and disputed the findings and conclusions of the investigative authority and objected to the investigative/ procedural actions taken.

The Authority found that only that part of the notifier's submission can be regarded as a request for the exercise of data subject's rights, which concerned information about the processing of his personal data and the related information; the other parts of the submission cannot be regarded as such. In relation to this, the Authority underlined that all the information the controller has to provide under a request for the exercise of data subject's rights is the information about the personal data of the data subject processed by it and the related information as defined in Section 17(2) of the Privacy Act.

To exercise his right of access, the notifier asked for information concerning all his personal data processed by the controller. However, the controller's answer concerning the exercise of the right of access was limited to the processing of the personal data in the notifier's request submitted to the controller and the controller provided the information based on Article 15(1) of the General Data Protection Regulation. In this context, the Authority established that the notifier's request submitted to the controller relate to the law enforcement task of the controller, hence the processing of the personal data in the request should be regarded as processing for law enforcement purposes, to which the provisions of the Privacy Act apply.

Pursuant to Section 17(3) of the Privacy Act, the controller may restrict or reject the enforcement of the data subject's right to access, provided that this measure is indispensable for securing an interest specified in Section 16(3)(a)-(f) of

the Privacy Act. No information was raised in the course of the procedure concerning the controller restricting or rejecting the notifier's right of access. In the course of its investigation, the Authority found that the controller granted the notifier's request to exercise his right of access not on the basis of the relevant provisions of the Privacy Act and not in full, whereby it infringed his right to access according to Section 14(b) of the Privacy Act, as well as Section 17(1)-(2) of the Privacy Act. Pursuant to Section 56(1) of the Privacy Act, the Authority called upon the controller to meet the notifier's request to exercise his right of access with respect to all the personal data of the notifier processed by it on the basis of the provisions of Section 17 of the Privacy Act, or notify the notifier of the restriction or rejection of granting the request. Finally, the controller granted the part of the notifier's request to exercise his right of access in accordance with the Authority's call and based on the provisions of Section 17 of the Privacy Act.

II.2.2. Evaluation of a request repeatedly submitted for the exercise of data subject's rights

In an Authority procedure for data protection launched upon request, the Authority investigated the lawfulness of the procedure of a national security service (hereinafter: controller) related to requests for the exercise of the right to access. In his submission, the petitioner requested access to his personal data and classified personal data concerning his state of health from the controller and requested information whether he had been exposed to neurotoxin or any other harmful agent. The submission lodged with the controller did not specify clearly the subject matter of the request, the wording of the submission did not reveal that a part of the petitioner's request was to exercise his right of access. The controller does not keep records of the health-related data of citizens; it processes personal data, classified personal data and law enforcement related personal data for the purpose of performing its national security tasks, which may include health-related personal data in the case of certain data subjects. Because of that, the controller informed the petitioner that it had no competence or powers to grant the request in his submission.

After this, the petitioner clarified his request, and a part of it was clearly to exercise the right of access according to Section 14(b) of the Privacy Act. The petitioner submitted requests to exercise his right of access to the controller several times within a short period. The controller evaluated the merits of the petitioner's request for accessing his personal data qualified as national in an administrative authority procedure. The controller also evaluated the merits of the petitioner's

request submitted earlier to access his personal data and informed the petitioner of rejecting his request to exercise his right of access.

The petitioner repeatedly requested the controller to provide access to his classified personal data. Evaluating the petitioner's request to exercise his right of access, the controller rejected it in its order pursuant to Section 46(1)(b) of the General Administrative Procedures Act, together with the decision concerning the permissions to access. However, the controller's procedure related to the evaluation of requests for the exercise of the right of access is not an administrative authority procedure, thus the request for the exercise of the right to access should not have been rejected pursuant to Section 46(1)(b) of the General Administrative Procedures Act.

The relevant provisions of the Privacy Act do not provide a possibility for the controller to refrain from evaluating the merits of requests to exercise the right of access submitted repeatedly. Section 15(3) of the Privacy Act authorises the controller only to demand reimbursement of the costs directly incurred in relation to the repeated and unfounded enforcement of the data subject's rights from the data subject. In the meantime, a change took place in the range of personal data processed by the controller.

In every case, controllers must respond to requests for the exercise of data subject's rights pursuant to the provisions of Section 17 of the Privacy Act. Under Section 17(4) of the Privacy Act, in the event of restricting or rejecting the enforcement of the right to access, information must be provided to the data subject of the fact of the restriction or rejection of access and its legal and factual justification, if making them accessible to the data subject does not endanger the assertion of an interest defined in Section 16(3)(a)-(f), as well as of the rights to which the data subject is entitled pursuant to this Act, and the mode of their enforcement, in particular about the fact that the data subject may exercise his right to access through the involvement of the Authority.

The Authority established that the controller did not act lawfully when it rejected the petitioner's request for accessing his personal data in accordance with Section 14(b) of the Privacy Act based on Section 46(1)(b) of the General Administrative Procedures Act. The controller violated the petitioner's right to access according to Section 14(b) of the Privacy Act, as well as its Section 17 as it provided information on granting or restricting or rejecting the petitioner's request to enforce his right to access not in accordance with the provisions of the Privacy Act. In view of this, the Authority ordered the controller to grant the pe-

titioner's request to access in accordance with Section 17 of the Privacy Act, or to notify him on the restriction or rejection of the request in accordance with the Privacy Act. [NAIH-5383/2023]

II.2.3. The lawfulness of processing related to mail to detainees from organisations indicated in Section 174(4) of the Penalties Execution Act:

Based on a notification, the Authority investigated the lawfulness of the processing practice of a penitentiary institution in connection with the correspondence of detainees. The processing of data related to the correspondence of detainees, its recording and checking by a penitentiary institution constitutes processing for law enforcement purposes, to which the provisions of the Privacy Act apply. Pursuant to Section 5(1)(a) of the Privacy Act, personal data may be processed, if it is ordered by law or – on the basis of an authorisation by law within the range specified therein, in the case of data that do not qualify as special category data or law enforcement-related personal data – by decree of a municipality for a purpose based on public interest. Pursuant to Section 76(1) of Act CCXL of 2013 Execution of Penalties, Measures, Certain Coercive Measures and Detainment for Misdemeanours (hereinafter the Penalties Execution Act), a penitentiary institution as the organ responsible for enforcement may process the personal data of the detainees in relation to enforcement for the purpose of discharging its tasks specified in this Act. Pursuant to Section 76(2)(m) of the Penalties Execution Act, a penitentiary institution can lawfully process the personal data of detainees required for the exercise of its rights and the performance of its obligations. Pursuant to Section 174 of the Penalties Execution Act, detainees have a right to correspondence and based on Section 174(2) the penitentiary institution is responsible for forwarding letters written by the detainees and delivering letters to detainees. Pursuant to Section 174(3) of the Penalties Execution Act, the penitentiary institution is both entitled and obligated to carry out a security check of correspondence. At the same time, Section 174(4) of the Penalties Execution Act contains a restrictive provision, according to which the content of the correspondence of the convict with the authorities, international human rights organisations recognised by an international convention promulgated by law as competent, the fundamental rights commissioner, the organisation or staff member of the national mechanism for prevention and the defence attorney may not be checked.

In this case, the documents of a litigation sent to the notifier by a district court electronically through the OBH system were received and filed by the penitentiary institution in the Robotzsaru [Robot Cop] system and copied to an external

media to provide access to the documents for the notifier. The staff members performing case management tasks had partial access to the content of the documents of the litigation in the course of their case management operations in order to identify the recipient detainee and the case type to select the specialised area acting in the case and the personal data contained therein. Owing to the technical features of the Robotzsaru system, the case management staff can identify the recipient of electronic documents sent by the courts, whether they are for the penitentiary institution or a detainee, only after opening such mail and partially accessing its content; it is only after this that the case type can be identified and the specialised area taking action can be selected, hence partial access to the content of documents is indispensable for performing case management operations and the identification of cases in progress.

At the same time, pursuant to the restrictive provision in Section 174(4) of the Penalties Execution Act, penitentiary institutions are not authorised to have access to and process the content of detainee correspondence with the organs defined in Section 174(4) of the Penalties Execution Act and the personal data therein.

Section 99(3) of Decree 16/2014 (XII. 19.) IM on the detailed rules of the execution of imprisonment, detention, pre-trial detention and detention in lieu of a fine authorises penitentiary institutions only to record the dates of dispatch and receipt and the recipient or the sender in relation to the detainee's correspondence with the organisations defined in Section 174(4) of the Penalties Execution Act and with the defence attorney.

In its answer, the penitentiary institution stated that during the execution of imprisonment, the detainee's right to electronic administration is suspended, penitentiary institutions have to provide an opportunity for studying electronic documents in view of Section 127(1) of the Penalties Execution Act. The Authority called the attention of the penitentiary institution to the fact that under Section 127(1) of the Penalties Execution Act, the possibility for studying electronic documents must be provided to detainees in penitentiary institutions with respect to documents generated in cases in progress or former criminal procedures against the detainee. In the case under investigation, the district court sent documents to the notifier generated in relation to a property settlement litigation. Furthermore, according to Section 127(1) of the Penalties Execution Act, the court, the prosecution or the investigative authority may not forward the documents or copies generated in current or former criminal procedures as electronic mail, which pen-

itentiary institutions receive through the Robotzsaru system, instead they send such documents on electronic media.

In the course of its investigation, the Authority found that the practice of the penitentiary institution related to processing mail sent to detainees through the Robotzsaru system by organisations defined in Section 174(4) of the Penalties Execution Act was non-compliant from the viewpoint of the protection of personal data as the case managers or administrators on the staff of the penitentiary institution were not authorised to access the content of the notifier's electronic correspondence with the district court and the notifier's personal data therein, some of which were also recorded in the subject column of the filing system. So, there was an infringement in relation to the processing of personal data.

As this was an infringement related to the general practice of the penitentiary institution, the Authority made recommendations based on Section 56(3) of the Privacy Act to the National Command of Penitentiaries(hereinafter: BVOP) as the supervisory organ of the penitentiary institution. The Authority called upon BVOP to transform the practice of penitentiary institutions related to the processing of mail for detainees from organisations defined in Section 174(4) of the Penalties Execution Act through the Robotzsaru system by applying technical and organisational measures, so as to comply with the protection of personal data and the provisions of Section 174(4) of the Penalties Execution Act, or to notify the organisations defined in Section 174(4) of the Penalties Execution Act forwarding documents to the detainees electronically in accordance with Act CCXII of 2015 on the General Rules for Electronic Administration and Trust Services, if they send the documents this way, the penitentiary institutions are unable to comply with the rules of data protection and data security. In view of the fact that the right of detainees to electronic administration is suspended, sending the documents addressed to them in hard copy or electronic media in closed envelopes complies with the rules of data protection. [NAIH-3949/2023]

II.2.4. Violation of the principles of purpose limitation and data minimisation in criminal procedures

Upon request, the Authority investigated in an authority procedure for data protection whether the prosecutors lawfully forwarded the law enforcement-related personal data of the petitioner to the plaintiffs and their legal representatives in a criminal procedure. According to the Preamble to Act XC of 2017 on Criminal Procedures (Criminal Procedures Act), the Act lays particular emphasis on the intensive protection of the plaintiffs in criminal procedures and the enforcement

of their rights, hence this is also a responsibility for the organs acting in criminal procedures. In its decision, the Authority established that the prosecution met its express responsibility specified in the Criminal Procedures Act (*particular protection of plaintiffs of criminal procedures and the facilitation of the enforcement of their rights*) by forwarding an abstract of the indictment constituting a part of the documents of the procedure accessible to the plaintiffs in view of their position in the procedure to the plaintiffs and their legal representatives, particularly in view of the fact that the accused kept secret the court and authority decisions, which established with final force, the infringement of the companies earlier represented by the petitioner, in the payment order and distraint procedures initiated by the accused against the plaintiffs. In view of their procedural position, the plaintiffs and their representatives were authorised pursuant to the relevant provisions of the Criminal Procedures Act [Sections 98(3), 51(1)] to have access to the abstract of the indictment as a document related to a criminal act affecting them. The legal basis for processing by the individuals who had access to the abstract of the indictment through having it forwarded by the prosecution, i.e. the plaintiffs and their legal representatives, is Article 6(1)(f) of the General Data Protection Regulation, according to which personal data are lawfully processed, if it is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, and Article 9(2)(f) of the General Data Protection Regulation, which states that special category data – in this case law enforcement-related personal data – can be processed if processing is necessary for the establishment, exercise or defence of legal claims, or whenever courts are acting in their judicial capacity. The prosecution made an abstract of the indictment, in which the accused were identified only by the first letter of their surname and their given names, it did not contain their identification data and the companies concerned and named in the indictment were terminated without a legal successor after the submission of the indictment. Yet, anonymisation was not realised by making such an abstract of the indictment. The Authority underlines that in relation to anonymisation, the expectation is that it should be impossible to re-establish the link between the anonymised data and the identified or identifiable natural person, i.e. the natural person should not be identifiable. In this case, the person of the petitioner remained identifiable based on the content of the indictment, particularly for the persons concerned in these cases.

In view of the fact that the abstract of the indictment contained the law enforcement related personal data of the petitioner in a manner that could be linked to the petitioner, the Authority examined whether the prosecution acted in compliance with the principles of purpose limitation and data minimisation when forwarding the personal data included in the abstract of the indictment. Sections

4(1) and (2) of the Privacy Act stipulate the principles of purpose limitation and data minimisation. The principle of purpose limitation is one of the most important principles of processing developed internationally, according to which personal data can only be processed for a clearly determined lawful purpose to exercise a right and to meet an obligation. When the principle is complied with, the controller processes only those personal data, which are necessary for performing its tasks and functions. Compliance with the principle of data minimisation guarantees that only the narrowest justified range of data are processed with a view to the purpose of processing. The requirements of purpose limitation and data minimisation extend to all stages of data processing, including the transfer of data. It is to be underlined that controllers have to take into account the principles of data protection, including those of purpose limitation and data minimisation when forwarding personal data. Even if there is a legitimate purpose of processing, only the data indispensable and suitable for achieving the purpose of processing can be processed and forwarded.

The Authority established that the prosecution failed to separately examine the purpose limitation and necessity of processing with regard to the individually forwarded personal data when it forwarded the abstract of the indictment. The abstract of the indictment disclosed the law enforcement-related personal data of the petitioner related to his former conviction and criminal record and the prosecution failed to support the necessity of forwarding these personal data for achieving the purpose of processing, i.e. the enforcement of the rights of the plaintiffs. In view of this and based on Section 61(1)(b)(ba) of the Privacy Act, the Authority established the infringement of the processing of the petitioner's personal data because the prosecution violated the principles of purpose limitation and data minimisation set forth in Section 4(1)-(2) of the Privacy Act in the course of a data transfer operation.

Having taken all the circumstances of the case into account, the Authority did not deem it justifiable to levy a fine on the prosecution. The Authority rejected the part of the petitioner's petition concerning the prohibition of the unlawful processing of personal data as the prosecution lawfully processed the personal data of the petitioner, including the law enforcement related data concerning his former conviction. However, in the course of the data transfer, the prosecution should have taken into account the principles of data protection, including those of purpose limitation and data minimisation.

Both the petitioner and the prosecution submitted petitions to the Budapest Municipal Court against the Authority's decision; the court procedure is in progress. [NAIH-601/2023]

II.2.5. A police station failed to inform the contacted bank that it can lift the restriction according to Section 264(7) of the Criminal Procedures Act

In his complaint launched with the Authority, the complainant stated that the police station conducted a criminal procedure against him, under which it contacted the bank and requested the bank data of the complainant as set forth in the Criminal Procedures Act. The complainant saw no confirmation that the request for data had been authorised by the prosecution and even though the investigative phase of the criminal procedure was completed at the bank, the investigative authority did not notify the bank that it can lift the restriction of information concerning the complainant, hence his data subject rights were breached. The complainant also objected to the fact that the police station failed to let the complainant know of the fact at the time of presenting the documents in the criminal procedure that his data subject rights were restricted by the bank. Based on Section 38(3)(a) of the Privacy Act, the Authority launched an investigation to establish whether any infringement took place in relation to the processing of personal data.

Answering the Authority's question, the police station informed the Authority that it sent the case to the prosecution recommending indictment; no final verdict has been brought in the case in the absence of which it is not possible to comply with the provisions of Section 264(7) of the Criminal Procedures Act. According to Section 264(7) of the Criminal Procedures Act, if providing any information about the data request would jeopardize the success of the criminal proceeding, the organ requested to provide data, if specifically instructed by the organ requesting the data may not provide any information to any other person or entity about it and it shall ensure the secrecy of the request, its content, or any data transferred in the course of complying with the request. If a person affected by the request for information concerning the processing of his own personal data, he shall be provided with information that does not reveal that his personal data were transferred for the purpose of a data request. The organisation requested to provide data shall be advised about this provision in the data request. Pursuant to Section 264(8) of the Criminal Procedures Act, the restrictions specified in paragraph (7) may remain in place until the preparatory proceeding or the investigation is completed, unless lifting the restriction would jeopardise the success of another criminal proceeding conducted against the person concerned. The organisation

requested to provide data shall be notified about lifting the restriction. To clarify the facts of the case, based on Section 54(1)(a) and (c) of the Privacy Act the Authority contacted the police station again, asking them to justify in detail what impeded the lifting of the restriction in the case of a procedure completed with the recommendation to indict in view of the provisions of Section 264(8) of the Criminal Procedures Act. The police station stated that the member of the investigative authority taking action in the case failed to inform the bank of lifting the restriction according to Section 264(7) of the Criminal Procedures Act after the receipt of the indictment by the investigative authority and the completion of the investigation in accordance with Section 348(5)(b) of the Criminal Procedures Act. The prosecution submitted the indictment to the Budapest Municipal Court, which brought a judgement of first instance. Based on the information provided orally by the prosecution, the judgement of first instance was not yet final as the petitioner appealed it. The investigative authority contacted the bank based on Section 262(1)(e) lawfully and on good grounds, just as it ordered the restriction according to Section 264(7) of the Criminal Procedures Act. The petitioner's data subject's rights were not breached because of the failure to provide information concerning the lifting of the restriction according to Section 264(8) of the Criminal Procedures Act as simultaneously with accessing the documents of the investigation, he learned of the investigative authority contacting the bank.

Based on Section 56(1) of the Privacy Act, the Authority called upon the police station to inform the bank of the lifting of the restriction according to Section 264(7) of the Criminal Procedures Act and take measures to enforce the rule as set forth in Section 264(8) in the course of criminal procedures. In the document enclosed with its answer, the police station notified the bank based on Section 264(8) of the Criminal Procedures Act that the maintenance of the restriction according to Section 264(7) was no longer justified as the investigation had been completed. The police station also informed the Authority that in order to avoid similar cases in the future, measures were taken to ensure that data requests sent by the regional and local agencies of BRFK to the contacted organ only include a warning pursuant to Section 264(7) of the Criminal Procedures Act if it is absolutely justified and necessary for the success of the criminal procedure and the necessary measures should be taken to lift the restriction ordered according to Section 264(7) of the Criminal Procedures Act following the completion of the procedure. Measures were also taken so that senior staff carry out random checks of the full execution of the above. [NAIH-5889/2023.]

II.2.6. Cases related to restricted processing

II.2.6.1. Failure to process personal data in a restricted manner in the course of a criminal procedure

Two petitioners submitted a joint petition in a case to the Authority, in which they objected to the 11th District Police Station of the Budapest Police Headquarters' failure to process their data in a restricted manner despite their express request. According to the petition, the petitioners lodged a report with the Police Station, in which they requested the restricted processing of all their data including their names in accordance with Section 99 of the Criminal Procedures Act, in view of the fact that they were relatives of the person reported, so they had an overriding interest in not revealing the fact that they lodged the report. One of the petitioners repeatedly requested the restricted processing of his data in the course of his hearing as a witness.

A decision of termination was made in this criminal case, which the Police Station sent to the accused in addition to one of the petitioners, and to the defence attorney of the accused, containing the name of the petitioner.

The petitioners turned to the Police Station requesting information whether their personal data were indeed sent to the accused and his defence attorney. The Police Station investigated the submission and established that the petitioners indeed requested the restricted processing of all their data including their names. Owing to a failure by the case manager, the abstract of the minutes drawn up of the questioning of one of the petitioners as witness, the name of the petitioner was indicated, which was then sent to the defence attorney of the accused as part of the documents of the investigation. The Police Station failed to anonymise the documents of the investigation sent with regard to either of the petitioners, and the name of one of the petitioners as informant was shown in the decision terminating the procedure. This infringement of the provisions of Section 99 of the Criminal Procedures Act concerning restricted processing of the data gave rise to a data breach because the protection of the personal data was violated by letting the accused have access to the personal data of the petitioners. The Police Station notified the data subjects of the data breach, however, it did not report the data breach to the Authority, because in their view it did not pose a risk in view of the fact that the petitioners were relatives of the person they accused, hence they knew one another's personal data in any case.

With reference to Section 99(10) of the Criminal Procedures Act, the person in charge of the case deemed that the name otherwise to be processed in a restricted manner could be shown in the decision terminating the procedure and it could be forwarded also without the consent of the data subject. However, the commentary on Section 99(10) of the Criminal Procedures Act states that data subject to restricted processing may be indicated only in cases and to the extent absolutely necessary – e.g. instead of a full address, it suffices to show the name of the settlement in determining the competence of the court. In these cases, the protection of personal data can be ensured only with the stringent application of the absolutely necessary extent. In the case under investigation, the part of the decision containing the name of the petitioner was the one providing for who the document should be delivered to. Pursuant to the provisions of Section 363 of the Criminal Procedures Act, a decision brought in criminal proceedings – including the decision terminating the proceedings – need not contain the identification data of the persons to whom the decision has to be delivered. The introductory part of the decision has to include the names and identification data of the person(s), to whom the provision applies. Showing the name of the addressees in the decision ab ovo violates the principle of purpose limitation because showing them is absolutely unnecessary as it could only have administrative reasons. Had the petitioner not requested the restricted processing of his data, the Police Station should still have shown the delivery data (name, address) of the addressees in a separate delivery clause.

With regard to the practice applied, the Police Station made the following statement: *"After the closure of every procedural act, minutes are drafted, signed by the person concerned in the procedure following reading it. This means that the data subject can see already on the signed document which of his data were processed in a restricted manner and which are the ones that are visible."* According to the Authority's position, this procedure is insufficient to ensure restricted processing because even if the content of the document is anonymised, the petitioner by signing the minutes drawn up on his hearing as witness has to show his name in the document and if it is legible, it becomes accessible to the accused when studying the documents. It follows that the signature should be blocked.

The Police Station also stated that when signing the minutes of his witness hearing, the petitioner was aware that no data other than his name was shown in the document; however, in view of the fact that the petitioner did not specifically indicate with regard to which of his data he requested restricted processing, in the Authority's view his statement should be interpreted that all his data including his name are to be protected. In view of all these, the Authority established the

fact of the unlawful processing of personal data based on Section 61(1)(b)(a) of the Privacy Act, because of the violation of data security measures set forth in Section 25/I(1) and (3)(b) and (h) of the Privacy Act.

The Authority did not accept the argument of the Police Station, according to which the data breach implied no risk because of the relationship of the informants (petitioners) and the accused. It was precisely because of the family implications of the case that the petitioners requested the restricted processing of their personal data expressly including their names because in their view they had an overriding interest in not revealing their identities exactly because they were relatives. In their case, their names were in themselves data to be protected, so that they are not linked with their capacity as informants. Precisely what they wished to avoid took place with the failure to process their personal data in a restricted manner, hence this incident was injurious for them. The petitioners have a law-given right to request restricted processing; moreover, the fundamental law ensures the right to respect privacy and family life for them. Based on Section 25/K(1) of the Privacy Act, a data breach is high risk, if it may be concomitant with consequences substantially influencing the enforcement of a fundamental right to which the data subject is entitled. It is the Authority's position that in this case the right of the petitioners described above and ensured in the Fundamental Law was violated as a result of the data breach, hence it can be established that it was of high risk. According to the Authority's position, the Police Station should have notified the Authority of the data breach based on Section 25/J(1) of the Privacy Act. As the Police Station failed to notify the data breach, the Authority established the infringement of Section 25/J(1) of the Privacy Act.

The Authority considered all the circumstances of the case and based on Section 61(1)(b)(g) of the Privacy Act decided to impose an administrative fine on the Police Station. [NAIH-1637/2023]

II.2.6.2. Failure to grant restricted processing of personal data, delayed notification of a data breach

In relation to the notification of a data breach by a Police Station, the Authority carried out an authority supervision followed by an authority procedure. According to the data breach notification, minutes were drafted of the report by a person concerned in the data breach.

The notifier (as aggrieved party) requested the restricted[3] processing of his personal data confirmed by his signature. The person drafting the minutes of the report failed to delete the data whose restricted processing was requested from the minutes and forwarded the minutes to the competent prosecution. The notifier lodged a complaint with the Police Headquarters objecting to the fact that the person he reported gained knowledge of his address as his data were not processed in a restricted manner.

In the case under investigation, the hard copy file indicated the request for the restricted processing of the data (minutes of the report) in the RZsNeo system. The case manager had an extract made, but failed to delete the data for which restricted processing was requested from the minutes and uploaded it in the RZsNeo system in this way. Monitoring restricted processing would have been expected not only from the case manager but also from his direct manager, the head of the Criminal Department of the Police Station concerned, as well as from the administrator of the filing operation in this case. No unblocked minutes should be retained in the RZsNeo system among the electronic files, yet this happened in the case under investigation. According to the statement of the Police Station, no organ or person had access to the personal data other than the persons participating in the administration of the notifier's report and the prosecution. The prosecution concerned in the case under investigation was not aware that the personal data of the data subject should have been processed in a restricted manner, hence it was not in a position to protect the data before the submission of the complaint. Because of this, the person reported by the data subject learned of the data subject's address in the absence of restricted processing.

In the case under investigation, it was found that the range of data affected by the data breach was wide as the minutes contained the data subject's identification data and contact data, which could then be linked with law enforcement-related personal data. Unauthorised access to the minutes may provide an opportunity for identity fraud; furthermore as a result of the data breach, the person of the notifier and his position in the criminal proceedings became known to the accused.

3 *Restricting processing in the case management and administration system of the police (hereinafter: RZsNeo system) operates in such a way that personal data appear in the minutes even if data are processed in a restricted manner. Restricted processing should be done by printing the entire minutes after reading the pop-up window shown after writing the minutes, which must be signed by the client (in this case the informant/aggrieved party) and the person taking the investigative action. Then the minutes are displayed in full in an editable format, from which the personal data, for which the data subject requested restricted processing have to be erased one by one. The extracted minutes must be signed and then placed with the hard copy documents of the investigation.*

Having taken all the circumstances of the case into account, it was established that the data breach was of high risk. As evidenced by the statements made in the course of the authority investigation, the Police Station did not take the appropriate data security measures to prevent personal data subject to restricted processing appearing in the RZsNeo system. The case manager failed to complete the action for making an extract because he failed to delete the data subject to restricted processing from the minutes. The Authority also established that the Police Station notified the Authority of the data breach with a delay exceeding 72 hours after learning of the data breach.

The Authority established the infringement of the provisions of Section 25/I(1) and (3)(b) and h), as well as of the obligation set forth in Section 25/J(1) of the Privacy Act. The Police Station carried out its processing operations not in accordance with the relevant legal regulations as it failed to do restricted processing and notified the data breach with a delay. For these reasons and based on Section 61(1)(b)(ba) of the Privacy Act, the Authority established the fact of the unlawful processing of personal data. [NAIH-7702/2023]

II.2.7. The Authority's recommendation to amend the Penalties Execution Act

The Office of the Commissioner for Fundamental Rights (hereinafter: AJBH) received a notification by mail on 20 September 2021, according to which persons in the Female Ward of the Judicial Institute for Observation and Mental Treatment (hereinafter: IMEI) are upset by the cameras in the dining hall and above the nurses' counter, which allegedly have a negative impact on the health of certain patients. AJBH transferred the complaint to the Authority on 14 April 2022. The Authority launched an ex officio investigation in the case.

Section 150 of the Penalties Execution Act applies to the surveillance of convicts and not a wider category, i.e. that of detainees. The Authority pointed out that in the case of IMEI, the category of detainees consists not only of convicts, but also of persons subject to involuntary medical treatment and pre-trial detainees may also stay in the field of vision of the cameras objected to. In the case of persons subject to involuntary medical treatment and pre-trial detainees, there are no references in the Penalties Execution Act to rules applicable to convicts.

The Authority established that there was a direct threat of violation of rights in relation to the exercise of rights set forth in the Privacy Act, in view of the fact that the legal regulation of the possibility of applying instruments of electronic surveillance was not clear with regard to the category of detainees as it was re-

stricted to the surveillance of convicts, while in practice IMEI and penitentiary institutions interpret the possibility of applying instruments of electronic surveillance or instruments of surveillance ensuring control with regard to persons who may be subject to surveillance. So, the Authority made a recommendation to the Minister of the Interior to review Section 145(1) and Section 150 of the Penalties Execution Act in view of the unclear provision and to consider the extension of processing required by these provisions to the entire range of detainees, or in the case of IMEI – in view of its special category of detainees, which differed from that of other penitentiary institutions – review whether a separate piece of legislation should be enacted, to settle the detailed rules of security measures in the case of this institution. The purpose of the recommended measure is to align Sections 145 and 150 of the Penalties Execution Act with legal practice and that the legislator should clearly clarify the legal framework in relation to detainees held on other grounds in addition to convicts.

In its answer of 24 August 2023, the Ministry informed the Authority that because of the unclear regulation of the subject matter, it deems that an amendment of the Penalties Execution Act is justified, it shared the position of the Authority that it is necessary to address the legal basis of using instruments of electronic surveillance with regard to persons subject to involuntary medical treatment and those subject to pre-trial involuntary medical treatment, the purpose of use, the location of installation in line with the purpose, and the conditions of recording, retaining, erasure, as well as the use of the recording and the personal data therein.[NAIH-4848/2023]

II.2.8. Detainee requests for having access to recordings made on account of camera-related processing by a penitentiary institution

Based on the notification of a detainee (hereinafter: notifier), the Authority conducted an investigation in a penitentiary institute (hereinafter: institute) in relation to the camera surveillance of detainees in the course of work. The Authority examined the issue of data subject's access to the camera recording made with a view to checking work, the processing of the recording with regard to the period of retention, as well as the identity of the controller and the issue of joint processing. In addition to the processing of the camera recordings, the Authority investigated the data security measures underpinning the availability of requests submitted by detainees.

At the time of the recording under investigation, masks were mandatory because of Covid during work organised for the detainees of the institute. The notifier got

a disciplinary penalty because of the violation of the mask-wearing rules. The notifier requested several times, both orally and in writing, that the camera recordings be made available to him as evidence; however, all his requests were denied. According to the institute, looking at the recordings revealed that the notifier violated the mask-wearing rules on several occasions. The institute handled the submissions of the notifier as requests to access documents. The investigation also revealed that it was primarily the company established by the institute to provide work for the detainees that had access to the camera recordings, the persons supervising work watched the event giving rise to the disciplinary procedure, the result of which was recorded in writing, which was then included in the documentation of the disciplinary procedure.

Indeed, the requests of the notifier were not formulated in such a way as to grant access to the camera recordings as a data medium containing personal data or to view the recordings as personal data. Essentially, however, they were aimed at having access to the recordings containing the personal data of the data subject. The existence of the recordings as personal data is independent of the disciplinary procedure, they were made prior to the procedure. Viewing the recording containing personal data must be ensured for the data subject under the right of access regulated by the Privacy Act provided that the recording is still available. An access request may be denied only if the conditions set forth in the Privacy Act obtain. Even in such a case, the data subject must be informed of the fact of the denial, its legal and factual justification and, furthermore, of the possibilities of legal remedy and of the fact that pursuant to Section 17(4)(b) of the Privacy Act, the data subject may exercise his rights also through the Authority. Information about the factual and legal justification of a denial may be waived only in the cases specified by law.

According to the institute, pursuant to Section 26 of the Penalties Execution Act the exercise of data subject's rights is implemented so that the detainee may inspect the documents available in hard copy, may request copies of them and he may have access to documents available in an electronic format on a data medium or in a printed form. Section 26(4) of the Penalties Execution Act specifies the documents to which the right of access does not apply. However, it can be established that the recordings are not included in the category under Section 26 of the Penalties Execution Act, hence access to them cannot be excluded. According to the institute's statement, the camera recording did not constitute a part of the documentation of the disciplinary procedure. Essentially, the disciplinary documents recorded only that in the course of the disciplinary proceedings during his hearing, the notifier did not ask for a checking of the recordings, nev-

ertheless they were viewed on the basis of which a violation of the rules of mask-wearing was established.

The Authority found that the part of the request for access to the camera recordings should have been assessed as a request to access submitted as part of the exercise of data subject's rights according to the Privacy Act and answered accordingly. If the institute did not have the recording, they should have directed the notifier to the controller. The Authority underlined that with regard to the recordings made by the camera system, the detainee deployed at the venue of work must be informed, inter alia, of the person of the controller, the name and contact details of the data protection officer, the rights to which data subjects are entitled, as well as the mode of their enforcement based on the provisions of Section 16 of the Privacy Act as information provided in advance. In possession of this information, the persons in the recordings would know what rights they can enforce with whom in relation to their personal data in the recordings.

In terms of the retention and the availability of the submitted requests, the investigation exposed that there were no measures to ensure the protection of detainee requests as data media containing personal data in the phase of the processing when the detainee submits his request to the person authorised to receive it to the point when it is recorded in the Főnix 3 electronic information system. Such a security measure could be, for instance, if the fact, time and date of receipt and the subject matter of the request were confirmed at the time of the submission of the request and the detainee could retain a copy of the request.

The investigation found that the recordings were erased after 60 days according to the default setting of the camera system, which in the case under investigation was in compliance with the legal requirements. The controller verifiably did not receive a request to waive the erasure of the recordings within the statutory period and the disciplinary procedure in which reference was made to the recording was completed well before the date of the erasure.

The processing of the camera recordings was carried out for the purpose of surveying the work according to Section 3(13) of the Penalties Execution Act, which was organised by a limited company as the business entity set up to organise the mandatory employment of detainees. The recordings were not included among the documents of the disciplinary procedure carried out by the institute; the institute did not have it in the course of the procedure. The person supervising the work of detainees as part of the company's activities noted the violation of the mask wearing rules and it was after this that he viewed the recordings. The

fact and the result of viewing the recordings were entered into the supervision log issued by the Production Department of BVOP Ltd. Then, the same person performing supervision initiated the disciplinary procedure using the disciplinary sheet issued by the institute, which was approved by another person on the staff of the institute.

Based on the provisions of Section 25/B of the Privacy Act, if joint processing takes place according to the actual situation with regard to the processing of camera recordings made in the course of work organised for detainees, then – according to the Privacy Act, in the absence of governing legal regulation containing all details to the extent not regulated by the legal obligations governing them – the joint controllers have to specify the performance of their obligations related to joint processing in a written and published agreement. In particular, they have to specify the obligations related to answering data subjects' requests, as well as the division of their responsibility related to any eventual failure with regard to these obligations. As to the camera system used by the company during the work it organises, the company and the institute involved in the processing activities operating the camera system, managing the recordings and eventually using them, have to enter into an agreement with the above provisions and based on Section 25/A(3) of the Privacy Act – if the controller is subject to an obligation to appoint a data protection officer – they have to enact and apply internal data protection and data security rules in accordance with the actual situation and the legal regulations. The Authority underlined that in the event of joint processing, such an agreement has to cover the tasks related to meeting and answering requests related to data subject rights.

The data protection officer of the company referred to Section 5 of the cooperation agreement concluded between the company and the institute on 11 February 2021 with regard to the processing of the images recorded in the case under investigation; however, this agreement was concluded after the recordings were made. According to Section 5 of the agreement referred to, the institute is the controller of the recordings made by the camera system, to which the company may have access according to a separate agreement, or for the purpose of investigating the suspicion of disciplinary acts, misdemeanours or criminal acts if needed.

Paragraph (1) of Section 150 of the Penalties Execution Act amended as of 1 January 2023, now specifically mentions processing by means of electronic surveillance instruments at the venue of the work managed by a penitentiary institute; the provision of the new paragraph (1)(a) enables the use of electronic

surveillance instruments operated by another law enforcement organ located at an external venue of work, which is not managed by the penitentiary institute for a purpose specified in paragraph (1). This means that the latter provision enables joint processing as set forth in the law, but it does not regulate its details. On that basis, if the work organised by the company qualifies as work carried out at an external venue and the penitentiary institute has direct access to the camera system, the penitentiary institute and the company as joint controllers have to specify their obligations and the division of their responsibilities in a written agreement made public.

As the data protection rules were not fully enforced in the course of the processing under investigation and there was an infringement related to the processing of personal data, the Authority called upon the institute and the limited company to review the processing and clearly determine the person(s) of the controller(s) and the eventual processor, to specify their tasks accordingly and to determine the appropriate authorisations and obligations. The controller has to take action to have the obligations set forth in Section 16 of the Privacy Act concerning advance information in the context of the processing operation by means of cameras under investigation. Requests for viewing the recordings of the camera system should be met by assessing them as requests to access and they should answer them or reject them as such based on the provisions of the Privacy Act. If the controller of the recording is not the penitentiary institute, it should provide information to the person requesting it about the identity of the controller in each case. The Authority called upon the penitentiary institutes to ensure that availability is not impaired and data are not lost and the path of the personal data be traceable following the submission of the requests with the appropriate data security measures (e.g., a copy retained by the detainee) with regard to the processing of requests as media containing personal data submitted by detainees to the penitentiary institute. [NAIH-4952/2023]

II.2.9. Processing of the HR file of a former professional staff member for defence purposes

A former professional staff member, now a reserve officer contacted the Central Archive of the Military History Archive of the Military History Institute and Museum of the Ministry of Defence (hereinafter: Central Archives) asking for information about the storage of his HR folder; but these documents were not available in the Central Archives. Then, he initiated an investigation by the Authority to determine what happened to the documents containing personal data related to his professional career and family, and his employment documents containing his

periods of service; how was it possible that years after the termination of his service, they could not be found.

Pursuant to Section 10(6) of Act XCVII of 2013 on Processing by the Army and Military Administrative Tasks related to the Performance of Certain Defence Obligations (hereinafter: Defence Administration Act) then in force, the Central Archives continue to process the data of Army staff – except for staff out of service – after the termination of service or other relationship for the performance of work. Pursuant to Section 13/A(2) of the Defence Administration Act, the data of those out of service are processed by the central human resources body of the Army. The investigation found that the former unit of the data subject forwarded his HR file to the central human resources body of the Army in that year, from which it was not transferred to the Central Archives after the expiry of the period specified by law.

According to the information provided by the Central Archives, the HR file of the data subject was not transferred to the Archives after the termination of his service; however, in relation to this case, they contacted the central human resources body of the Army once again, which informed them that the HR folder of the data subject was still managed by them.

The data subject requested to be transferred to *staff out of service* simultaneously with the termination of his legal relationship. Pursuant to Section 13/A(1) of the Defence Administration Act then in force and Section 51(2) of Act XXI of 2022 on Data Processing for Defence Purposes currently in force, the central human resources body of the Army processes the data of those out of service; accordingly, the folder was lawfully transferred to be processed by the central human resources body after the termination of the legal relationship. As the data subject was no longer on staff out of service, his folder should have been transferred to the Military History Institute and Museum of the Ministry of Defence for further retention; this, however, did not take place according to the information provided by the central human resources body. During the investigation by the Authority, the HR folder was verified to have been transferred to the Central Archives and the data subject was also notified of this. With regard to providing data from the HR folder, or accessing it, the investigation did not find any data breach or any provision of data, which would not have had an appropriately verified purpose.

The Authority called upon the central human resources body of the Army to review its procedures, so as to prevent any future delay in the transfer of personal data to be sent to the Central Archives based on legal regulation. After this,

the head of that body informed the Authority that the staff designated to handle the HR folders were given training on the provisions of Act XXI of 2022 on Data Processing for Defence Purposes. The HR folders were checked and in the future particular attention will be paid to have the HR folders of staff out of service sent to the Central Archives after the period required by law. To prevent delays, electronic records were implemented and two staff members were designated to check due dates. [NAIH-383-9/2023.]

II.2.10. Investigation into processing related to the public area surveillance system of the Town of Kerepes

The Authority ex officio launched an authority procedure for data protection concerning processing related to the public area surveillance system of the Town of Kerepes, which had been preceded by an investigation conducted on the basis of a notification in 2020. The subject matter of the investigation was the lawfulness of the operation of the surveillance system in the area of the Town of Kerepes. The notification related to an act of the Mayor of the Town of Kerepes (hereinafter: Mayor): on 16 June 2020, the Mayor disclosed a public post on Facebook together with a comment, displaying a photo of a resident of the 13th District of Budapest (according to the post), who was disposing garbage in the public area of the town and of his vehicle stating that the police was also informed of the case.

The investigation found that the recordings of the surveillance system were stored not only in a closed network, but the recordings, which require action were also stored on a separate drive, to which not only public area supervisors had access, but also the head of the technical department, the municipal executive as well as the Mayor. According to the statement of the Mayor's Office, the Mayor learned of the place of residence of the data subject "by hearsay".

In its investigative procedure, the Authority found that the disclosure of the recording made public on 16 June 2020 processed by the public area camera system and the posting to the Facebook profile of the Mayor arose from the violation of the rules of data security and data protection. In particular, it arose from the severely injurious practice that "*because of local custom, the Mayor had access to the recording for the purpose of lodging a report with the police up to the recording used by public area supervisors for filing reports through the separate drive accessible with authorisation"*. It was found that the export of the recording was not logged; furthermore, the identification of the number plate of the vehicle in the recording was made by "trial and error" – in a way that was unjustified and

unnecessary for filing the report with the police – from a register that can be used by public area supervisors for purposes other than reporting illegal disposal of garbage. As the export of the recording was not logged, Section 25/E(3) as well as the provisions of Section 25/F(1) and (4) of the Privacy Act were breached.

Later, these findings were supported also by the onsite inspection carried out by the Authority as part of the authority procedure, as there were no logged data related to this recording among the exported log files in the course of the authority procedure. The Mayor's Office – with public area supervision operating as part of one of its organisational units – failed to meet its obligation according to Section 23(2) of the Privacy Act (principle of accountability), since it failed to substantiate compliance of its processing by explaining its procedure with local custom. During the investigation, the Authority called upon the Mayor's Office on several occasions based on Section 56(1) of the Privacy Act. It called upon the Mayor's Office to pay particular attention, inter alia, to the logging procedure and the development of data security measures to prevent unauthorized persons from having access to the data and preventing the processing of personal data in the absence of a lawful purpose when developing the new rules. The Mayor's Office did take certain measures, however it failed to send appropriately revised rules, thus according to the available data, the unlawful conditions continued to apply in relation to the operation of the public area camera system and the use of its recordings.

Then, on 18 August 2022, the Mayor posted a recording of a person, who was masturbating in the Szilasliget train station, captured by a public area surveillance camera, to the facebook.com site. This video was made public together with a video recording of the Mayor's statement made in his official capacity. This fact, i.e. that the Mayor has disposal over the recordings of the public area surveillance camera system also supported the Authority's findings made in the course of the investigative procedure.

In view of this, the Authority closed the investigative procedure and launched an Authority procedure for data protection. To ensure the success of the procedural act without notification in advance, the Authority conducted an onsite investigation at the Mayor's Office of the Town of Kerepes.

During the inspection and in subsequent parts of the procedure, it was found that the video streams of five MÁV-HÉV cameras – which also record sound – were integrated into the camera system (hereinafter: System). The System provided for remote access (Quick Connect). The controller of the System, including the

recordings of the MÁV-HÉV Zrt.'s cameras, was the public area supervision functioning within the organisation of the Mayor's Office. The legal basis of processing is established by the Privacy Act and Act LXIII of 1999 on the Supervision of Public Areas (hereinafter: Public Area Supervision Act). With regard to the MÁV-HÉV camera recordings – irrespective of processing by MÁV-HÉV Zrt. – processing by the public area supervision could be established because they brought decisions of merit with regard to the camera images recorded by MÁV-HÉV Zrt. as it was not disputed that they stored also these recordings in their own system and on the given case viewed them, used them and forwarded them to the Police based on authorisation of the Public Area Supervision Act. Four recording streams were stored outside the closed system on another server of the Mayor's Office. The purpose and reason for processing the records in excess of the lawful retention period could not be established by the subsequent internal investigation of the Mayor's Office. Subsequently, they indicated the purpose of law enforcement as the purpose of processing, while Section 5(1)(a) of the Privacy Act was shown as its legal basis. The municipal executive had no knowledge of the use of the recordings.

The processing of these recordings beyond the retention period specified in the Public Area Supervision Act stored outside the closed camera system without a lawful purpose infringed Section 4(1)-(2) of the Privacy Act, the principle of purpose limitation, as well as the principle of accountability as set forth in Section 23(2) of the Privacy Act.

Facts contrary to the earlier statement were proven, according to which only a narrow group of persons had access to the recordings stored on a separate drive requiring action. The group of people having access to the folder containing the .mp4 files of the public area camera recordings was not restricted to those authorised to have access to the recordings; a wider group of people, beyond the municipal executive and the public area supervisor, was authorised to access the recordings stored on the separate drive. Beyond a single public area supervisor, the municipal executive and the former municipal executive, an additional 10 persons had access. Of these people, access by the Mayor, his assistant, one department head and another person on the staff of the Mayor's Office, who did not work as a public area supervisor during the period under investigation, was doubtless unauthorized. For the other six persons with access, there was no evidence that they had previously been public area supervisors and that their previous access to the recordings was therefore lawful.

Access by this group of persons fails to comply with the regulations set forth in Sections 7(3), 7/A(1) and (2) and 8(1) of the Public Area Supervision Act and through this – in view of the provisions of Section 5(a) of the Public Electronic Information Security Act – it severely violated the provisions of Section 25/I(3)(a), (b) and (c), as well as Section 5(a) of the Public Electronic Information Security Act, which was concomitant with an infringement of the performance of the general tasks of controllers as set forth in Section 25/A(1) of the Privacy Act. Section 25/A(2)(b)(ba) was also breached since the processing of personal data was not limited in terms of type of quantity of personal data to the extent and duration necessary for the purpose of the processing.

The Authority also established that the MÁV-HÉV Zrt. camera recordings also recorded sound, whose processing has no legal basis according to the Public Area Supervision Act for the public area supervision.

As to the lack of data security, the Authority found that the camera systems operator room and the elements of the processing system located there (workstation and server) lacked even the minimum conditions of physical security because at the time of the inspection, the electronic security system was not functioning. The access system logged entries only, not exits. In case of entering with a key, entries and exits were not logged, visitors were not checked or registered. Recordings of public area cameras were stored also on devices, for which connection of external media was not restricted. In this way, all users with access to the folder (whose group was wider than that of those authorised to process the recordings) could also access the recordings stored in this manner for an indeterminate period of time and in ways that could not be checked. The single user name and password for the system was known to the public area supervisor, the assistant supervisor and a former public area supervisor. The system was in operation without the information security officer being aware of its existence. Furthermore, the company responsible for the system administration of the Mayor's Office was not involved in the development of the system, they were not professionally contacted in relation to its development and they were only subsequently confronted with the deployment of the system. The Mayor's Office failed to meet its obligations arising from the Public Electronic Security Act.

The situation exposed with regard to the deficient and inadequate logging of data processing operations continued to exist at the time of the inspection during the authority procedure, and with regard to the processing of the recordings investigated during the procedure, despite the fact that, based on the findings of the investigative procedure, the controller already knew of these deficiencies and

stated during the investigative procedure that the logging of the processing operations related to the camera recordings would be carried out appropriately in the future. Similarly, the controller learned from the findings of the Authority made in the investigative procedure that access by the Mayor to the recordings made by the public area camera system was unlawful. The Authority found no log entries about back-ups, the Authority only learned of them from a hand-written log and the back-up history in the NVR 4.0 user interface. According to the IT expert opinion, there could be several reasons for this:

1. Different logging rules were set for each user, the logging settings assigned to the users under user authorization management and previous recordings were not exported with admin user. This was enabled by the system because access to the Hik-Connect platform needed for remote access to the security camera system was permitted in the settings. During the inspection, the status of the account was “Detached”, nevertheless the system could be accessed remotely at any time provided that the user knew the identifiers needed for connection. In the course of the inspection, the Authority exported the video files through the admin user and it was shown in the log with the appropriate time stamp, i.e. the processing activity of the admin was logged, while the activities of the user were not. The log file shows the back-ups made in the course of the inspection; the fact of the other back-ups can only be seen in the user interface, not in the log file.
2. Automatic back-ups are made of the recordings of the camera system, which are not logged by the system.
3. The log file was manipulated.

Whatever the possible reasons, it can be concluded that the controller failed to meet its legal obligation concerning electronic logging infringing thereby the provisions of Section 25/F(1) and (4) of the Privacy Act. With a view to checking the lawfulness of electronic processing operations, the controller has to record the data in an automated processing system (electronic log), so as to enable the determination of the scope of personal data concerned in the processing operation (in this case, the specific recording or recording stream) the purpose and justification for the processing operation, the exact time and date of the operation, the indication of the person carrying out the processing operation and if the data are transferred, the recipient of the data transferred. The data in the controller’s records and the electronic log have to be retained for ten years following the erasure of the processed data. In the case of all the recordings examined by the Authority, the data providing information in accordance with the provisions of

Section 25/F(1) of the Privacy Act were absent from the electronic logging system.

The rules of data protection and data security specified several data which, according to Section 25/E(1) of the Privacy Act, the controller's records have to contain; however, it did not hold all the data required by the regulation, hence the deficiency of the controller's records was also established. All this infringed the provisions of Section 25/E(1)(j) and (k) of the Privacy Act. The controller's records have to be kept in writing or in electronic format and have to be made available to the Authority [Section 25/E(3) of the Privacy Act]. The Mayor's Office was unable to present controller records containing data concerning the data breaches arising in the context of the public area camera recordings and measures restricting or denying the enforcement of the right of access of data subjects in accordance with this Act, or verifying the reasons for the absence of such information (data breaches have not yet occurred, they have not denied the exercise of data subject's rights). Nor did they have records of authorisations on the users having access to the recordings. Their existence would serve to verify whether a user carrying out a given processing operation according to the electronic log indeed qualifies as a person authorised to have access to these data and the tasks for the performance of which the user was granted access. Keeping records of authorisations would, together with the appropriate log data, enable the verification of the lawfulness of processing whereby it could be established who, for what specific purpose and on what legal basis carried out any given processing operation. The absence of this is also concomitant with an infringement of the principle of accountability [Section 23(2) of the Privacy Act]. According to this principle, the controller has to furnish evidence that the processing of personal data complies with data protection requirements – the burden of proof with respect to this is on the controller or the processor. In the case under investigation, the above provisions are of special significance as, according to the established facts of the case, camera recordings captured by or stored in the system were made available to the person operating the Mayor's Facebook profile, who then shared them. All this infringed Section 25/I(3)(a), (b) and (c) of the Privacy Act. They also failed to account for how these recordings were made public. Non-compliance with the safeguards required by legal regulation (keeping an electronic log and controller records) objectively and specifically thwarted compliance with the principle of accountability and the verification of the specific processing operations.

In view of the fact that a recording originally processed in the system was made public in the Mayor's Facebook.com site, it can be established that they failed to ensure the denial of access to the instruments to be used for processing by un-

authorized person and also failed to meet the controller's obligations concerning the prevention of the unauthorized reading and copying of data media, obviously violating the obligation to prevent the unauthorized access to personal data stored in the system. The appropriate measures were not taken to ensure the lawfulness of the processing in the light of all the circumstances of processing, in particular its purpose, the enforcement of the fundamental rights of data subjects and the risks of processing. The system was designed to serve processing for law enforcement purposes subject to the scope of the Privacy Act, while the controller failed to take the relevant technical and organisational measures [Section 25/A(1) and (2)(a) and b) of the Privacy Act].

The Authority established that there was a data breach with regard to the recording made on 15 August 2023. It is a fact that the recording was made public on the Mayor's Facebook page on 18 August 2023 and it is also a fact that it contained personal data as the aim of disclosure of the recording was to identify the person shown in the recording. Neither the public area supervisor, nor the other witnesses questioned in the course of the procedure were aware of how the recording was leaked. Hence the recording containing personal data got to the Mayor and the person who managed the Facebook page and posted the recording as a result of a data security breach through unauthorized access. The public area supervisor stated that he had heard that the Mayor posted the recording on Facebook, of which he also notified the municipal executive, so at least two persons who could have taken action were aware of the breach within the organisation of the Mayor's Office. Despite having learned of it, the Mayor's Office failed to notify the Authority of the data breach and also failed to take the necessary measures to investigate it, eliminate its reasons and prevent future data breaches. In the course of its procedure, the Authority found unchanged processing practices on the occasion of its inspection almost a month after the data breach. Because of this, the Authority also established the infringement of the controller obligations set forth in Sections 25/J(1) and 25/K(1) of the Privacy Act.
As a result of the its Authority procedure for data protection and based on Section 61(1)(b)(ba) of the Privacy Act, the Authority established the unlawfulness of the mode of processing carried out with the area surveillance camera system on the grounds of the breach of data security and the requirements of accountability, as well as the infringement concerning failure to notify and manage the data breach and decided to levy an administrative fine of HUF 8,000,000. [NAIH-507/2023]

II.2.11. Ex officio supervision

1. National supervision of the Eurodac system

One of the objectives of the Dublin System set up on 15 June 1990 was to prevent individual asylum seekers from lodging asylum applications in more than one Member State. As in the majority of cases, asylum seekers and irregular migrants do not have valid travel documents or other documents suitable for identifying them, fingerprint is an essential element of accurately identifying these persons. This was the reason for setting up the Eurodac system (European Dactylographic Comparison System), which enables countries applying the Dublin Regulation to establish through the comparison of fingerprints stored in the system whether a foreign citizen seeking asylum and illegally staying in one of the Member States of the Dublin area had earlier applied for asylum in another Member State or whether he entered the given area illegally. Based on the comparison of fingerprints, Member States are able to determine the Member State, which is entitled and obliged to conduct the asylum of aliens proceedings against the person concerned.

During the first half of 2023, the Authority conducted an ex officio investigation into processing carried out in the context of implementing the Eurodac Regulation. In the course of its investigation, the Authority examined whether the conditions specified for the lawfulness of processing were met, in particular, the logging of processing operations, the issue of purpose limitation and proportionality of processing, the activities of the designated data protection officer, the performance of tasks related to providing information to data subjects and compliance with the rules concerning retention periods and sensitive data. The supervision was carried out in accordance with the methodology issued by the Commission, based on the answers given by the agency under investigation to the series of questions expanded and edited by the Authority, starting from the questions compiled by the Eurodac SCG and conducting an onsite investigation at the Hungarian Institute for Forensic Sciences (hereinafter: NSZKK) and the National Directorate General for Aliens Policing (hereinafter: OIF). As a result of the investigation, the Authority did not establish unlawfulness concerning processing, however, it put forward recommendations for NSZKK to improve data security.

2. Hungarian Institute for Forensic Sciences (NSZKK)

The Expert Institute for Dactyloscopy (hereinafter: Institute), which is part of the NSZKK organisation, processes fingerprints, hence biometric data. The Institute employs experts and technicians. They forward biometric data (fingerprints) and identification data to NSZKK. The data received in the course of asylum and alien policing procedures are pseudonymised. The *Automatic Fingerprint and Palm Print Identification System* (hereinafter: AFIS) receives biometric data without encryption, but separated from the identifier personal data. AFIS records every intervention and event whether by or without users by logging. NSZKK carries out the processing of palm prints and 10-finger fingerprints. Palm prints have significance in processing for law enforcement purposes, not in queries in Eurodac. In alien policing procedures 100 percent of fingerprint sheets are received digitally, in such cases there are no hard copy queries. Annually, they receive five hard copy queries on average, so their number is infinitesimal relative to the total number of cases. Hard copy fingerprint sheets are stored in their physical form in the NSZKK facility, which is an administrative zone in full and is accordingly equipped with the appropriate physical protection. Only NSZKK communicates with the Eurodac system on behalf of Hungary. The answer to queries sent to Eurodac is either "there is a match / no match". If there is a match, NSZKK's expert has to confirm that it really is a match; in the course of this examination the expert does not see other identification data. As to the methodology of the examination, the various Member States work with different standards in the case of so-called numerical standard. The domestic practice applied by the Institute is the assessment of 10 characteristic points. If a sample does not contain 10 identification points (e.g., in the case of a fragment palm print recorded at a crime scene), the sample is unsuitable for identification. As to data subject's requests, the data protection officer explained that typically they are not submitted to NSZKK. However, it did happen that several detainees submitted requests of erasure and access within a short period of time. In view of the fact that personal data are stored in an anonymised form, these data subject's requests could not be granted and in the absence of authorization, NSZKK is unable to connect biometric data with the identification data. Without the consent of the assigning authority, it would not be possible to grant data subject's requests to exercise their rights because that could for instance impede investigation.

3. National Directorate General for Alien Policing (OIF)

Within OIF, OIF's Directorate for Asylum, the Dublin Coordination Division of the International Cooperation Department and the IT Department perform processing related to the Eurodac system. The Asylum Directorate is an independent organisational unit under the director general, which includes the Department

for Asylum Law and the Department for the Technical Direction of Receiving Institutions. The Department for Asylum Law and the Dublin Coordination Department do not directly send fingerprint and identification data to Eurodac. Data processing is carried out in the asylum procedure (based on the submission of requests for recognition as asylum seekers) and in alien policing procedures; the latter becomes necessary when the asylum seeker is unable to identify himself with documents. The purpose of processing in an asylum procedure is to establish whether the person requesting to be recognised as an asylum seeker has submitted such requests in other EU Member States, too. In the course processing, the 10-finger fingerprint of the person requesting recognition as asylum seeker (not the palm print) is recorded on a fingerprint sheet as well as his identification data, and they are forwarded to AFIS always in a digital format. Only the fingerprints are forwarded to Eurodac marked with an Eurodac identifier. If Eurodac points to a match in its answer, the next step is identification. If a request is received by the Dublin Coordination Division and additional information is requested based on the identification number under the Dublin procedure, the Dublin Coordination Division requests the additional information from the NSZKK Dactyloscopy Expert Institute.

4. Supervision of the domestic use of the SIENA application

SIENA is a secure information exchange network application provided by Europol for international law enforcement information exchange.

Pursuant to *Recital (24) of Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA. 2009/935/JHA, 2009/936/JHA and 2009/968/JHA,* with a view to facilitate information exchange between Member States, Europol, other Union bodies, third countries and international organisations, Europol as service provider provides the secure network for data exchange as a secure information exchange network application.

In itself, SIENA does not provide a legal basis for the disclosure of law enforcement data, it is merely a channel of communication; the exchange of law enforcement data may take place between the cooperating Member States only in the case of an appropriate legal basis. When performing queries, the cooperating Member States act in accordance with their own legal regulations. The SIENA application itself is a structural correspondence system. As national supervisory authority, the Authority carried out an onsite inspection at the head-

quarters of the International Law Enforcement Cooperation Centre (hereinafter: NEBEK) and the Law Enforcement Directorate General of the National Tax and Customs Administration based on Article 42 of the Europol Regulation to review processing operations related to SIENA. On the occasion of the onsite inspection, Authority's staff familiarised themselves with the SIENA work interface and inspected several workstations.

At NEBEK, among the bodies using the SIENA application, there are bodies that have full authorisation to communicate independently with the bodies of other cooperating states in the SIENA system. In addition, the director of NEBEK may grant full authorisation to use the SIENA system. The Department for the Protection of the Economy and the Investigative Department of the Budapest Police Headquarters have full authorisation. There are other bodies authorised to read and produce draft answers, which are then sent to the Europol Hungarian Liaison Office (hereinafter: EMÖI), which will finalise and send the answer. These are the bodies set up to perform general police tasks. NEBEK and EMÖI see every incoming and outgoing query and draft answer. NEBEK is able to monitor messages sent by bodies having full authorisation; it monitors the answers sent at random.

All of the organisational units of NAV (National Tax and Customs Administration) using SIENA have full authorisation, they communicate independently with the agencies of other cooperating states in the SIENA system. Initially, the Law Enforcement Coordination Department – as a professional filter – had full authorisation, and the other organisational units were only authorised to read and produce draft answers. The SIENA system retains data for three years from the last activity carried out in the given case. The data of the SIENA system are stored on the Europol server, Hungarian units do not store data.

II. 2.12. Consultation and cooperation with other agencies

The EES-ETIAS project of the European Commission

As the Authority had reported in earlier years, the EES-ETIAS project coordinated by the European Commission has been in preparation since 2016; relative to the plans its live operation has been slipping for several years. With the adoption of Government Decision 1538/2018 (X. 30.) on the establishment of a working group coordinating the government measures necessary for the development of the European Entry/Exist System (EES) and the European Travel Information and Authorization System (ETIAS), a working group performing tasks of coordi-

nation and supervision was set up for the Hungarian organisations taking an active part in the project, in which the Authority also participates in a consultative capacity. The achievements of the working group include the successful preparation of amendments to some Hungarian legal regulations; however, its main task has been the coordination of government measures and maintaining contact with EU institutions, reporting on the most recent EU level decisions and having Hungarian organisers report with a view to the successful implementation of the project.

The parts of the project are the following:

- Implementation of the 3rd generation of the Schengen Information System (SIS),
- Entry/Exit System – European Union (EES),

The European Entry/Exit System records and stores the time and place of the entry and exit of third country nationals authorised for a short stay (of up to 90 days in any 180-day period) crossing the borders of Member States using EES (the so-called EES file with personal data and biometric identifiers – facial image and fingerprints) and calculates the period of the authorised stay and taking into account the time already spent, generates warnings for the Member States upon the expiry of the period of the permitted stay.

- European Travel Information and Authorization System (ETIAS)

The goal of the ETIAS system is to set up an IT system for allowing the entry of third country nationals not requiring a visa into the Schengen area for a short stay (not exceeding 90 days within a period of 180 days) and checking them prior to their entry. This means that third country nationals not requiring visas will have to register prior to entry to the Schengen border and the system will subject them to a check in advance.

- centralised system (ECRIS-TCN) to identify Member States having information on judgments against third country nationals and stateless persons

The European Criminal Records Information System (ECRIS) has been in operation since April 2012; it is a decentralised system for exchanging information electronically available in criminal records for the central authorities of Member States. ECRIS-TCN will be a centralised system which, based on the uploaded

identification data, will enable Member States to identify the Member State(s) having information on previous convictions, brought in any Member State against third country nationals, so as to enable central authorities to send requests only to the central authorities indicated in the match in ECRIS and not to all the Member States.

– interoperability of EU information systems

The framework set up by the interoperability regulations ensures interoperability between EES, VIS, ETIAS, Eurodac, SIS and ECRIS-TCN.

– renewal of the Visa Information System (VIS),
– renewal of the Eurodac system

According to the plans, these elements would be implemented gradually in a predefined logical order. Implementation is cumbersome, so far only SIS was successfully introduced on 7 March 2023; in the case of other elements, EU legislation is still in progress, which means that it is not known for the time being what its full content will be. All in all, the SIS introduction was successful, even though there was an unplanned IT breakdown (loss of service towards border traffic), however, the situation was successfully managed. The greatest difficulty lies in the fact that all the Member States have to implement individual elements at the same time, which requires tight coordination among the Member States. Hungary is proceeding according to plan with implementation; however, the Justice and Home Office Council of the European Union has already been forced to adopt new schedules for implementation on several occasions leading to multiple modifications of the projects' final dates. The difficulties are illustrated by the fact that in the case of SIS, an existing system had to be updated and not a new one to be set up, yet the implementation of the system was not without problems. Completion of the implementation of the project may be forecast for 2026-2027, which may give rise to problems of financing because of the end of the EU budget cycle.

II.3. Authority procedure for the supervision of classified information

Lawfulness of the classification of national classified data generated in the context of issuing statements by specialised authorities used in alien policing procedures

The Authority received several notifications on checking the lawfulness of the classification of national classified data in the context of national classified data generated in the course of issuing statements by specialised authorities used in alien policing procedures. The notifiers stated that neither the decision of the authority conducting the alien policing procedure, nor the statement of the specialised authority establishing national security risk which was indicated as the reason for rejection contained the facts and circumstances constituting the basis for the specialised authority statements and as such, the basis for rejecting the request, because the specialised authority taking action included the data generated in relation to the national security investigation of the data subject in the course of its procedure preceding the issue of its statement in a classified document.

Albeit the data subject has a right to have access to his personal data of national classification based on an access permit issued by the classifier according to Section 11 of Act CLV of 2009 on the Protection of Classified Data (hereinafter: Classified Data Act), in the cases under investigation the classifier denied the issue of the access permit invoking Section 11(2) of the Classified Data Act. The data subjects underlined that they were unable to exercise their right to effective legal remedy in the alien policing procedure, because they had no knowledge of the reasons for rejecting their request and in their opinion, this procedure violated their right to access their personal data. In their notifications they explained that they believed it to be necessary to examine whether the classifier carried out the necessity-proportionality tests in the classification procedure and whether they brought a reasonable decision on the classification of the data, and whether the classifier considered the other private interests of the data subject, in addition to their right to access personal data, when weighing public interests.

According to the Hungarian legal regulations in force and the current interpretation and application of the law by Hungarian courts, the courts performing judicial review in alien policing procedures or in procedures initiated against decisions rejecting requests for access permits have no legal authorisation to examine the lawfulness of the classification of national classified data used in alien policing procedures, constituting the justification for decisions. An investigation into the lawfulness of classification can be carried out in an authority procedure for the supervision of classification according to the Privacy Act. In view of this, the data subjects lodged notifications with the Authority concerning the lawfulness of the classification of their national classified data constituting the reasons

for the rejecting decision in the alien policing procedure invoking Section 38(2), (3)(a) and (c) and Sections 51/A(1) and 52(1) of the Privacy Act.

Based on Section 38(3)(a) of the Privacy Act, the Authority launched an investigation to establish whether the documents of the file numbers indicated by the notifiers contain classified data and to identify the classifiers.

The Authority found during its investigations that the documents contain national classified data and identified the classifiers. Based on the findings of the investigations, the conditions for launching the authority procedure for the supervision of classification were met, in view of which the Authority concluded the investigations based on Section 55(1)(ac) of the Privacy Act and opened authority procedures for the supervision of classification in accordance with Section 62 of the Privacy Act to check the lawfulness of the classification of the classified data in the documents.

In the course of the classification procedure, the classifier has, inter alia, to balance the public interest in the accessibility of the data to be classified against the public interest in classification. The classified data examined in these authority procedures for the supervision of classification were not data of public interestor data accessible on public interest grounds; they were the personal data of the data subjects. The classifiers carried out the balancing of the public interests in the course of the classification procedures and concluded that the interests underlying the classification of the personal data in the documents outweighed the public interest in the accessibility of the data. In its decisions, the Authority underlined that the balancing of the private interests of the data subjects, their right to access their personal data against the public interest in classification is not part of the classification procedure, and these interests may be taken into account in the procedure for granting the access permit.

In its decisions, concluding the authority procedures for the supervision of classification, the Authority established on the basis of Section 63(1)(c) of the Privacy Act that the classifiers acted in accordance with the legal regulations applicable to the classification of national classified data, when classifying the data included in the documents referred to by the notifiers. Based on Section 62 of the Privacy Act, the Authority informed the notifiers of the conclusion of the authority procedure for the supervision of classified information. [NAIH-3976/2023, NAIH-4799/2023, NAIH-6768/2023, NAIH-6769/2023]

II.4. Reporting data breaches

In the course of the data breach procedures, the trend continued this year that, in most cases, the Authority had to examine the controllers' general data security compliance in parallel with handling of the data breach, because it was only possible through such a comprehensive exploration of the facts of the case to establish whether controllers acted in compliance with the GDPR requirements.

In 2023, 533 new data breaches were notified to the Authority, which shows some decrease relative to previous years (627 in 2022 and 781 in 2020). Of the modes available to controllers to notify data breaches, the data breach notification system dedicated to this purpose and accessible in the Authority's website (https://dbn-online.naih.hu/public/login) has been the most popular one as more than half of the data breaches, altogether 309, were notified using this system. Of the remainder, 176 notifications reached the Authority through the official gateway, 34 were sent by e-mail and 14 by mail.

II.4.1. Major data breaches subject to the General Data Protection Regulation

1. Shifting data security obligations onto the data subject

The Luxemburg Data Protection Authority contacted the Authority because of a complaint related to the processing activities of a company with its registered address in Hungary in a mutual assistance procedure. According to the submission, a Luxemburg national lodged a complaint with the customer service of the controller, in which he requested the reimbursement of the price of the service and his other costs incurred because of this.
The controller requested the complainant to forward the invoices issued on the costs incurred and an official bank statement on the complainant's bank account data in a pdf format by e-mail. The controller requested the complainant to send the pdf document containing the bank data in a password protected compressed file with a view to compliance with the data security requirements of the GDPR and to send the password to the customer service through a separate channel.
The complainant sent the document containing the bank data, but did not meet the request for password protection. In his view, the data security requirements set forth in Article 32 of the GDPR are requirements for the controller to guarantee security, which the controller cannot shift onto the data subject. According to the complainant, the controller should have provided a secure technical environment for the transfer of the data.

With regard to this practice of the controller, the Hungarian Data Protection Authority received complaints also from other data subjects.

In its decision brought in the case, the Authority declared as a matter of principle that the controller infringed Article 25(1)-(2) of the GDPR by creating a processing environment in such a way that it shifted the responsibility for taking data security measures to the data subjects for the management of some of the risks it has assessed. The decision also established that the controller violated Section 32(1)-(2) of the GDPR, which sets forth the obligations for guaranteeing the security of personal data. The reason for this was that the controller failed to take state-of-the-art technical and organisational measures proportionate to the risks involved to receive the data of the data subjects submitting claims for compensation.

Consequently, the Authority levied an administrative fine of HUF 40,000,000 on the controller. In the meantime, the company developed a more secure online platform, as well as a mobile app for receiving customer complaints, so the Authority did not call upon the controller to take additional measures to guarantee data security. [NAIH-109/2023]

2. Breach of data protection rights because of inappropriate erasure

The Authority received a notification in the public interest, which called the attention of the Authority to the fact that through certain links in the website of a district heating provider, several documents (minutes of complaint investigations) containing the personal data of natural person customers (e.g. name and address) were accessible.
The Authority launched an authority investigation concerning the notification in 2020 to examine whether the controller met its obligation set forth in Article 33-34 of the GDPR in managing the data breach because personal data were made public. According to the controller's answer, the accessible documents were uploaded as part of the new website created in 2017; these documents were generated to discharge its public duties and qualified as data of public interest; however because of an administrative failure, they were not appropriately anonymised. The company sent the minutes of the erasure of the data from the website to the Authority. The Authority accepted the information provided and the measures taken by the company in presenting the facts of the case and the management of the data breach and closed the authority investigation on 12 April 2021.

On 11 August 2022, the Authority received a new complaint from the previous notifier in the public interest, in which he called the attention of the Authority to the fact that all of the links previously terminated and the pdf files accessible through them, including the personal data therein, inter alia, the data of the notifier were again accessible through the same routes as before on the website. Because of this and in view of section 60(1) of the Privacy Act, the Authority ex officio launched an authority procedure for data protection against the district heating provider on 24 August 2022.

The answers of the company provided in the authority procedure revealed that although they had earlier removed the links to the mistakenly disclosed reports from the website, they were still accessible on the backup server, they were not erased from there. In other words, only the links to the documents were erased from the website, not the documents themselves. The natural person notifier entered his name in an internet search engine and it brought up the documents in its hit list. The company then repeatedly erased the documents from the website, but this time also from the backup server and contacted the internet search engine provider to remove the data from its hit list.

In its decision, the Authority concluded that data protection risks – in this case the risks of unnecessarily processed personal data can be found on the Internet through the company's website – are only adequately reduced by erasure as a result of which the data themselves are erased or appropriately anonymised in the relevant documents and not only the links to them. Merely removing the links from the website is neither proportionate to the risks, nor appropriate as a data breach management measure. Removing the links themselves is insufficient for guaranteeing data security, they should have been appropriately anonymised or erased from the server supporting the website as search engines could continue to index them and in any case they are accessible to anyone knowing the direct links. The controller only erased the specific documents upon the repeated request of the Authority and upon the launching of the authority procedure.
On these grounds, the Authority's decision of 23 June 2023 established that the company violated Articles 32(1)-(2) and 33(3)(d) of the GDPR and consequently levied an administrative fine of HUF 16,000,000 . [NAIH-6364/2023]

3. Data breach owing to the vulnerability of an obsolete system

A company providing IT services notified a data breach to the Authority. According to the notification, the controller's server accessible from the user (the so-called frontend server) was attacked, in the course of which the attacker exploited the

vulnerability of the content management system on the frontend side. The analysis of the network traffic logs revealed that the attacker generated substantial network traffic; altogether 8,547 items of data were concerned in the data breach. To remedy the data breach, the controller temporarily suspended the related service, it began to remedy the exploited vulnerability and took measures, inter alia, to automatically block network traffic and enforce password change; it also notified the users concerned in a public statement.

In the course of its procedure, the Authority examined compliance by the controller with the requirements related, on the one hand, to data breach management and data security, on the other hand. In relation to the management of the data breach, the Authority found that the controller acted in accordance with the provisions of Articles 33-34 of the General Data Protection Regulation.
As to the requirements concerning data security, the Authority found that the content management system used by the controller was generally in use in 2011-2012 and at the time of the attack, in 2022, this system was considered to be exceedingly obsolete. Furthermore, the Authority established that the controller failed to carry out a version update with regard to the content management system it used, which resulted in a vulnerability, which was exploited by the attackers carrying out an SQL injection-type attack resulting in the data breach.
Based on this, the Authority condemned the controller on the grounds of violating the requirement set forth in Article 32(1)(b) of the General Data Protection Regulation and ordered it to pay an administrative fine of HUF 27,000,000 due to the infringement. The Authority also ordered the controller to update the content management system it uses to the currently accessible, most recent version and if it decides to implement a new content management system it should verify this fact to the Authority. [NAIH-245/2023]

4. Breach of data protection rights due to the absence of appropriate data security measures

The Authority learned of an IT attack and data breach sustained by a company providing IT services based on articles published on various Internet news portals in November 2022 and decided to launch an authority procedure ex officio for data protection.
Based on the facts of the case explored in the course of the procedure, it was found, inter alia, that the attacker had access to the authorisations of one of the staff members of a client whereby the attacker could access the system developed by the client containing the personal data of millions of natural persons. It was not possible to prove in the course of the procedure whether the attacker

specifically accessed the personal data stored in the live system. This was due to the fact that the client applied inadequate data security measures, for instance, logging the IT activities of its staff was inappropriate. As the attacker entered the live system, he did so with valid authorisations, those of the user concerned, and because of the inadequate logging, the activities of the attacker could not be separated from the lawful activities of the holder of the hacked profile.

The Authority also established that although the direct trigger for the incident was an employee error, this could not have resulted in such dire consequences had the data security measures been adequate. After learning of the data breach in November 2022, the client introduced close to twenty measures, including systemic changes, measures that were essential and expected according to the state of the art, although had the trigger of the incident been no more than inattention on the part of an employee, all this would not have been necessary. The Authority held it against the client that the security measures mentioned were implemented only after learning of the data breach, because in the case of a system processing such a large number of personal data, these measures should already have constituted part of the system. Had these measures been part of the client's security system at the time of the attack, it would not have been successful, or could have been detected much earlier. Another decisive element of the facts of the case was that the two-factor authentication to access the live version of the system developed by the client was introduced for the client's staff also only after the data breach. The fact that the data breach constituting the subject matter of this case took place and it was not the client itself that learned of its severity, but became aware of it only through the message of the attacker more than one-and-a-half months after the breach of security was substantial evidence that the client did not appropriately comply with the data security requirements of the GDPR.

In its decision of December 2023, the Authority established that the client failed to meet its obligation set forth in Articles 32(1)(b), (2) and 33(2) of the GDPR. Based on this, it ordered the client to inform data subjects of the findings of the decision within thirty days from receipt of the decision and levied an administrative fine of one hundred and ten million forints because of the infringements. In January 2023, the client lodged an appeal against the decision, the court review of the case is still in progress. [NAIH-1245/2023]

II.4.2. Data breaches subject to the Privacy Act

Inadequate management of a data breach concerning health-related personal data

Based on a notification, the Authority launched an investigation against a penitentiary institution (hereinafter: controller) concerning the assumed unlawfulness of the processing of the notifier's health-related personal data. The processing of health-related personal data records of detainees by penitentiary institutions is processing for law enforcement purposes, to which the provisions of the Privacy Act shall apply.

The notifier submitted a request to the controller for issuing his health documentation, i.e. to enforce his right to access; the controller denied the request stating that the requested health-related personal data were not available.

Pursuant to Section 79 of Act CCXL of 2013 on the Execution of Penalties, Measures, Certain Coercive Measures and Detainment for Misdemeanours (hereinafter: Penalties Execution Act) and Section 32(1) of Act CVII of 1995 on the Penitentiary Organisation (hereinafter: Penitentiary Act), the penitentiary institution has to retain the health-related personal data of detainees for twenty-five years from the execution of the penalty or measure, or the end of enforceability. The execution of the penalty of the notifier was in progress at the time of the notification, the retention period of the documents containing his health-related personal data requested had not yet expired, so the controller had to process and store the health-related personal data of the notifier requested as part of the exercise of his right to access based on the legal regulations referred to.
Nevertheless, the hard copy documents containing the health-related data of the notifier could not be found in the controller's records and the electronically recorded health-related data were not accessible for a certain period (in the period between 17 December 2022 and April 2023), i.e. the notifier's health-related personal data requested as part of the exercise of his right to access were not available to the controller.

Based on above, the Authority established the violation of data security, which resulted in the loss of the personal data stored in the hard copy records and the temporary inaccessibility of the notifier's health-related personal data recorded electronically, which thus constituted a data breach.

Pursuant to Section 25/J(1) of the Privacy Act, in the event of a data breach, the controller has to record the nature of the data breach including, where possible, the scope and approximate number of data subjects and the scope and approximate number of personal data records affected, the likely consequences of the data breach, and the measures taken or proposed to be taken by the controller to address the data breach including, where appropriate, measures to mitigate the possible adverse effects resulting from the data breach. If the data breach poses a risk to the enforcement of data subject's rights, the controller has to notify the data breach to the Authority without delay but not exceeding seventy-two hours after having become aware of it.

Based on the available information, the Authority established that the data breach qualified as risky because it resulted in the violation of the notifier's data subject right as he was unable to exercise his right to access for months because the health-related personal data requested, which qualify as special category personal data, were not available to the controller because of loss and temporary inaccessibility and the controller learned of the data breach only in relation to the rejection of the notifier's request or complaint. The controller informed the notifier that the health-related personal data requested could not be found among the hard copy records and the requested personal data could not be accessed in the electronic records because of a software error; the notifier was also informed of having written to the developer of the software.

The controller failed to inform the Authority of the data breach; the Authority became aware of the breach only in the course of the investigative procedure. Because of the failure to meet the notification obligation, the data and information related to the data breach as set forth in Article 25/J(5) of the Privacy Act were only partially known to the Authority.

The Authority assessed the fact that the controller contacted the software developer to ensure access to health-related personal data stored in the electronic records as a measure taken to remedy the data breach. In the meantime, the IT developer successfully retrieved the health-related personal data of the notifier stored in the electronic records, i.e. the data breach was partially remedied. As a result, the controller was able to grant the notifier's request to exercise his right to access.

Based on the controller's answer to the Authority, it was not possible to determine whether the controller recorded the data according to Section 25/J(5)(a), (c) and d) of the Privacy Act (how many persons and roughly what quantity of

data were affected by the breach) what was the controller's risk assessment of the breach, whether it investigated the reasons for and circumstance of the data breach, whether it provided the information in accordance with Section 25/K(3) of the Privacy Act and whether any other measures were taken to remedy the data breach in addition to contacting the software developer.

The Authority established that an infringement related to the processing of personal data occurred because the controller failed to act in accordance with the requirements set forth in Sections 25/J-25/K of the Privacy Act in notifying and managing the data breach. Based on Section 56(1) of the Privacy Act, the Authority called upon the controller to immediately meet its obligation of notification according to Section 25/J(1) of the Privacy Act with regard to the data breach and to act in accordance with the requirements of Sections 25/J-25/K of the Privacy Act in notifying and managing eventual future data breaches. [NAIH-3957/2023]

II.5. Data protection licensing and preliminary consultation procedures

II.5.1. Data protection licensing procedures

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

Pursuant to Article 43 of the GDPR, without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, certificates are issued and renewed by certification bodies having an appropriate level of expertise in data protection. Of the options offered by the GDPR in Article 43(1), the Hungarian solution implements point (b), i.e. accreditations are carried out in accordance with EN-ISO/IEC 17065/2012 and Regulation (EC) No. 765/2008 of the European Parliament and of the Council and by the National Accreditation Authority (NAH) in accordance with the supplementary requirements established

by the Authority, and the Authority acts as specialised authority in the course of such procedures. The document containing the supplementary requirements is accessible both in English and Hungarian on the website of the Authority.[4]

In 2023, there was one occasion in which a preliminary specialised authority statement was issued on the basis of the above in a procedure launched upon the application submitted by TAM CERT Magyarország Kft.

In this context, it should be noted that, after the relevant amendments, Decree 45/2015. (XII. 30.) NGM now contains the administrative service fee payable for the Authority's procedure as specialised authority, which is
a) HUF 192,000 in the accreditation procedure of the data protection certification body,
b) HUF 192,000 in the procedure to expand the area of its accredited status,
c) HUF 76,800 in the supervisory investigative procedure launched upon its request.

II.5.2. Impact assessment preliminary consultation procedure for applying body cameras in the course of loading luggage at an airport

According to data processing proposed by Budapest Airport Zrt., it would require employees of ground handling organisations performing loading and unloading activities to wear body cameras in the course of their luggage and cargo handling work processes. The reason for this is that in recent years, loaders violated the law through the unlawful opening of luggage in the area of the Budapest Ferenc Liszt International Airport in numerous cases. In addition to high value assets that may potentially be stolen, arms and ammunition, martial arts instruments, other dangerous equipment, objects and materials carried with permission were also affected by the pilferage of luggage. The number of such luggage can reach thousands per day in peak periods (such as the summer season). In the event of the illegal opening of luggage, loaders have uncontrolled access to these objects, they can take them at any time, they may transfer them to unauthorized persons, whereby their cleared, so-called "sterile" status is lost. Body cameras used during loading operations therefore monitor and make safer an area, which had hitherto been outside the scope of monitoring controls.

4 https://www.naih.hu/adatkezelokent-fordulok-a-hatosaghoz/magatartasi-kodex-ellenorzo-szervezet-engedelyezese

Experience and the statistics of reports attached to the impact assessment document showed that employees who underwent different background checks commit abuses in high security areas and critical parts in the course of loading and handling luggage. Budapest Airport Zrt. regards the use of body cameras as the most efficient solution to reduce risks to air transport security and flight safety. The purpose of processing is to reduce the risks to air transport security and flight safety, to minimise the risks of unauthorized access to incoming and outgoing luggage and cargo in aircraft holds, and to comply with international and domestic legal regulations.

Budapest Airport Zrt. compiled a data protection impact assessment document on the implementation of processing with body cameras based on Article 35 of the GDPR, in which it assessed the emerging data protection risk factors. Upon the request of Budapest Airport Zrt., the Authority launched a preliminary consultation procedure in accordance with Article 36 of the GDPR concerning the risk assessment of the proposed processing.

Based on the impact assessment, body cameras proved to be the most secure and most reliable solution in contrast to other state-of-the-art means under study that do not jeopardise flight safety (mobile camera, fixed cameras located in the loading area) when selecting the means resulting in data processing. The entire airport is covered by cameras (CCTV camera system), their use is established practice in all of the airports of the Member States of European Union, they are necessary elements of the security system. However, this system does not cover (is unable to oversee) the loading areas of planes where unauthorised luggage opening takes place. The areas in question (the cargo bays of aircrafts) cannot be monitored through fix cameras installed as the structure of the aircraft may be compromised when mounting them, which means a critical security risk. The technical and maintenance experts consulted on retrofitting of “fixed” cameras, even temporarily, on aircraft pointed out the risk that on the one hand there is no fitting method that would be suitable for all types of aircraft (including different weather conditions); furthermore, when mounting the cameras on or close to the aircrafts’ door, or when it is done quickly, carelessly or forcefully, damage may be caused, which could lead to the delay or even cancellation of the flight.

The ground handling organisations expressed a concern about the use of body cameras in that personality rights may be violated, if the loading staff equipped with cameras make recordings of the members of the travelling public. Budapest Airport Zrt. endeavours to minimise this risk factor by disallowing the loading or handling staff to have access to the recordings. The recordings may be down-

loaded and stored only on a dedicated computer, which has special software installed developed for this purpose to read the recordings, which also requires knowledge of the technical key known to the administrator. When exporting the recordings from the computer, there is an option to process the exported recordings through a face blurring system, which practically blurs every face in the recordings so as to be unidentifiable. In addition, the risk analysis addressed and mitigated the risks of constant surveillance and psychological influence on the loading staff through data protection awareness, providing information and defining the period of retention within the shortest necessary timeframe (limitation to the process of loading).

The Authority fully reviewed the impact assessment documentation submitted by Budapest Airport Zrt. and the ground handling organisations and did not identify unacceptably high residual risks from the viewpoint of the data subject's rights and freedoms in relation to the proposed measures. In view of the above, the Authority did not make additional recommendations or orders in the course of the preliminary consultation procedure and closed it. [NAIH-3773/2023]

It should be noted that as of 1 January 2024, Section 67/B of Act XCVII of 1995 on Air Transportation made the use of body cameras mandatory for the ground handling organisations while loading cargo and luggage.

III. Freedom of information

Based on the provisions of Section 71/D(8) of the Privacy Act entering into force on 1 January 2024, the Authority "annually produces a report as part of its account specified under Section 38(4)(b)" on its monitoring activity regulated in Chapter VI/B of the Privacy Act. In view of the fact that this monitoring activity is closely related to the Authority's functions and powers related to monitoring and facilitating the enforcement of the right to access data of public interest and data accessible on public interest grounds – some of its elements are inseparably overlapping – the Authority publishes this entire chapter of its annual report as the report required by Section 71/D(8) of the Privacy Act and commends it to the attention of the Reader.

2023 was the year that could be described as a "*historical milestone*" in the history of the freedom of information in Hungary because it was on 28 February this year that NAIH was authorised to monitory and rectify the performance of special disclosure obligations newly defined in the Privacy Act with regard to disclosure on the Internet in authority procedures for transparency as the Hungarian supervisory organ designated to monitor and facilitate the enforcement of the right to access data of public interest and data accessible on public interest grounds,. This new legal institution requires a new approach from the obligees, as well as from the Authority, which is fundamentally different from that hitherto applied; in addition, it has or may have a positive impact on proactive freedom of information, on the practice of electronic disclosure, as well as on ensuring the accessibility of data of public interest as it directs attention to the requirement and consequences of the even more perfect and more accurate enforcement of the fundamental right.

A substantial increase was observed in all the types of cases, notifications and complaints, affecting the freedom of information, received by the Authority (complaint, consultation, the so-called "borderline" authority procedures for data protection) relative to 2022. Interestingly, some 450 litigations for data requests were launched at the courts of first instance in 2023, the Authority conducted 660 investigations concerning the freedom of information in the same period.

There has been a newly evolving trend since the termination of the cost reimbursement that could be charged on the grounds of the disproportionate use of labour resources: the organs performing public duties concerned by the data re-

quests increasingly refer to the circumstance among the reasons for rejection that they do not process the requested data in the requested format, and they are not obliged to generate them or they do not qualify as controllers. However, for some reason, they do not tell the person requesting the data about the reason for the latter case or whether data have been generated and, if so, from whom they can be requested. Several submissions addressed the mode of meeting the data requests, the operation of the HIKAP/KIKAP portal, the accessibility of the data, their downloading, the use of the opportunity for access exclusively in person, the prevention of making notes or copies, the problems related to the machine readability of the data sent and the use of a digital "*watermark*" on the data issued referring to the person requesting the data.

Parliament adopted a new paragraph of Section 30 of the Privacy Act at its session of 13 December 2023, which provided for new reasons for rejection for the organs performing public duties, so as of 1 January 2024, the organ is not obliged to issue the requested data of public interest or data accessible on public interest grounds, if it does not actually process the data or it would necessitate the procuring or collecting data that are processed by an organ performing public duties under the direction or supervision of the former. A request may also be denied, if its fulfilment would necessitate the production of new data relative to the data actually held by the body, by comparing the data of public interest or data accessible on public interest grounds. The use of these reasons for rejection is not mandatory and they may not be applied to data requests in progress.

The legislator added a new Section 3/A to *Act CXXII of 2009 on the More Economical Operation of Publicly Owned Companies* resulting in the restriction of the accessibility of data for reasons of public interest. In the case of foreign investments, if access to

- financial,
- technical and
- business data

in documents related to contracts concluded, the underlying decision support, the conclusion, modification or termination of contracts, or in documents concerning the future development, modification or termination of foreign policy or the external economic relations, or in documents generated for the preparation of relevant decisions would jeopardise the pursuit of Hungary's foreign policy or external economic interests free of undue external influence, or its national secu-

rity interests, compliance with the request to grant access to the data as data of public interest or data accessible on public interest grounds has to be denied as long as the public interest quoted as the basis for denying the request prevails, but at most for 10 years from the date of their generation or the date of signature. This restriction extends to similar data in contracts and documents concluded on the basis of international contracts processed by a business organisation in public ownership. The minister exercising ownership rights of the business organisation or supervising it decides on the accessibility of data based on an opinion developed by balancing the public interest in accessing the data and the public interest in the denial (cogent public interest test), which has to be issued at the latest within fifteen days. The period from requesting the opinion until it is issued or the unsuccessful expiry of the period open for providing the opinion is not included in the period available for complying with the request to access the data.

III.1. Data provided by organs performing public duties and statistical data from the Authority's monitoring freedom of information in 2023

III.1.1. Reporting by organs performing public duties

Hungary Recovery and Resilience Plan C9.R26. In order to implement the reform entitled Improvement of transparency and access to information of public interest (milestones 229 – 233), it is necessary to draft reports on six-month periods for the second half of 2022 and thereafter each year until the first half of 2026.

To meet this commitment, *Act CI of 2023 on the system of the utilisation of the national data assets and certain services* added a new chapter VI/B. [Section 71/D.] to the Privacy Act, which gave new functions and powers to the Authority (hereinafter: monitoring freedom of information) and linked to this it specified a reporting obligation for organs performing public duties that was expanded relative to the previous requirements set forth in Section 30(3) of the Privacy Act.

Based on the provisions of the law, organs performing public duties, specifically including municipalities and business organisations in public ownership, have to provide data on the preceding years from 2024 by 31 January of each year

a) on the number of granting and rejecting requests to access data of public interest and data accessible on public interest grounds and the characteristic reasons of rejection,
b) the average number of days needed to grant the request to access data of public interest and data accessible on public interest grounds, and
c) the accurate internet accessibility to the location where data of public interest and data accessible on public interest grounds are published.

Pursuant to Section 30(3) of the Privacy Act, organs performing public duties have to keep records on the requests refused and the reasons for refusing them from then on as before.

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

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

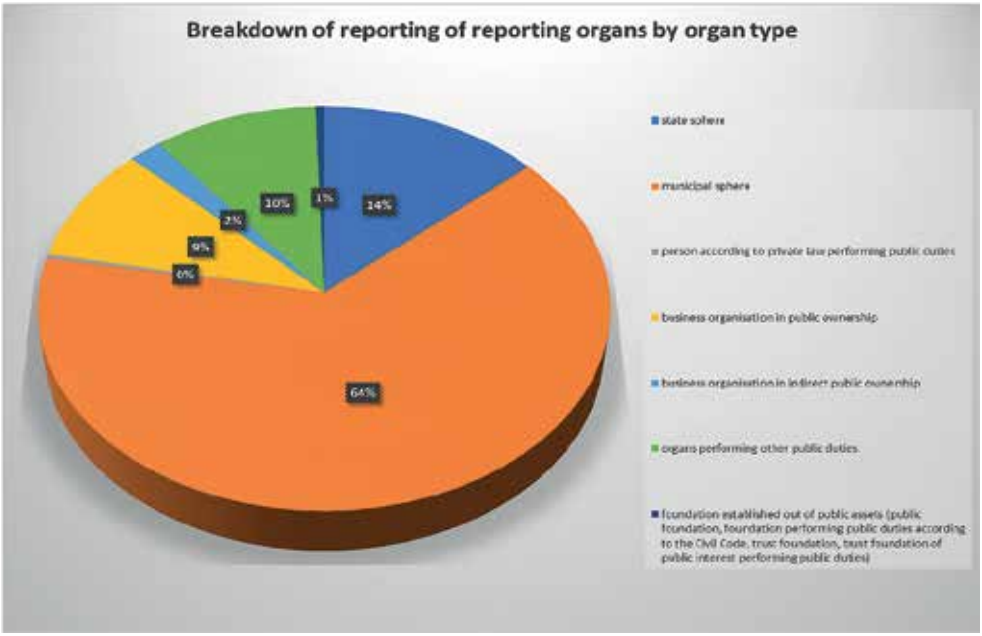
In the rather short period available for preparation between the promulgation of the regulation (22 December 2023) and its entry into force (1 January 2024), the Authority took every measure to apply the regulation efficiently and smoothly.

As part of this, the Authority published a smart data sheet for meeting the reporting obligation through the link at https://naih.hu/adatlap-eves-jelenteshez. In order to inform the largest possible number of organs performing public duties of the reporting obligation, extended relative to the previous requirement, which entered into force on 1 January 2024 and was to be complied with by 31 January 2024, the Authority took action to publish the bulletin in the Hivatalos Értesítő (Official Gazette) and initiated the provision of information to local governments through the Ministry of Public Administration and Rural Development.

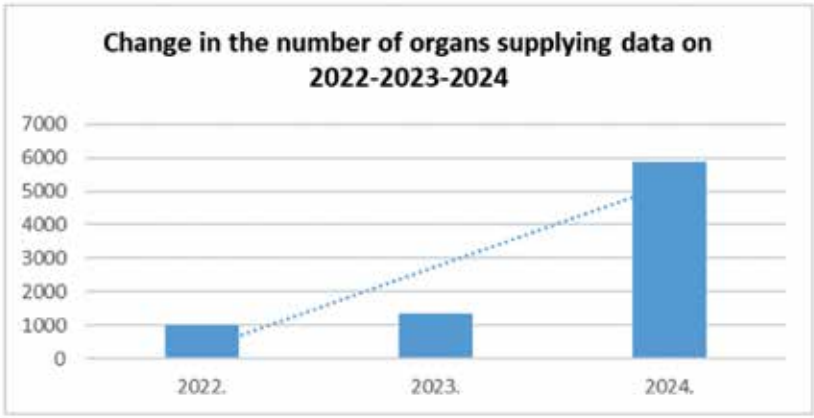
Following the preparations, the Authority received reports from **altogether 5,895** organs. The reporting obligation applies to the following organ types:

- state-owned business organisation, state public authority, state public institution, budgetary organ according to the Act on Public Finances, legal entity according to the register of the State Treasury, public body (state sphere);
- local government, body of representatives and its organs, budgetary organs founded and supervised by the local government, minority governments and their organs (municipal sphere);
- person according to private law performing public duties;
- non-profit business organisation in public ownership, state-owned business organisation performing public duties specified in legal regulation, state-owned business organisation or municipal business organisation operating with a share in state ownership to be kept among national assets of outstanding significance for the national economy (business organisation in public ownership);
- foundation established out of public assets (public foundation, foundation performing public duties according to the Civil Code, trust foundation, trust foundation of public interest performing public duties);
- business organisation in indirect public ownership; and
- other organisations performing public duties: water management and forestry management associations, sport unions, higher education, organisation for copyright protection, other organisation performing public duties in the area of the administration of justice (organs performing other public duties).

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



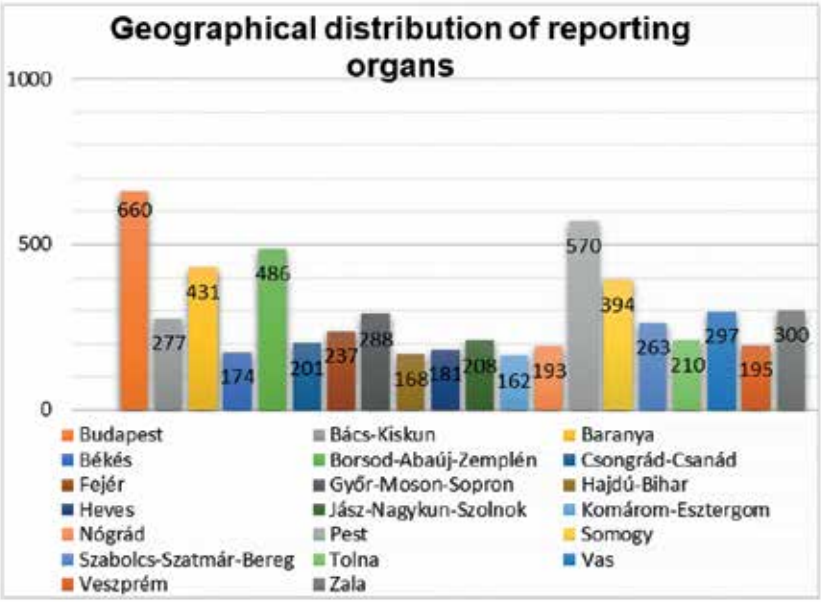
Looking back to preceding years, there was a major increase in terms of the reporting obligation to be complied with in 2023 relative to 2021 and 2022 because of the change in the legal regulation described above as reports were received from 997 organs in 2022 and 1,350 in 2023.



Local governments and minority governments as well as their organs in the municipal sphere had the largest cardinality.

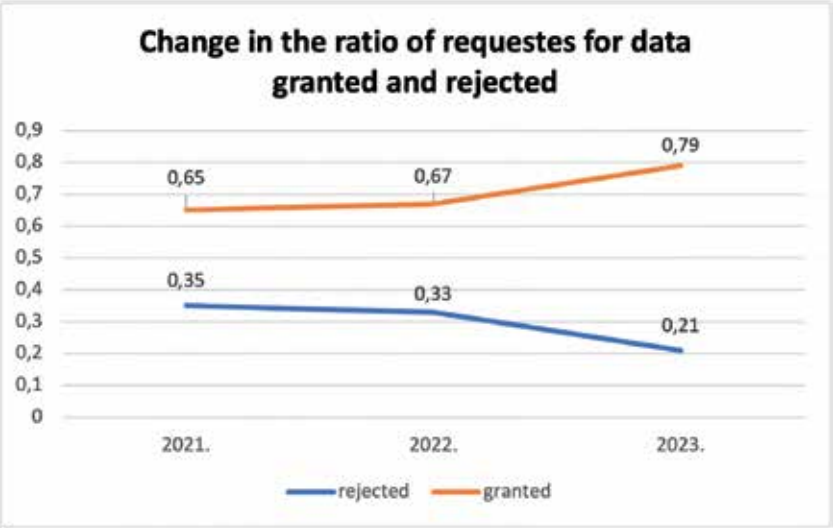
Besides the 432 local governments and their organs, 15 minority governments submitted reports on 2021; 584 local governments and their organs and 25 minority governments submitted reports on 2022. Reports on 2023 were submitted by 2,612 local governments and their organs, 870 budgetary organs founded and supervised by local governments and 301 minority governments and their organs totalling: **3,783 municipal organs**.

Based on the regional distribution of reporting organs, Budapest submitted the largest number of reports (660), followed by Pest County (570), with Komárom-Esztergom County coming last (162).

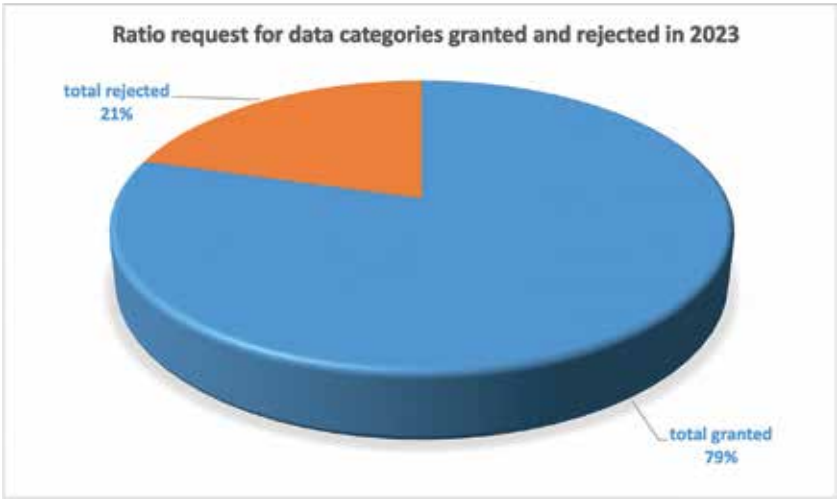


Similarly to the increase in the number of reporting organs, the ratio of requests for data of public interest granted and rejected showed a positive change relative to the data of the preceding years.

- In 2022, in the reports on 2021, 3.881 (**35%**) requests for data of public interest were rejected out of a total of 11,019;
- In 2023, with regard to 2022, 3,260 (**33%**) out of 9,739 data requests were closed with the restriction or exclusion of access to data of public interest.
- In 2024, in the reports on 2023, the controller organ performing public duties declined to grant access to data of public interest in 6,210 cases (**21 %**) of the 14,840 data requests involving 30,238 data types.



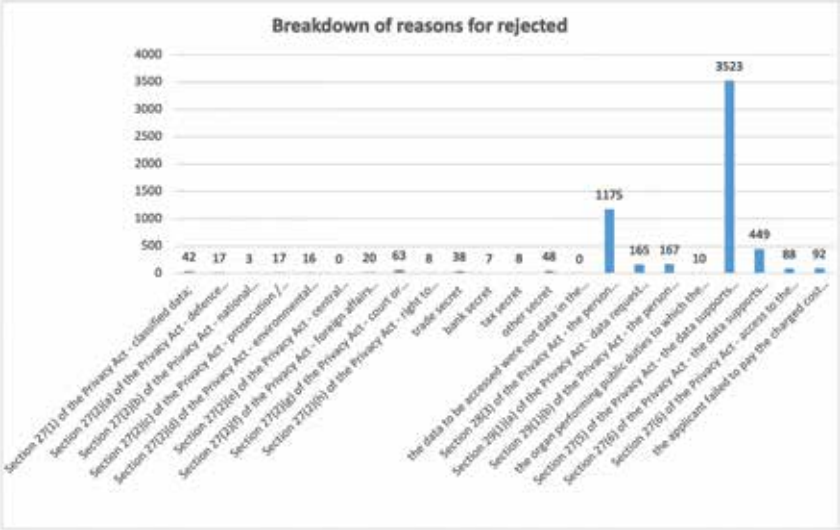
The expansion of the content of the reporting, which entered into force on 1 January 2024 showing the number of data requests submitted in the given year and the average number of days spent on meeting the data request, shows a more detailed picture of the practice of organs performing public duties regarding the assessment of data requests.



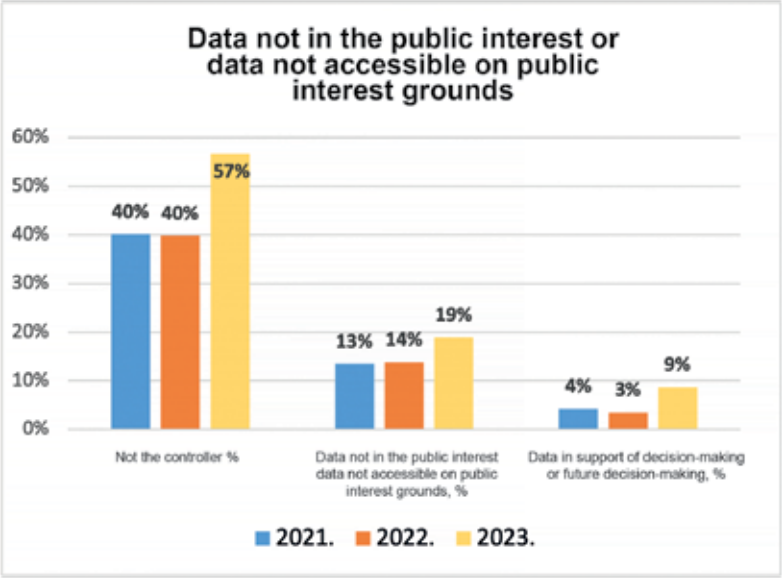
The reasons given by the organs performing public duties for excluding access to data were the following:

- Section 27(1) of the Privacy Act - classified data;
- Section 27(2)(a) of the Privacy Act - defence interest;
- Section 27(2)(b) of the Privacy Act - national security interest;
- Section 27(2)(c) of the Privacy Act - prosecution / prevention of criminal acts;
- Section 27(2)(d) of the Privacy Act - environmental or nature conservation interest;
- Section 27(2)(e) of the Privacy Act - central financial / foreign exchange policy interest;
- Section 27(2)(f) of the Privacy Act - foreign affairs interest;
- Section 27(2)(g) of the Privacy Act - court or administrative authority procedure in progress;
- Section 27(2)(h) of the Privacy Act - right to intellectual property;
- trade secret
- bank secret
- tax secret
- other secret
- the data to be accessed were not data in the public interest, or data accessible on public interest grounds,
- Section 28(3) of the Privacy Act - the person requesting the data failed to clarify the identity of the controller;
- Section 29(1)(a) of the Privacy Act - data request was for the same type of data repeated within a year;
- Section 29(1)(b) of the Privacy Act - the person requesting the data fails to give his/its name and contact data;
- the organ performing public duties to which the data request was submitted does not process the data to be accessed;
- Section 27(5) of the Privacy Act - the data supports decision-making;
- Section 27(6) of the Privacy Act - the data supports additional future decision-making,
- Section 27(6) of the Privacy Act - access to the data would jeopardise the lawful functioning of the organ performing public duties, or the performance of its functions and powers without undue external influence, such as, in particular, the free expression of its views while generating the data during the preparatory stage of decision-making;
- the applicant failed to pay the charged cost reimbursement.

A case when the person requesting the data withdraws the data request does not qualify as a reason for rejection, but, as part of the practice to issue data, it was included in the reports. As the reports address the practice of a year, in the case of requests for data of public interest submitted in the last days, it may occur that the controller lawfully extends the period open for compliance by an additional 15 days, so it may occur that the submitted data request is not answered by the time the report is completed (submitted but not assessed data request).

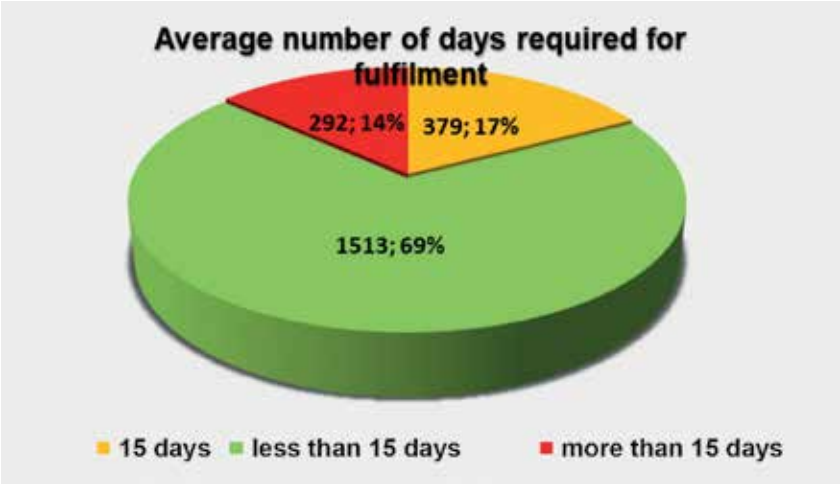


The reasons for rejection most frequently quoted in the previous years (2021, 2022) were also quoted in the first place in the 2023 reports. In terms of the use of reasons for rejection, one item differed substantially (17%) from the practice in preceding years: data not processed by the organ to which the data request was submitted.



The amendment of the law, which entered into force on 1 January 2024, added further information on the data related to fulfilling data requests to the content of the data provided. Such additional information includes the average number of days needed to answer data requests. A substantial number, i.e. 3,711 (63 %) of the reporting organs submitted a “zero” statement, in other words, they did not receive requests for data of public interest in 2023, hence the time spent on answering them was also zero.

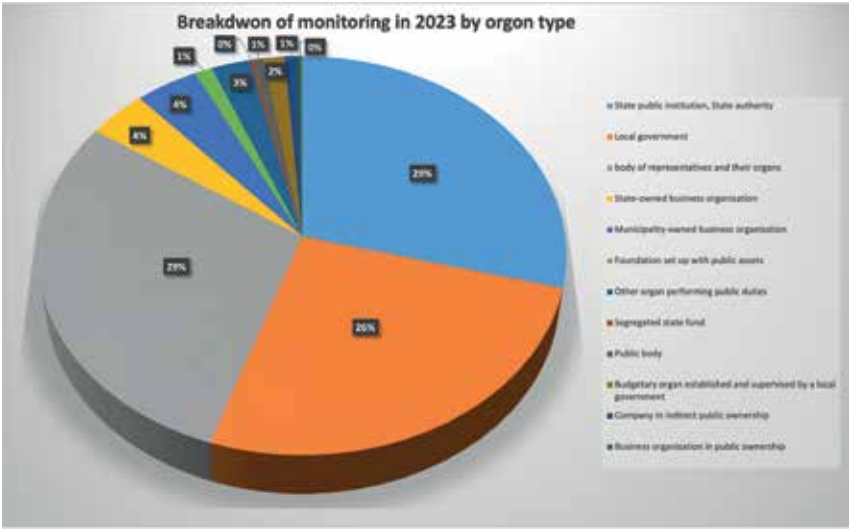
Of the organs (2,184) which received requests for accessing data of public interest, 69% (1,513) answered the request in less than 15 days; for 17% (379) this period was 15 days, and for 13 % (292) this period exceeded 15 days.



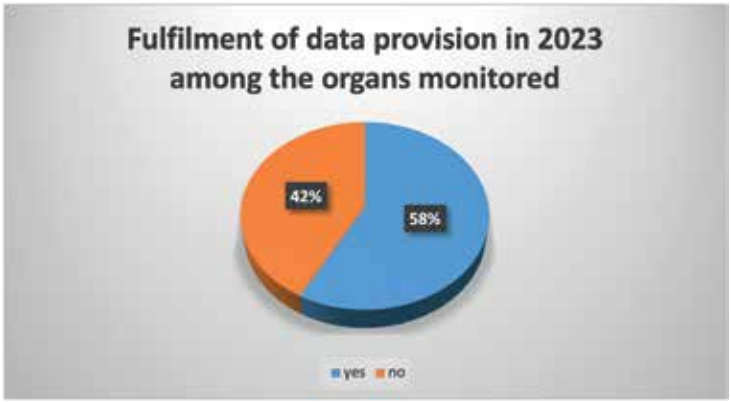
III.1.2. Statistical data of the Authority's freedom of information monitoring activities in 2023

In 2023, the Authority launched 509 cases for freedom of information monitoring to enforce the fundamental right to access data of public interest. The complaints in 96% (483) of the notifications concerned access to data of public interest by way of data requests, while 4% (20) complained against the electronic publication practice of certain organs performing public duties.

The monitoring covered the data access and data issue practices of altogether 426 organs performing public duties, of which the three outstanding groups of organs were state public institutions (124, 29%), local governments, bodies of representative and their organs (125, 29%) and state authorities (111, 26%).

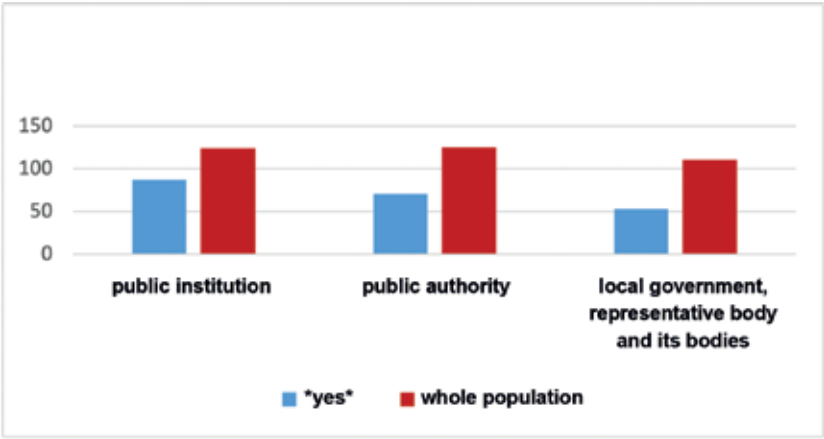


Of the monitored organs, 58% complied with and 42% failed to comply with their reporting obligation according Section 71/D(4) of the Privacy Act.



In the case of the three organ groups of large numbers concerned in the monitoring:

- 87 (70%) of the state public institutions (124)
- 53 (48%),of the local governments, bodies of representatives and their organs (125) and
- 71 (57%) of the state authorities (111) complied with the reporting obligation set forth in Section 75/D(4) of the Privacy Act.



Of the cases of freedom of information monitoring launched in 2023, the Authority issued calls in accordance with Section 56(1) of the Privacy Act in 140 instances, which had to be repeated in 30 cases. In 12 cases, the Authority issued reports according to Section 59 of the Privacy Act and made three recommendations to controllers and the supervisory body of the controllers based on Section 56(3) of the Privacy Act.

III.2. The Central Information Register of Public Data and the authority procedure for transparency of the Authority

Based on Section 37/C of the Privacy Act in force as of 29 November 2022, budgetary organs have to publish some of their financial data in the Central Information Register of Public Data (hereinafter: Platform). As from 1 March 2023, the Authority monitors compliance with this obligation in its authority procedures for transparency based on Sections 63/A and 63/B of the Privacy Act. In view of the fact that the deficiencies of the operation of the Platform and of regular reporting by the organs may jeopardise the payment of EU funds, the

Authority pays particular attention to monitoring compliance with this new obligation and the elimination of infringements.

By 6 February 2024, 1,836 budgetary organs submitted 7,268 reports to the Platform, of which 5,930 reports were made on completed data sheets free of formal errors. The Transparency Authority Division of the Authority in operation from 1 March 2023 monitored 740 organs and launched 109 procedures by 28 June 2023. During the period from 29 June 2023 to 28 December, an additional 312 organs were monitored and 75 authority procedures for transparency were launched. Of the 160 decisions made in authority procedures for transparency, the Authority established infringements in 145 decisions, of these it ordered the budgetary organ to improve or supplement its report in 25 decisions. Fines had to be levied in no more than 4 procedures. The Authority did not levy fines according to substantive law, because the budgetary organ terminated the infringements in every procedure and in 120 procedures not even an order was needed.

Orders were related to the termination of minor deficiencies; the organs added the greater part of the data concerning missing contracts even without an order. The remaining deficiencies arose from the fact that subsequent performance was not in line with the provisions of the Guidelines[5] produced by NAVÜ or was technically erroneous. In these procedures, the clients did not respond to the questions posed in the Authority's orders. Finally, it was not necessary to levy fines according to substantive law even in these procedures as the clients terminated the infringements prior to bringing the decision.

Prior to the due date for submitting the first report, the Authority called the attention of the budgetary organs to the new obligation in several statements. In spite of this, in many cases they failed to submit the reports, because the organs were not aware of the new obligation. Surprisingly, this occurred in the case of a major university [NAIH-6341/2023], and significant central budgetary organs [NAIH-9470/2024, NAIH-4798-13/2023, NAIH-5084/2023, NAIH-6346/2023,].

The majority of hospitals also failed to produce their reports by May 2023 [NAIH-5367/2023, NAIH-5365/2024, NAIH-5366/2024, 5297/2023, 5438/2023], so the Authority requested information from the National Directorate General for Hospitals and published a notice calling the attention of the hospitals to the obligation. As a result, numerous hospitals complied with the reporting obligations on 15 May 2023.

5 Guidelines for Filling in the Data Sheet, https://kif.gov.hu/adatszolgaltatasok/adatszolgaltatoknak

As reasons for their failure to submit the reports or their deficiencies, the organs mentioned administrative errors, lack of human resources or the departure of adept staff members most of the time. It is a frequent problem that although the contract missing from the Platform has already been concluded, it is not entered in the organ's register for a long time, so the data are not provided within the time limit, in violation of the law. In the cases of several organs, there was not only one deficiency that led to the infringement. For instance, a budgetary organ received a letter informing them of the new obligation to publish, but because of data deficiencies in-house and the personal failures causing this, they failed to upload the data. Later, a storage enlargement had to be carried out in the filing system, but they failed to migrate the required contract data from the system into an Excel table and so, they again failed to upload the data. Later, changes in management, changes in personnel concerning hand-over-take-over procedures and the anomalies arising from them led to the subsequent failure to upload. In part, the reason for the anomalies included the lack of clarification of responsibilities, their overlaps and the transformation of the internal information system. Following the authority procedure for transparency, the organ applied the consequences related to personal failure. [NAIH-8974/2023]

The lack or deficiency of performance was frequently due to a misinterpretation of the law. Several organs arrived at the erroneous conclusion that they had to provide data only with respect to contracts in force, or only after the performance of the contract. It follows from the text of Section 37/C of the Privacy Act that the coming into being of a contract already generates an obligation to provide data, the Privacy Act does not link this obligation to the entry into force of the contract. The legislator's intention was to publish the contracts that were concluded and this was not subject to the condition of the contracts being in force. [NAIH-7042-8/2023, NAIH-7253/2023]

The actual movement of funds is also not a condition of the reporting obligation. According to the position of an organ acting as a central purchasing authority, the contract in question was not subject to the scope of the obligation to provide data as set forth in Section 37/C of the Privacy Act, because it was a framework agreement. The client conducted the procedure to conclude the framework agreement not for its own purpose and not to debit its own funds, but acting as a central purchasing body. In its decision, the Authority expounded that in view of Section 37/C(2)(b), (3)(b) and (4) of the Privacy Act, the obligation to publish on the Platform applies to contracts exceeding a net value of five million forints, and the regulation does not include any provision that only the data of the con-

tracts have to be published on the Platform in relation to which actual movement of funds takes place. According to the Authority's position, central purchasing bodies are subject to the reporting obligation even though the eventual future payments based on the framework agreements would not take place to debit the client's budgetary funds. In this case, the client has such wide-ranging authorisations in the course of the "Individual Procedures" to be conducted on the basis of the framework agreement, which substantially influence the elbowroom of the organisations concluding the individual contracts. According to Section 3(26) of the Public Procurement Act, centralised purchasing means an activity by a central purchasing body pursued permanently for the purpose of placing orders for products and services for resale to contracting authorities as defined in the Public Procurement Act, or entering into supply contracts, service contracts and works contracts or framework agreements for contracting authorities as defined in the Public Procurement Act. The Authority established that the client appeared as contracting authority in 41 cases acting within its responsibilities as central purchasing body, but only in one contract as a contracting party; the Authority deemed that the failure to provide the data was an infringement with regard to this contract. As a result of the procedure, the client published the data related to the contract concerned. [NAIH-5298/2023]

Section 37/C(3)(b)(ba) of the Privacy Act also requires the publication of the value of the contracts subject to the reporting obligation on the Platform. However, the determination of the value of the contracts to be published gave rise to several questions concerning the interpretation of the law. Section 37/C(4) of the Privacy Act states that as regards periodically recurring contracts concluded for a period exceeding one year, the calculation of value shall be based on the amount of consideration for one year. Several budgetary organs interpreted this provision, as meaning that the part of the total value of a contract calculated for one year has to be shown in the platform as the value of a contract concluded for more than one year. However, according Section 37/C(3)(b)(ba) of the Privacy Act the total net value of the contract has to be published and not the value calculated for one year. In Section 37/C(4) of the Privacy Act, "calculation of value" means the operation when the budgetary organ determines whether the value of the contract calculated for one year exceeds five million forints, i.e. whether the contract is subject to the reporting obligation. Always the total net value of the contract has to be shown in the data sheet, even if the contract was concluded for several years. [NAIH-9468/2023]

A government office did not provide data on a contract because, in its interpretation, if the commencement of the performance of a contract and the date of

its performance are in two separate financial years, the value of the contract will be half the total value, even though the contract was not concluded for a period longer than a year. The Authority established that the term “concluded for a period exceeding one year” in Section 37/C(4) of the Privacy Act is not to be understood as financial year in view of the fact that the legislator in the next sentence of the same paragraph specifically mentions the term “financial year”. [NAIH-7650/2023]

Another recurrent problem related to the value of contracts is the deduction of the value of the eventually unused optional parts from the total value of the contract. However, the Privacy Act does not contain a provision that the full consideration of a concluded contract as set forth in the contract could or should be adjusted in view of the used or unused contract option(s) or the amount(s) actually paid, as the case may be, based on the contract concerned when meeting the obligation to publish on the Platform. [NAIH-8616/2023]

The question whether the own funds of an organ qualify as domestic funds arose both as a question for consultation and in an authority procedure for transparency. Some 92% of the revenues of a client (hospital) was financed by the National Health Insurance Fund of Hungary (financial funds of social security) under the heading B16, Revenues of support for operation from within public finances. The client’s position was that it was under an obligation to publish procurement procedures financed by budgetary funds and EU funds pursuant to the Act on Public Finances, and not the contracts concluded to debit its own budget. The Authority stated that Section 37/C(2) of the Privacy Act specifies three categories for publication: budgetary support, contracts and payments. The obligation to publish is conditional upon their extent exceeding five million forints and that they are implemented from national or European Union funds, but not conditional upon being funded from budgetary support. The joint interpretation of the introductory provision, justification and Section 1(1) of Act CLXXXI of 2007 on the transparency on public grants from public funds reveals that funding from the subsystems of general government qualify as domestic funds. Pursuant to Section 6/A(1)(c) of the Act on Public Finances, budgetary revenue estimates and expenditure estimates in the act on the central budget appear as appropriations for the financial funds of social insurance. Section 6/A(4) of Act on Public Finances requires that the financial funds of social insurance in the course of the operation of the system of social insurance serve to settle the budgetary revenues to be collected on behalf of the state and the budgetary expenditures to be performed. Pursuant to Article 39(3) of Hungary’s Fundamental Law, public funds mean the state revenues, expenditures and claims. That means that the client’s operation

is financed by the financial funds of social insurance from budgetary revenues to be collected by the state from within general government, i.e. domestic funds and public funds. So, the Authority declared in its decision that the client's own budget qualifies as domestic funds, hence the data of the contracts to be implemented out of these funds are subject to the scope of the obligation to publish. [NAIH-7661/2023, NAIH-6881/2023]

In many cases, deficient reporting could have been avoided, had the budgetary organ checked the reports that actually appeared on the platform following the submission of its datasheet. It has been a frequent problem that even though an organ shows the currency of the value of the contract/grant/payment, it does not appear in the data sheet published on the platform. In these cases, currency appears as formatting in the .xlsx files set by the budgetary organ not as the three-letter abbreviation specified in the Guidelines entered after the amount. As the currency is a format and not a data entered, it is not included in the database in the course of processing, consequently it cannot be generated in the .pdf document either. [NAIH-6631/2023]. Not all data sent in appear on the platform despite submitting the report, if a line remains empty on the datasheet or the organ modifies the format of the datasheet (e.g. supplements it with additional worksheets). [NAIH-6473/2023, NAIH-8363/2023]

The Guideline produced by NAVÜ is not only an indispensable instrument for the correct completion of the datasheet, budgetary organs have an obligation to complete their datasheets in accordance with the Guidelines. Section 4 of Government Decree 499/2022 (XII. 8.) on the detailed rules of the Central Information Register of Public Data requires those subject to the obligation to publish on the platform to make sure that they appropriately complete the datasheet in accordance with the provisions of Section 37/C of the Privacy Act, this Decree and the User's Rules. According to Section 2(1) of the same decree, the Guidelines constitute part of the User's Rules. In spite of this, currencies and the data pertaining to the legal basis and the form of the contract are not shown in accordance with the Guidelines.

However, the experience gained in almost a year of authority procedures for transparency it can be established – despite the above deficiencies – that the new obligation of budgetary organs to publish has proved to be an efficient means to increase the transparency in the use of public funds. As a result of the authority procedures for transparency, the use of HUF 324.9 billion in public funds became more transparent on the platform by 27 September 2023.

Many organs provide data for the Platform that have no general publication scheme at all, or they have one, but there are no financial data on them at all. As it is no longer mandatory to republish the data affected by the new obligation on the websites of the organs, the new Platform is increasingly becoming the central database for the most important financial data. It contains data, which can be found in other public databases, but here public procurement data, grant data and payments can be found collected in a single database for 10 years. It is possible to conduct searches in the database, for instance, we can learn which ministries concluded contracts with a given contracting party.

As a result of the authority procedures for transparency, budgetary organs reported that:

- *"they built the obligation into their work processes, rules and quality assurance audits,"*
- *"they renewed their internal processing and commitment processes; their acceleration became necessary, hence to speed up the data entry and uploading processes, they initiated the development of new rules,"*
- *"labour force was regrouped within the organisation in order to be able to comply with their reporting obligations on time in the future,"*
- *"uploading was not carried out because of an internal communication problem, but new procedures were introduced".*

These corrective solutions at organisational level should be underlined not only because they can facilitate the lawful meeting not only of the new obligation, but also of the general obligation to publish.

However, a deficiency of Section 37/C of the Privacy Act is that its scope does not cover all the organs performing public duties and spending public money, but the budgetary organs only, for instance, the new obligation does not apply to municipalities (it does, however, apply to the budgetary organs founded by them, such as the mayor's offices). [NAIH-6137/2023, NAIH-5558/2023]

III.3. The most important decisions of the Constitutional Court and of the courts of justice concerning the accessibility of data

III.3.1. Constitutional Court decisions

Decision 3/2023 (IV. 17) AB concerning the establishment of unconstitutionality caused by an omission related to the accessibility of bank secrets that qualify as data of public interest or data accessible on public interest grounds. [NAIH/5942/2022 – providing an opinion]

The petitioner initiated a lawsuit for the issue of data of public interest against Eximbank. The courts sustained the petition and ordered the bank to issue the data. The court of second instance upheld the decision. The Curia repealed the final judgment, changed the verdict of the court of first instance and rejected the petition. According to the position of the petitioner, the bank secret is not an unconditional impediment to the freedom of information, instead it is a restriction as a trade secret, based on a test regulated by law. The Curia was wrong in applying it as an absolute impediment, whereby it violated the enforcement of the freedom of information. In the course of its proceedings, the Constitutional Court contacted the Nemzeti Adatvédelmi és Információszabadság Hatóság (hereinafter: NAIH). The Authority deemed that "in the case under investigation, based on the identity of the controller (an organ performing public duties) and the activities carried out by it (management of public assets, public funds with a view to the implementation of governmental cooperation and economic policy), the provisions of the Privacy Act concerning the issue of data of public interest should apply". At the same time, "it would create a clear-cut legal situation, if the reference to obligations concerning data of public interest – and hence the legal exemption from bank secrets – were to appear among the provisions of the Exim Act". In its decision, the Constitutional Court established that in the present regulatory environment the bank secret excludes the data of all the clients of Eximbank (even if they are legal entities) without regard to the fundamental right of the freedom of information in a manner excluding consideration from the public, in spite of the fact that in the context of tied-aid loans, the bank performs public duties as the organ implementing government decisions, in the course of which it manages public funds, which fact is known in advance to the beneficiaries of the loans. Within this category, the constitutional interest in the accessibility of data as a main rule takes precedence over the interests in protecting secrets. However, the accessibility of dual nature data, held by Eximbank, i.e. data of public interest(or accessible on public interest grounds) covered within the notion of bank secret is not at all ensured in the current regulatory environment: the restriction of accessibil-

ity is total, not tailored to the unconditionally necessary and proportionate extent and there is no possibility for considering whether the data may be issued. The Constitutional Court therefore established that the legislator created a breach of the Fundamental Law by omission, failing to enact guarantee rules enabling the enforcement of the freedom of information with regard to the accessibility of bank secrets qualifying as data of public interest or data accessible on public interest grounds held by Eximbank that performs public duties and manages public funds, so the Constitutional Court called upon the Parliament to meet its legislative duties related to this.

Order 3525/2023. (XII. 14.) on the rejection of a constitutional complaint: until the commencement of the performance of the public duties, the request to access data is premature [antecedent: Budapest Court of Appeal Pf. 20.290/2023/6.]

Based on Section 53/A(1) of Act CLXXXV of 2012 on Waste, the contract concluded with the state entered into force on 1 July 2023 with the provision that the concession company will be entitled to exercise the concession only "*if it obtains the necessary permits and concludes the contracts providing for capacity"* by 31 December 2022 at the latest. On 31 January 2023, the petitioner submitted a request for data of public interest to the concession-holder, in which he requested the permit and the one or more contracts providing capacity. The Constitutional Court established that it does not follow from the final court decision approving the rejection of the request as the basis that *data related to the preparatory activity in the context of the performance of public duties are not data of public interest under any circumstance, but that the request to access the data is in fact premature until the commencement of the performance of the public duty.* Until the entry into force of the concession contract, essentially a contingent legal situation obtains, or if the concession contract does not enter into force for any reason, with regard to the concession-holder (and the concession company founded by it) cannot be said to be performing public duties and so there are no data of public interest in view of Section 3(5) of the Privacy Act. Based on all this, not even a doubt concerning unconstitutionality influencing the court's decision in merit arose, hence the Constitutional Court rejected the complaint. [See also Budapest Court of Appeal Pf. 20.540/2023/4]

Decision 3483/2023 (XI.7.) AB Accessibility of the benefits of senior employees of the National Office for the Judiciary (OBH)

In his request for the issue of data of public interest, the petitioner *r*equested the sending of data concerning certain benefits paid to the leaders of the National

Office for the Judiciary (OBH) in a breakdown by name and the year of payment. In its answer, OBH refused to grant the request for data because, in their view, these do not qualify as data accessible on public interest grounds. In its decision, the Constitutional Court established that OBH as an organisation managing public funds is under an obligation to provide information on the total amount of benefits paid to its employees and their background. However, it is not an unnecessary and disproportionate restriction of the right to access data of public interest when the controller refuses the request for data extending to the benefits of every employee in a managerial position. The final court judgment found a fair balance between the accessibility of data and the protection of personal data, hence it did not result in a violation of the petitioner's right set forth in the Fundamental Law. Because of this, the Constitutional Court rejected the constitutional complaint.

Constitutional Court Decision 3359/2023 (VII. 5.) AB
The data generated in a contractual relationship between an association and third persons do not qualify as data accessible on public interest grounds, even if they concern the use of funds affecting the central budget.

The association received a state grant of 150 million forints to develop a visitor's centre under one of the programmes of the agency for tourism, which amount was to be used to purchase real property, to obtain the venues of the planned investment, to prepare a feasibility study, to implement the required zoning classification, to prepare constructions plans and to launch a public procurement procedure. After this, the petitioner submitted a request for the issue of data of public interest to the association and requested the issue of the purchase and sale contracts concerning the real property bought by the association. The association did not respond to and did not comply with the request for data of public interest.

The regional court deemed that in the absence of the relevant public service contract and a budgetary grant to finance the task, it cannot be said that the association would have been under an obligation to perform the public duty indicated. The regional court also established that the association supports the performance of the public duties indicated through its activities for the public good, hence the respondent cannot be regarded as an organ performing public duties. The contracts of purchase and sale concluded by the respondent cannot be regarded as data of public interest merely because they were concluded by the respondent. The association did not conclude the contracts requested to be issued by the petitioner with a subsystem of general government, but it pur-

chased real property from a third person out of the state grant paid, based on a grant contract concluded with a person belonging to the subsystem of general government. The data generated in a contractual relationship established between an association and third persons do not qualify as data accessible on public interest grounds, even if they are related to the use of funds affecting the central budget.

The Constitutional Court deemed that the court decision contested by the petitioner does not suffer from deficiencies that would raise doubts of unconstitutionality influencing the judicial decision in merit, or any fundamental issue of constitutional significance.

III.3.2. Court decisions

III.3.2.1. Court decisions concerning the freedom of information in 2023, in which statements of NAIH were referred to

Kúria Pfv. 20.087/2023/6., Issue of public interest, (Reference to statement NAIH/2017/2408/2/V)

The respondent's responsibilities include the development of the documentation of the review of Hungary's National Energy and Climate Plan (NEKT) due in 2023. An independent part of this is the so-called final environmental assessment (SKV). In a request for data of public interest, the petitioner requested the respondent to issue data of public interest indicated in altogether four points.
The respondent informed the petitioner that *the data requested to be accessed support decision-making, hence it is not in a position to send them.* In their answer, they stated that the EU regulation for setting up the framework for consultation does not provide for a time limit; the draft of the first update of NEKT has to be produced by 30 June 2023; the submission would be preceded by social consultation; the decision on its process would be made later. The petitioner requested that the respondent be ordered to issue the environmental assessment produced for Hungary's National Energy and Climate Plan.

The court of second instance, in the justification of its judgment upholding that of the court of first instance, sustained the petition referred to in statement NAIH/2017/2408/2/V of the Hungarian National Authority for Data Protection and the Freedom of information, in which *the Authority declared that examining accessibility of environmental information as data of public interest in the regulatory system of the Privacy Act leads to the establishment that the provisions re-*

stricting accessibility to data supporting decision-making – Section 27(5)-(6) of the Privacy Act – cannot be applied to environmental information because their nature supporting decision-making is based not only on formal criteria, but also on those of content.

According to the judgment of the Curia, the respondent's (controller) request for review is ungrounded, no specific justification for the reasons for restricting accessibility was given in the specific case, the respondent referred to the fact that NEKT had to be reviewed based on EU regulations only in general and this requires the processing and reassessment of the SKV asked to be issued. The courts taking action correctly referred to the fact that legal regulations require the publication of the SKV. *According to the Curia's statement of principle, if a separate legal regulation requires the publication of a document containing data of public interest, the controller may not refuse access to the document by referring to the data as supporting decision-making. General reference to the nature of the data as supporting decision-making without any specificities is insufficient for denying the issue of the data.*

Kúria Pfv. 20.112/2023/5.– Issue of data of public interest, data of government meetings

On 6 January 2022, the petitioner submitted a request for data of public interest to the respondent (Prime Minister's Government Office) requesting the electronic transmission of the dates of government meetings held in October 2009, the copies of the summaries of the meetings and the annexes thereto.
On 22 January 2022, the respondent extended the period open for granting the data request, then in its answer sent on 21 February 2022 refused compliance with the request based on Part IV of the justification to the Constitutional Court's Decision 32/2006. (VII. 13.) AB.

In its earlier precedent-setting decision, Curia stated as a matter of principle that the obligation to provide data of public interest is independent of the type of organisation concerned, its ownership relations, its activities; the obligation to make data of public interest accessible is established merely by the fact of possessing the data of public interest (Kúria Pfv.IV.20.911/2018/4.). In line with this, the Authority's statement of 28 February 2022 declared that in general it is not an impediment to issuing the data that the data themselves do not relate to the operation of the organ performing the public duty in itself, or were generated in the context of its own operation, merely the fact that the data were in the possession of the controller (which was not disputed in the given case) in itself lays

the ground for the obligation to issue the data. Nevertheless, the courts taking actions did not violate any legal regulation when they did not order the petitioner to furnish additional evidence with regard to the nature of the requested data as data of public interest, or the activities of the respondent controller. Overall, it can be established that the requested data qualify as data of public interest, irrespective of whether they apply directly to the activities of the respondents or were generated in relation to its activities.

Budapest Court of Appeal Pf. 20.236/2023/5. Issue of data of public interest – Accessibility of data of government meetings

The court of first instance correctly stated in its decision that the data requested to be issued in the lawsuit qualified as data of public interest not on the basis of Section 7(3) of the Administration by Government Act but under the provisions of the Privacy Act.[...] The Constitutional Court in its decision (32/2016 (VII. 13.) AB) stated on the one hand that the classification of certain data of government meetings cannot be regarded as anti-constitutional and on the other hand that pursuant to Section 7(1) of the Administration by Government Act, the meetings of the government are not public.[...] It follows that the data requested by the petitioner qualify as data of public interest, the capacity of the respondent as controller can be established and, furthermore, the data were not classified by a person or organisation entitled thereto in a procedure specified by legal regulations, they were not classified data, hence the data have to be issued upon request.

Budapest Court of Appeal Pf. 20.376/2023/4., Issue of data of public interest, Hungarian Association of Judicial Officers (MBVK) (case of the same subject matter: NAIH-2825-8/2022.)

By a request for data of public interest, the petitioner requested the respondent, the Hungarian Association of Judicial Officers (MBVK) to issue the contracts concluded with six legal entities in relation to the performance of its public duties, and any eventual contract amendments and annexes. The respondent denied the petitioner's request stating that in its view the requested data qualified as personal data as the data of natural persons can also be found in the contracts and that the contracts also contain trade secrets. It also stated that the entirety of the contracts as documents are not within the notion of data of public interest or data accessible on public interest grounds, hence the requested contracts cannot be issued even under a request for data of public interest.

In its judgment, the court of first instance ordered the respondent to issue the requested documents to the petitioner within 15 days obliterating the personal data in the documents. The court's position was that pursuant to Sections 34/A(1), 250(1) and (2) of Act LIII of 1994 on Judicial Enforcement, the respondent doubtlessly performs public duties when discharging its duties related to enforcement. In view of this, the data in its possession concerning its activities and financial management are data of public interest, which the respondent has to make accessible to anyone. With regard to the personal data included in the contracts, the courts declared that even if the contracts requested to be issued have such content that, however, does not provide grounds for denying the issue of the entire document. The court also explained that the respondent must grant the request to issue the data in such cases, while blocking the personal data.
The court declared that the legal regulation does not contain any restriction as to what extent of the data content of contracts subject to the disclosure of data can be requested; these contracts meet the notion of data of public interest and the petitioner lawfully requested their issue, in view of which the denial by the respondent was qualified as unlawful.

In its appeal, the respondent expressly acknowledged that it performed public duties. With regard to the accessibility of data of public interest, Section 26(1) and Section 3(5) of the Privacy Act are of decisive significance; this regulation does not specify the fact of managing public funds as a condition of performing public duties and indirectly as a criterion of having access to data of public interest. Based on the definition of the notion of data of public interest with regard to the right to access data of public interest, the following are of outstanding significance: - the requested information should be processed by the organ performing public duties; - the data apply to the activities of the organ performing public duties, or be generated in relation to the performance of its public duties; - the data do not qualify as personal data. Based on Section 1 of the Privacy Act, the notion of personal data as set forth in Section 3(2) of the Privacy Act can only be applied to natural persons. Judicial practice has been consistent in that if in a lawsuit for access to data of public interest the respondent refers to the existence of a trade secret only in general, by invoking a legal regulation, this does not lay the grounds for the restriction of accessibility. The link between a trade secret and the blocking of personal data in the documents may only relate to the personal data of natural persons, and therefore no inference can be drawn from this to the existence of a trade secret or the disproportionate i*njury by the disclosure.*

Budapest Court of Appeal, Pf. 20.555/2023/6. (NAIH-873/2022, NAIH-977/2023) – Production of new data, formal reference

The respondent (Central Administration of National Pension Insurance – ONYF) was unable to prove beyond any doubt that they rejected the data request for well-grounded reasons based on Section 31(1) of the Privacy Act and that granting the request would have qualified as the production of new data based on the criteria of Constitutional Court Decision 13/2019. (IV. 8.) AB. So the information requested by the petitioner qualified as data of public interest according to Section 3(5) of the Privacy Act processed by the respondent and the court of first instance ordered the respondent with good grounds to render them accessible based on Section 26(1) and 28.(1) of the Privacy Act. In his request for data, the petitioner requested the detailed data of allowances disbursed by the ONYF for the years 2017-2022 in a breakdown. The respondent did not dispute that the requested information can be produced in its answer to the Authority, it even referred to the data processing steps required; the facts of the case did not have to be supplemented in this regard. The burden of proof with respect to the lawfulness and justification of the denial lay with the controller, i.e. the respondent. As a justification for denial, the respondent stated that it had to produce new data to comply with the request and it was not under an obligation to produce the data. Consequently, based on Section 31(2) of the Privacy Act, it had to prove that generating the requested information was such a complex task which, in view of the justification of the Constitutional Court Decision, qualifies as the generation of new data, hence it does not process the requested data of public interest. It cannot be assumed that the required IT and legal knowledge was not available to the respondent that processed large quantities of personal and other data. The respondent did not state either in the lawsuit or in the procedure before the Authority that providing the information would jeopardise its operation or eventually involve a disproportionate volume of work and would be abusive. Hence, it was not necessary to consider whether the right to access data of public interest could be restrictive in the interest of protecting a constitutional interest in accordance with the justification of the Constitutional Court Decision (paragraph [56]). Pursuant to the Constitutional Court Decision (paragraph [58]), the fact that the requested information of public interest is not available elsewhere (data monopoly) has to be taken into account. In its procedure, the Authority attempted to clarify the accurate operations, data processing steps; however, in its answer the respondent did not specifically present the processing steps leading from the personal data to the requested information, it merely referred to general mathematical and IT operations, on the basis of which, in view of the electronic processing of the data, it was not possible to make any conclu-

sions concerning the justification and the grounds for the denial. Nor could any conclusion be drawn as to what extent the described mathematical and IT operations qualify as complex. In this respect, it must be taken into account that the respondent has processed the elementary (personal) data electronically, which was not disputed. So, the same processing operations which may qualify as complex on paper and involve a substantial workload can be carried out quickly and simply electronically with or without algorithms and functions for a person with IT qualifications, depending on the circumstances and the IT possibilities of searching and anonymisation. The information obtained in this way can be filtered, sorted and summarised in tables using the same operations. The necessary data of the tables can be summed by simply adding up the lines of the tables using IT methods (simple mathematical operations). In this context, it should be borne in mind that a request for the collection of the recorded data, their sorting according to specific criteria and arranging them in tables cannot fundamentally be denied according to the justification of the Constitutional Court Decision (paragraph [55]) Depending on the circumstances, it is possible that in possession of a methodology known, based on an earlier request for data, the data requested by the petitioner should be perceived according to the justification of the Constitutional Court Decision (paragraph [49]) that the requested information "is ready and available". The respondent failed to present any other specific fact enabling the assessment of the processing steps. In its answers to the questions posed in the Authority's procedure, it failed to make any statement of merit concerning the time and labour required for the operations, and the statistics used to process the data of pension payments. Instead, the respondent underlined both in the procedure before the Authority and the court its position that the required processing operations described go beyond simple mathematical or IT operations, however, this statement could not be checked in the absence of the presentation of the specific data generation steps. Without the possibility of checking the content of the reasons for denial, the denial of a request to access data of public interest with reference to the generation of new data proved to be a mere formal reference, which in the practice of the Constitutional Court is an impermissible restriction of the freedom of information, hence it is not lawful. In this context, the Budapest Court of Appeal underlines that under the justification of the Constitutional Court Decision {paragraph [61]}, it has to be examined with the greatest of care whether the data request is indeed for the generation of new data, which qualitatively differ from the processed data as denial of access to data of public interest may ultimately impede informed participation in debates on matters of public inter*est.*

III.3.2.2. Further court decisions concerning access to data

Kúria Pfv. 20.041/2023/6. Issue of data of public interest: data to support decision-making

According to the arguments of the respondent (*Prime Minister's Office*) in the review proceedings, the procedure of furnishing evidence did not violate the law, but the court of second instance failed to enforce the constitutional criteria for excluding access to the requested data with sufficient weight, which was an issue of substantive law affecting the legal basis of the petition. [...] In these cases, the point of departure is that preparation for decision-making by civil servants should be carried out freely, informally and free of the influence of the public as a safeguard for the quality and efficiency of the work by civil servants [Constitutional Court Decision {21/2013. (VII. 19.), Justification [43]. [...] Once the decision is made, the principle of accessibility is again applicable to the data as a main rule, and – within the period specified in paragraph (5) – the data request may be denied only if the data support additional future decision-making or access to the data would jeopardise a lawful operation or the performance of the functions and responsibilities of organs performing public duties free of undue external influence, thus, in particular, the free expression of the views of those generating the data in support of decision-making [Constitutional Court Decision {3190/2019. (VII. 16.) Justification [39]) [...] According to the four-step test, the data supporting decision-making must be related to a specific decision-making procedure; the entire document irrespective of its content cannot be qualified as data supporting decision-making; instead of the document principle, the data principle has to be applied; the controller may not invoke so-called "criteria of convenience"; the decision rejecting the data request must be justified in terms of content and the court taking action must equally examine the grounds for denying the provision of the data and the deficiencies of its content based on the document constituting the subject matter of the data request.

Kúria Pfv. 20.509/2023/4. – Issue of data of public interest – data supporting future decision-making as the reason for refusal

The Curia had to come to a decision whether there is a reason to restrict accessibility based on Section 27(6) of the Privacy Act. [...] According to Section 27(6) of the Privacy Act, within the time limit of 10 years referred to in paragraph (5) – a request for access to data used for supporting decision-making may be refused after the decision is adopted, if

– the data supports also future decision-making, or
– access to it would jeopardise the lawful functioning of the organ performing public duties, or the performance of its functions and powers without undue external influence, such in particular the free expression of its views generating the data during the preparatory stage of decision-making.[...]

As the Curia also accessed the content of the report, it upheld the position taken by the court of second instance that the report fundamentally contained facts and data, whose issue would not in any way materially affect the lawful operation of the respondent, which has a professional staff, or the exercise of its functions and powers without undue external influence .[...] In this context, the Curia emphasised that the accessibility of data of public interest has a constitutional role: to render the operation of the state and the use of public funds transparent and the report is expressly linked to this.

Kúria Pfv. 20.234/2023/3. Issue of data of public interest – threat to IT security

According to the interpretation of the law by the Curia, the following provisions of the Information Security Act, ensuring protection of the electronic system, facilitate the attainment of this objective of the law: Section 1(1)(8) of the Information Security Act defines the notion of secrecy (the feature of an electronic information system that the data and information stored therein can be accessed, used or disposed of only by people authorised thereto and only according to their level of authorisation).[...] The above provisions of the Information Security Act as the law referred to in Section 27(2)(c) of the Privacy Act clearly state who is authorised to access data stored in a closed system depending on security classification and under what conditions and that the principle of secrecy must be implemented through the entire life cycle with a view to the protection of the national data assets.[...]

According to the Curia's interpretation based on Article 28 of the Fundamental Law, bearing in mind the objectives indicated in the Recital to the Information Security Act, an interpretation of the provisions ensuring the protection of the electronic information system containing the register of personal data and residential addresses at the highest level, which would render protection contingent on which element of the system architecture it applies to, goes against common sense.[...] Although the laws restricting the freedom of information should be interpreted strictly, in the given case under a different interpretation, the full protection of the electronic system containing the register of personal data and

residential addresses cannot be guaranteed, this restriction is expressly permitted by Section 27(2)(c) of the Privacy Act for the prosecution or prevention of criminal acts and it means a legitimate restriction of the accessibility of certain data of public interest.

Budapest Court of Appeal Pf. 20.369/2023/3. Issue of data of public interest – data of hospital infections – National Centre for Public Health and Pharmacy

Exemption from the obligation to make data public cannot be based on the argument that the disclosure of the data – without knowledge and assessment of the additional information necessary for the analysis of the data – leads to incorrect interpretation or conclusions.

Reference to the fact that the requested data were unavailable was not made in the course of the lawsuit, only in the appeal based on Section 14(1) and (2) of Decree 20/2009. (VI. 18.) EüM on the prevention of infections related to healthcare and the professional minimum criteria and supervision of these activities. [...] Based on all this, the obligation of electronic publication does not influence the requirement of meeting the petitioner's request for data in view of the fact that not even the respondent argued in the lawsuit that from the links indicated in its answer sent to the petitioner in the course of the preliminary procedure, the summary reports of the infection data of the given years were accessible.[...] The Budapest Court of Appeal agreed with the position of the court of first instance that the reference that the publication of the number of infections in individual healthcare institutions and their eventual propagation could be misleading, and that there could be a risk that the misinterpretation of information on hospital infections would result in decreased confidence in certain institutions could not be used by the respondent for exemption from the obligation to issue the data. [...] The Curia (in its judgement Pfv. 21.081/2018/5 stated that although the court may not examine the purpose of lawful processing, it attached importance to stating in view of the specific nature of the data that the accessibility of data of public interest is closely related to the right to freely express opinions, which right should be exercised with responsibility.

Budapest Court of Appeal Pf. 20.385/2023/4. – Meeting a request for data of public interest by inspection

The respondent did not dispute that it was an organ performing public duties or that the data wished to be accessed by the petitioner where data of public inter-

est, so it had to be examined whether the possibility of inspection offered by the respondent qualifies as meeting the petitioner's request to access data of public interest.
The court of second instance emphasized that according to Section 30(2) of the Privacy Act, data requests shall be complied with in a comprehensible manner and if the organ performing public duties that processes the data in question is able to bring it about without disproportionate difficulties in the form and manner requested by the requesting party.
During the litigation, it was not disputed that complying with the request in the manner indicated by the petitioner would not have given rise to disproportionate difficulties for the respondent (an organisation performing public duties), hence it should have met the data request in the manner indicated.

III.4. Access to personal data accessible on public interest grounds

Since the General Data Protection Regulation (GDPR) has become applicable in May 2018, the joint and interactive application of the rules on the protection and the accessibility of data poses particular challenges for the organs performing public duties as controllers. The Authority has addressed this issue with emphasis already in its 2022 report: whether personal data should be issued and if so, under what conditions and for what processing purposes they may be used, disseminated and made public.

Only law may make personal data public on public interest grounds; such a provision is, for instance, Section 26(2) of the Privacy Act, but so are the provisions of the sectoral laws pertaining to the legal status of certain persons discharging public duties. However, the fact that the personal data are accessible on public interest grounds by provision of a law does not mean that the provisions and principles applicable to the protection of personal data would not at all be applicable to their processing. In the 21st century, the accessibility of data and the associated consequences are to be interpreted and enforced differently, despite the fact that the requirement of technological neutrality is enforced in the course of processing; however, for instance, ensuring the right to be forgotten – on the worldwide web, social media and applications – pose additional challenges to the data subjects of data accessible on public interest grounds, their controllers and publishers.

There are other instances related to the accessibility of data, which merely give rise to violations of the right to informational self-determination; these are the

cases when unauthorised third person outsiders have access to personal data to be protected in official documents published on the Internet, which otherwise qualify as data of public interest (e.g., submissions for municipalities, minutes of meetings of the body of representatives, decisions or matters disclosed orally during a public meeting). The accurate delineation of data protection and data accessibility requires particular care and professional skill in these municipal matters concomitant with multi-level, multi-dimensional accessibility, for which not only the municipal executive and the civil servants, but the body of representatives, the members of committees, the persons lawfully present in public or closed meetings have joint but also individual responsibility.

Another contemporary feature is the expression of opinions on social media platforms and the related processing of the data, whereby a new data processing, disclosure and publication is implemented using personal data accessible on public interest grounds, or have already been made public or disclosed by the data subject, as well as non-public personal data, which has paramount consequences for personality rights in addition to the right to informational self-determination. In general, the perpetrators of infringements, shrouded in the benevolent shadow of anonymity, ride roughshod through others' dignity, entering the swamp of areas beyond the law, with no regard for accountability.

Section 1 of the Privacy Act ensures that (personal) data accessible on public interest grounds be accessible and disseminatable with a view to ensuring the transparency of public affairs in line with the Recital to the Act. The processing, use and publication of data must be in line with this purpose in view of the principles of data processing already referred to, such as data minimisation, the right to be forgotten, etc.

III.4.1. Enforcement of data subject's rights with regard to personal data published in Magyar Közlöny (Hungarian Official Journal) or submissions of bodies of representatives

In an authority procedure for data protection, the data subject wished to have his name (personal data related to his civil service appointment) from the 2013 volume of the Hivatalos Értesítő (prior to the application of GDPR), which is an annex to Magyar Közlöny. The purpose of processing is that Hungary's official journal, including the Hivatalos Értesítő, which is its annex, be accessible to the public continuously and without distortion for reasons of legal security, which may be deducted from Article B)(1) of the Fundamental Law. The controller could not comply with the erasure request based on Article 17(2)(b) of the General

Data Protection Regulation and it notified the petitioner of this. The issues of the Hivatalos Értesítő cannot be removed from the website and its notices cannot be subsequently modified. The data subject withdrew his request. [NAIH-5869/2023]

In another authority procedure, the data subject requested the erasure of his name and his former work e-mail address from a document published on a municipal website as part of a submission of the body of representatives. The municipality failed to substantiate the priority of its interests in processing the data, whether it is necessary to further disclose personal data generated years before in 2011 in order to exercise the right to the freedom of expression and obtaining information. The municipality also failed to state the specific public affair for the debate of which it would be important to continue to maintain the publication of the data on the Internet today. The Authority found the request for erasure as well-grounded to ensure "*the right to be forgotten*" and established that the rejection of the request was unlawful. [NAIH-5517/2023, 307-1/2024]

III.4.2. The data of municipal officials accessible on public interest grounds and the conclusions that may be drawn from them

A mayor wanted an answer to the question whether the net amount of payments to municipal representatives, the mayor, the deputy mayor and the external members of committees under various headings (emolument, reward, cost reimbursement, etc.) can be issued upon request for data of public interest. In the case of the requested data accessible on public interest grounds, their gross amount was sent to the person requesting them, but with regard to the net amount, certain individual benefits subject to Act CXVII of 1995 on Personal Income Tax (hereinafter: Income Tax Act) qualify as personal data. Gross personal dues (wages, emoluments, rewards, etc.) include the various taxes and contributions specified by legal regulations (personal income tax, pension insurance, health insurance and labour market contributions). It is a fact that gross personal dues consist of the net dues received by the given employee and the public dues payable by him. The Income Tax Act separately provides for the various personal income tax benefits, which reduce gross income with regard to individual persons. As to the persons indicated, the net income requested as data accessible on public interest grounds – just as gross income – can be issued in a single amount to the person requesting the data as in the case of the gross income, it is not detailed what income element it consist of, nor the taxes and contributions to be deducted are detailed per person when issuing the data. [NAIH-1563-2/2023]

III.4.3. The mayor's school qualification

A municipal executive rejected the data request concerning the school qualification of the mayor of a village. The person requesting the data argued that the mayor named his qualifications in the course of earlier election campaigns, as well as in his statements. In the campaign, he referred to his degree, his graduation from a doctoral school and his professional skills. Based on the legal regulations in force, it can be established that the school qualifications of a mayor qualify as data accessible on public interest grounds to the extent that the qualification is a precondition to performing a municipal task or filling a position. Accordingly, the data concerning the mayor's qualifications do not qualify as data accessible on public interest grounds from the viewpoint of the Mayor's Office as controller. It is a different case when the mayor discloses the data concerning his qualifications voluntarily or through another controller based on his clear consent. The Authority's position is that in this case the data are accessible as data accessible on public interest grounds. According to the municipal executive's answer, the mayor had disclosed his school qualifications in the course of the election campaign on flyers; however, the mayor did not confirm this. The Authority recommended to the mayor to consider providing the information to the person requesting the data, so that he as a person performing public duties, as an alderman of the village, prevent that issues of integrity and reputation arise or be disputed in the local community. The data were not issued in the course of the investigation. [NAIH-3526-8/2023

III.4.4. Transparency of the decisions of the Public Service Arbitration Committee

The Authority received a question on the accessibility of the decisions of the Public Service Arbitration Committee. The relevant data request was rejected by the Prime Minister's Office with reference to the fact that Act CXXV of 2018 on Government Administration (Government Administration Act) and Government Decree 69/2019. (IV. 4.) on the arbitration committee does not require the publication or sending of the decisions. Although the procedure of the Arbitration Committee is limited to the legal relationship between the parties taking action in front of it, and the subject matter of the procedure related to the employment relationship of the given government official, i.e. it was related to his private sphere, there might be a public interest in accessing the individual decisions of the Arbitration Committee as an organ performing public duties. If the Board taking action brought a decision extending to issues of principle, the president of the Arbitration Committee could decide whether to publish it on the website

as an Arbitration Committee decision of principle. The fact that no legal regulation requires the accessibility of data, it does not follow that they would not be accessible as data of public interest.[6] According to the Authority's position, the Arbitration Committee is required to comply with a request for data of public interest with regard to decisions made in procedures launched on a specific subject matter, concerning a specific period, or on the basis of complaints against a given government organ in accordance with the provisions of the Privacy Act. Therefore, the Arbitration Committee has to send copies of its decisions concerning the individual case groups to the requesting party based on Section 29(3) of the Privacy Act, if so requested but only after their anonymisation covering their case number in accordance with Section 30(3) of the Privacy Act.
If the requesting party lodges the data request with the government organ affected by the decision, the government organ involved in the procedure as a party itself is under an obligation to issue the decisions of the Arbitration Committee concerning the specific subject matter, or individual case groups, in an anonymised format as described above. With regard to the existence of the obligation to comply with the data request, it is not necessary to examine whether the organ performing public duties is a controller according to the definition in Section 3(9) of the Privacy Act, but whether the condition specified in Section 26(1) of the Privacy Act is met, i.e. whether the data requested to be accessed is actually processed by it.[7] [NAIH-3218-6/2023]

III.5. Transparency of municipalities

III.5.1. The rights of municipal representatives under the law

The Authority examined the issue of the delineation of the right of municipal representatives to obtain information and of their right to access data of public interest or data accessible on public interest grounds in several notifications, i.e. the joint application of the provisions of Act CLXXXIX of 2011 on Hungary's Local Governments (hereinafter: Municipalities Act) and the Privacy Act. According to the Authority's legal practice, the municipal representative can have access to data of public interest and data accessible on public interest grounds, the same way as anybody else; the provisions of the Privacy Act are to be applied to the data request. The rights specified in Section 32(2) of the Municipalities Act to

6 Kúria Pfv. IV.21.093/2020/5., Budapest Court of Appeal Pf.20.023/2022/10., Budapest Court of Appeal Pf.20.066/2022/5.

7 Constitutional Court Decision 6/2016. (III. 11.) AB [31]-[33], Budapest Court of Appeal 2. Pf.20.567/2022/3.

which municipal representatives are entitled do not grant additional rights to access data of public interest and data accessible on public interest grounds.

It is a different case, if the law or the municipal decree enacted based on authorisation by law authorises the representative to have access to some kind of data and to process them with a view to performing his public duties or if the body of representatives of the municipality entrusts him individually or as a member of a committee with the planning, organisation or control of a task within the competence of the municipality. In such cases, the representative may process the personal data indispensable from the performance of the tasks and those listed in legal regulation complying with the principle of purpose limitation. The rules of the General Data Protection Regulation and the Privacy Act apply to all other processing operations involving the processing of personal data, including requests for information in their capacity as a representative. The capacity of being a representative does not in itself authorise a person to access and process personal data.

In relation to a submission, a member of the financial committee of the municipality requested the inspection of the pay list of public employees and civil servants employed by the municipality, the list of their fringe benefits and their base documents. The Authority pointed out what was explained above and called the attention to the rules applicable to the tasks of the financial committee as set forth in the Statutes of the Body of Representatives of the Municipality (hereinafter: Statutes) as a municipal decree. In that specific case, the financial committee and its member could act within the powers specified by the Municipalities Act and the Statutes not by the Privacy Act, but even in this case attention has to be paid to the accessibility of data to be protected, their anonymisation, if needed, and in the case of personal data accessible on public interest grounds to compliance with the principle of purpose limitation in the context of their dissemination. [NAIH-5878-2/2023]

III.5.2. A case of tenement flat rental

The question arose in relation to a municipal representative who was not a member of a committee set up by the body of representatives whether he could inspect the documents laying the foundation for rentals with regard to the municipality's tenement flats. In the cases of tenement flat rental, with emphasis on rental based on welfare issues, the committee processed not only the identification data of the natural person concerned, but also his other personal data

related to his assets, family, welfare and health situation in order to make the decision. Pursuant to Section 32(2)(d) of the Municipalities Act, the representative may participate in the public or closed meetings of any committee set up by the body of representatives, of which he is not a member, and as a representative he may have access to the submissions and minutes of all the public meetings of any committee. However, with regard to the committee of which he is not a member, he may not have access to the submissions prepared for the agenda points of closed meetings and the data needed for decision-making. Based on Section 32(2) of the Municipalities Act, the representative has a right to participate in the closed meetings of committees with the right of consultation. While exercising this right, he may have access to the decision-making procedure, even though he does not directly participate in the assessment of individual cases. In this case, the Authority took the view that it was not necessary to have access to the documentation of the specific individual cases and the data therein for the representative exercising his powers according to the last sentence of Section 32(2)(d) of the Municipalities Act. [NAIH-5924-4/2023]

III.5.3. Regulation of requests for data of public interest in the Statutes

The Authority conducted an investigation against a district municipality because in its Statutes it included the determination of the mode of compliance with requests for data of public interest submitted by representatives within the powers of local legislation, pursuant to which, if the data request was of substantial extent or involved a large number of data, it would be complied with through the inspection of documents. Sections 30(2) and 29(2) of the Privacy Act contains clear rules for compliance with requests for data of public interest; furthermore, the Privacy Act does not grant authorisation for the enactment of municipal decrees to further specify the mode in which requests for data of public interest may be fulfilled. In relation to the municipal decree, the Government Office of the Capital City of Budapest underlined that the rights of representatives guaranteed through the joint application of the Fundamental Law, the Privacy Act and the Municipalities Act may not be restricted with the regulation referred to, and municipalities are not authorised to enact municipal decrees with regard to the essential elements of content of the right to access and disseminate data of public interest as a fundamental right. In spite of the consistent position of the Government Office, the body of representatives adopted the decree (the amendment of the Statutes) as described above. With a view to avoiding the future violation of the fundamental right to access data of public interest and data accessible on public interest grounds, the Authority made a recommendation to

the body of representatives of the district municipality to annul the regulation referred to.[NAIH-922-11/2023]

III.5.4. Transparency of the data concerning the lawful operation of the municipality

In a submission, a question related to the transparent operation of municipalities arose as to whether the call for compliance by a Government Office qualifies as data of public interest. When answering the question, the Authority's point of departure was Constitutional Court Decision 32/1992. (V. 29.) AB, which states that the primary function of the freedom of information is to ensure the transparency of the state and control of decision-making by public powers. Pursuant to Sections 26(1) and (2) and 32 of the Privacy Act, the data generated in the course of government offices performing their tasks of compliance control are – as a main rule – data of public interest or data accessible on public interest grounds, to which the provisions of the Privacy Act are to be applied. In terms of the enforcement of the freedom of information, the Authority highlighted that in this case, an organ performing a public duty (Government Office) supervised another organ performing public duties (body of representatives of a municipality), i.e. the Government Office within the scope of its performance of public duties controls the activities of the body of representatives performing public duties. The purpose of the investigations is to re-establish lawful operation and to terminate an unlawful situation and the data relating to this are of public interest by virtue of the definition of the Privacy Act. Once the compliance procedure is closed and the call for compliance is made, the document is public, accessible to anyone, if necessary after the anonymisation of the data to be protected. [NAIH-1678-2/2023]

III.5.5. Publication of data on rent arrears to improve the propensity to pay

The publication of the amount of the overdue rent for the tenement flat owned by the municipality and the name of the debtor on the website of the municipality was subject to investigation. The body of representatives of a city municipality enacted a decree on publishing the names of debtors with overdue rent amounting to a million forints, outstanding for more than thirty days, as well as the amount of the debt on the website of the municipality as long as the debt exists. With regard to the processing of personal data as carried out in this case (online publication), the Authority established that the controller municipality did not have the appropriate legal basis for processing as Act LXXVIII of 1993 on regulating the utilisation of real property held by municipalities, their rules, the

rent of tenement flats and premises and certain rules for their disposal does not grant authorisation for the regulation of the processing of personal data at local level (the enactment of municipal decree), to which the municipality could have referred to as the legal basis of the processing objected to. In addition to establishing the fact of unauthorized processing, the Authority also underlined in its statements made with regard to the purpose limitation of processing: judicial enforcement used by the municipality was successful, hence there was no need for any further processing of the complainant's personal data, in particular, for the publication of the personal data in order to enforce public interest. The Authority made a recommendation for the annulment of the relevant rules of the municipal decree, which the body of representatives complied with. [NAIH-2086-11/2023]

III.5.6. Disclosure of the data of a municipal employee

Based on a notification, the Authority investigated the publication of the personal data of a person employed part-time by a municipality, who was also instrumental in the operation of a workers' hostel held by the municipality. As to the person of the notifier, the Authority established that according to the job description included in his employment contract, he has been carrying out his tasks as a general legal staff member. The minutes of the meetings of the body of representatives and the statement of the municipal executive accessible to the public revealed that he qualifies as an exceptional public actor in the context of performing the public duties in operating the municipal workers' hostel, hence he has an obligation to tolerate the purpose-limited publication of data accessible on public interest grounds related to the performance of the public task: his name, the public task he carries out, his (planned) position and in relation to that, the amount of his (planned) and current wages. The notifier in his capacity as a person performing public duties, voluntarily undertook to operate the workers' hostel of the municipality, hence accepted the publicity concomitant with his position and his obligation to tolerate opinions and criticisms related to his activity. [NAIH-3279-17/2023]

III.5.7. Transfer of a request for data of public interest to the organ performing public duties processing the data

In an investigative case, the municipal executive of one of Budapest's districts informed the Authority of having transferred the notifier's request for data of public interest to the controller Kerületi Közszolgáltató Zrt. as the Mayor's Office did not have the requested data and informed the notifier also of this fact. After this, the notifier submitted a request for an authority procedure for data protection to

the Authority because, in his view, his personal data were forwarded to another independent controller without a legal basis. The Authority rejected the request and underlined the relevant rules of the Council of Europe Convention on access to official documents, which was promulgated in Hungary by Act CXXXI of 2009. Article 5(2) of the Tromsø Convention requires the controller to refer the request to the competent public authority, where possible, or to inform the data subject of the competent public authority to which he may address the request. The municipal executive forwarded the data request to the business organisation held by the municipality that had the data in order to facilitate an outstanding fundamental right, the applicant's access to information of public interest, which the Authority regards to be good practice for the best possible enforcement of the freedom of information. The decision is accessible on the Authority's website based on the case number. [NAIH-1096-16/2023]

III.5.8. Publication of invitations and submissions prior to a meeting

In these cases, the notifiers objected in relation to the public meetings of bodies of representatives of municipalities that the invitations to and submission for the meetings were published on the websites of the municipalities only on the day preceding the date of the meeting, or not at all, and therefore the submissions under discussion were not accessible to the residents prior to the meeting.
In these specific cases, the Authority found that the Mayor's Offices of the municipalities acted unlawfully because they published the invitations to and submissions for the meetings not within the time limit specified by the municipal decree pursuant to the Statutes of the municipality (hereinafter: Statutes) and the Privacy Act on the websites of the municipalities. Beyond this, the Authority also examined the provisions of the Statutes and determined that the time limit set in the Statutes governing the dispatch of invitations and written submissions to the representatives and their publication on the websites in view of Annex 1 II. 9 of the Privacy Act ("*within two days prior to the meeting*") as unjustifiably short, jeopardising the freedom of information and it does not adequately facilitate the accessibility of the points on the agendas of the meetings and the submissions discussed there by the public prior to the meeting. On these grounds, the Authority made recommendations concerning the amendment of the Statutes to the municipalities, whose bodies of representatives put the recommendation to amend the Statutes on their agendas; one of them adopted a municipal decree concerning the amendment of the Statutes, while the other discarded the recommendation. [NAIH-2613/2023, NAIH-7613/2023]

III.6. Accessibility of data of public interest processed on the basis of the general administrative procedures

Earlier in its 2018 report, the Authority analysed the rules pertaining to two fundamental rights – inspection of documents under the General Administrative Procedures Act and accessibility of data of public interest under the Privacy Act – in a separate point entitled "*General Administrative Procedures Act vs. the Privacy Act, or public data in administrative procedures*". The Authority explained its position, according to which the fact itself that the data requested to be issued are otherwise used in an administrative authority procedure does not deprive these data from their character as data of public interest. Whether a restriction of accessibility is justified in view of the administrative authority procedure can only be assessed with regard to a specific case. In its final conclusion, the Authority established that the purpose of the restriction according to Section 27(2)(g) of the Privacy Act is not to restrict the accessibility of data generated in closed administrative authority procedures.

According to the consistent opinion of the Authority, Section 33(3) of the General Administrative Procedures Act only sets forth the data types whose accessibility is subject to conditions. This section of the General Administrative Procedures Act does not contain any restriction on data of public interest or data accessible on public interest grounds, all the provision requires is to render personal data or other protected data unidentifiable. The commentary on this section of the General Administrative Procedures Act also arrives at a conclusion, which is identical to the argumentation of the Authority, according to which the provision refers to protected secrets and documents containing other data protected by law (for instance, personal data). The reason for this wording of the provision is that if the documents contain data of public interest or data accessible on public interest grounds, anyone can access them without separate proof of authorization based on the rules of the Privacy Act.

Based on the practice of the court, it is also incorrect to interpret the legislation, "when the organ performing public duties interprets the regulation under the Privacy Act and the General Administrative Procedures Act in a *lex generalis – lex specialis* relationship". [Debrecen Court of Appeal Gf. 30.126/2016/5.] The judgment referred to also states that *"The respondent had to take action in the specialised authority procedure according to the rules of the General Administrative Procedures Act; however, in the absence of the express prohibition and restriction of the procedural act concerning this could not have affected the obligation of rendering the data of public interest accessible as set forth in*

the Privacy Act; as Curia judgement Pfv.IV.20.455/2015/4 also pointed out, the fact in itself that the requested data of public interest are otherwise used in an authority or judicial procedure does not automatically deprive the data of their public interest character".
In its judgement Pf. 21.108/2019/8, the Budapest Court of Appeal (annulled for legal technical reasons) established that only the provisions of the Privacy Act contain the rules applicable to access to data of public interest. This is distinct from inspection of the document of the administrative procedure based on the General Administrative Procedures Act regulated by its Sections 33-34.
The decision made in administrative authority procedures conducted according to the General Administrative Procedures Act represents data related to the performance of the public duty of a given organ, which is data of public interest based on Section 3(5) of the Privacy Act, with regard to which Section 33(5) of the General Administrative Procedures Act accurately specifies which authority decisions are accessible with what data content: *"If a law does not restrict or exclude the accessibility of the decision, the final decision which does not include personal data and protected data, as well as the order annulling the decision of first instance and ordering the authority making the decision of first instance to carry out a new procedure, may be made accessible to anyone without restriction, once the procedure is completed."*

In one of its procedures, the Authority examined the accessibility of a minister's opinion concerning the protection of heritage and world heritage upon a request for data of public interest. According to the position of the Ministry that holds the data, the requested data are needed to conduct an administrative procedure in progress before another authority, hence it is part of the documentation of this authority procedure governed by the provisions of the General Administrative Procedures Act. With reference to the fact that the requesting party was not a client in the authority procedure concerned, the Ministry refused to issue the requested document. The positions of the Authority and the Ministry have not come any closer, even though the Authority called attention to the fact that the data requested to be accessed qualify as environmental data, hence the restriction of their accessibility should be narrowly interpreted; in addition, the Authority highlighted the public interest in exploring this information.

The notion of "*anyone*" used in the General Administrative Procedures Act corresponds to the definition of "*anyone*" as set forth in Article VI.(3) of Hungary's Fundamental Law and Section 26(1) of the Privacy Act, which includes a client concerned.

The General Administrative Procedures Act grants the right of inspecting documents for a client in the authority procedure, in the course of, and after the closure of the procedure, while the Privacy Act provides an opportunity for any "*third*" party not concerned in the authority procedure to have access to the final anonymised decision, but only after the closure of the procedure. If a person concerned in an authority procedure – as part of the notion of "*anyone*" – requests data of public interest with regard to his own case from the organ performing a public duty, the Curia stated in its judgement Pfv.20.045/2023/7. that *the data request of the requesting party concerning his own case does not promote the transparency of public affairs*, hence it does not meet the requirements set for requests for accessing data of public interest, so *it cannot be qualified as a request to access data of public interest*. The reason for this is that the purpose according to the Privacy Act cannot be interpreted through the data accessed by the client requesting the data against himself (Kúria Pfv.IV.20.419/2021/6.).
The requesting party as client is entitled to exercise his rights as client according to the provisions of the General Administrative Procedures Act, whereby he can have access to the relevant data and information related to the case by way of inspecting documents. On the whole, access by the client to information linked to his own data cannot be reconciled with the social calling of the fundamental right, it does not contribute to the attainment of the goal declared in Section 1 of the Privacy Act, the enforcement of the right to access and disseminate data of public interest and data accessible on public interest grounds and the transparency of public affairs in the subject matters under the scope of the law.

A notifier turned to the Authority because the Mayor's Office (hereinafter: Office) denied granting his request for data of public interest, in which he asked for a copy of the memo prepared by the public area supervisor concerning the onsite supervision on the notifier's terrace, based on a complaint related to the music played by a catering place close to the notifier's residence (hereinafter: memo). The Office denied granting the data request, stating that compliance with the data request is impeded pursuant to Section 27(2)(g) of the Privacy Act as the notifier as client may have access to the requested document in accordance with the rules of document inspection according to Sections 33-34 of the General Administrative Procedures Act after his identification. Relative to this, the Authority found in the course of its investigation that there was no administrative authority procedure in the case subject to the notification and that the requested memo contained all the information concerning the notifier. In view of this, it pointed out that the notifier's request for sending the memo does not in fact qualify as a request for data of public interest as the notifier wished to obtain information on his own case. According to the Authority's finding, the Office

should have identified the notifier's request as one according to Section 15(3) of the General Data Protection Regulation, i.e. as a request for sending a copy of the notifier's personal data processed by the Office and should have complied with that request in accordance with the provisions of Article 12 of the General Data Protection Regulation. The Authority ordered the Office to comply with the data subject's request following the identification of the person of the notifier as needed. [NAIH-7974/2023]

III.7. Cases of restriction on accessibility

III.7.1. Trade secret

The requesting party wished to have access to specific data of contracts concluded by a business organisation in the exclusive ownership of the municipality with a third person; in the relevant investigative procedure, the Authority explained that a given document (such as a contract or price quotation) may include data, which do not belong to any of the data categories indicated in Section 27(3) of the Privacy Act (for instance, priced budget, know-how), or data which have been classified as a trade secret by the other party to the contract with the business organisation held by the municipality. The Authority summarised its position concerning the collision of trade secrets and the freedom of information in its recommendation issued under NAIH/2016/1911/V. According to the recommendation, business organisations at least the majority of which is held by the state/a municipality may not invoke trade secrets with regard to the public duty performed by them (including the management of public assets); at the same time, facts, information, solutions or data qualified as trade secrets are of paramount importance for a business organisation subject to market competition because their corporate and economic plans and strategies are based on them, this information is the basis of their decisions, which ensure their place in the market, thus disclosure of such information may result in them being driven out of the market. Resolving the conflict between trade secrets and the freedom of information, Section 27(3) of the Privacy Act qualifies "quasi" trade secrets related to the budget of the central government and the local governments, the use of European Union funds, benefits and allowances involving the budget, the management, possession, use, utilisation and disposal and encumbering of central and local government assets, and the acquisition of any right in connection with such assets, as data accessible on public interest grounds with a view to

ensuring the transparency of managing public funds. If the holder of the secrets (whether the municipal company or its contracted partner) took the necessary legal measures to keep the trade secret (e.g. express marking of parts concerning the trade secret and detailed explanation of the justification of protection), the business organisation held by the municipality and its contracted partner may not make it public without authorisation. If these data and protected information were to be accessed by the competitors of the business organisation in public ownership, or its contracted partner, it could result in the violation of the legitimate business interests of the contracting parties. [NAIH-6203/2023]

III.7.2. Generating new data

According to the practice of the Constitutional Court, the ordinary courts and the Authority, restriction of the accessibility of data of public interest is only possible at the level of the law, by ensuring the discretion and the obligation of the controller with a view to protecting the interests specified in the Privacy Act; criteria of convenience may not justify the rejection of a data request.
In the case under investigation, the notifier did not ask for the forwarding of a complete register, he only asked for access to a line of data, which can be queried with a simple IT query operation. In view of Constitutional Court Decision 13/2019. (IV. 8.) AB, Justification paragraph [55], the Authority explained: *if the data request applies to the selection by queries according to specific criteria, of existing and processed (recorded) data and, for instance, organising them in a table, the request may not be denied. The request must be complied with*, irrespective of the form of recording and irrespective of whether the data has to be found through the review of the controller's records and/or documents stored by the controller. Just as the controller may not deny compliance with the data request on the basis that it would require the review of the documented processes and the separation of the accessible and the inaccessible data in it. The Authority also underlined that mere administrative considerations may not result in the restriction of the freedom of information. [Constitutional Court Decision 12/2004. (IV. 7.) AB]

In summary, the Authority consistently holds the position that the performance of simple IT operations, such as query and adding up, do not qualify as the generation of qualitatively new data. To comply with the data request constituting the subject matter of the case, there was no need to perform operations beyond simple IT, mathematical or other operations causing substantial difficulties. In the case of the data request under investigation, the subject matter was to query

data stored, data that could be queried by simple (or additional) work as set forth in Constitutional Court Decision AB 13/2019. (IV. 8.), so compliance with the request did not require the obtaining or collection of new data from other organs, the provision of explanations or drawing conclusions.

A merely formal reference to Constitutional Court Decision 13/2019. (IV. 8.) AB without the actual examination of the content of the individual issues of the request for data for public interest and of the answers to be given to them qualifies as *undue restriction of a fundamental right* set forth in Article VI.(3) of the Fundamental Law clashing with Article I.(3), and therefore *it is anti-constitutional.* [NAIH-9111-2/2023]

III.7.3. Government Integrated Portal for the Disclosure of Data of Public Interest (KIKAP Portal), Authority Integrated Portal for the Disclosure of Data for Public Interest (HIKAP Portal)

In the investigations of the Authority based on complaints against the operation of the HIKAP and KIKAP Portals, all the complaints objected to the fact that the data of public interest or data accessible on public interest grounds made public through an URL were accessible for 15 days after uploading, thereafter the data were archived and erased after 90 days. The data of public interest "made public" on the HIKAP and the KIKAP Portals are accessible exclusively to the requesting party or to the person who has the URL sent by the controller for downloading the data, for 15 days.

The controller (the organ issuing the data) does not monitor whether the requesting party receives the data or document requested to be accessed by him. The requesting party has to notify that he is unable to access the requested document for some reason, in which case the controller sends a link again to the e-mail address of the requesting party. An additional problem discovered in the course of the investigation was that the KIKAP and the HIKAP systems automatically place two watermarks on the given document: the e-mail address of the requesting party and the KIKAP caption. According to the controllers, the purpose of this is the "one step identification" of the requesting party.

According to the position of the Authority, the watermark applied on documents issued upon requests for data of public interest – even if the watermark does not block the data of public interest in a given case – impedes the right to disseminate data of public interest as ensured by the Fundamental Law, particularly if

the watermark also includes the personal data of the requesting party (such as his e-mail address). [NAIH-7525/2023., NAIH-44/2023., NAIH-584/2023.]

III.7.4. Portal used by the Hungarian Association of Judicial Officers (MBVK) to comply with data requests

According to a complaint related to granting a data request, the download did not start when clicking on the "*Download*" button, and the series of data disappeared. The complainant also objected to the fact that he could have been able to download the answer uploaded for the data request only once within a period of two weeks, and that the watermark running across the entire page, including his personal data (his name, the date of the data request and his e-mail address) blocked one of the key data.

To provide data of public interest electronically, MBVK developed a portal for providing data. According to MBVK, its advantages include the minimisation of data loss, an increasingly transparent form of the uploaded materials and complete protection of the personal data of the requesting parties. The provider of the data receives confirmation of the downloads sent to the users. At the same time, the controller does not ascertain whether the requesting party has actually accessed or downloaded the data of public interest. As a result of the investigation, the watermark is no longer applied and downloading the uploaded documents is no longer restricted.

III.7.5. Portal to grant data requests used by the Supervisory Authority of Regulated Activities (SZTFH)

The notifier objected to the fact that SZTFH answered his data request in a format, which he could not access and the answer was archived. The notifier did not receive any information about how long the answer would be accessible and how many times could be downloaded.

The HIKAP Portal is used for uploading data of public interest and data accessible on public interest grounds made public through compliance with requests for data of public interest and for sending them to the requesting parties. In addition, SZTFH cited the rationalisation of internal administrative operations and increasingly efficient, more secure and faster management of cases as arguments in favour of the use of the system. The requesting party receives the URL for data access and information on legal remedy in a letter sent to his e-mail address provided in the course of requesting the data.

As a result of the investigation, SZTFH has modified the general operation of the HIKAP Portal so that the answer to the data request is accessible for a year following publication on the portal, after which the data content is archived for 90 days.

III.8. The accessibility of environmental data

Similarly to previous years, controllers mainly refer to Section 27(5)-(6) of the Privacy Act when rejecting data requests for environmental information.

The notifier requested an expert document from the municipality of a city with county rights which contained the results of a hydrological test of an area, which the municipality intended to sell subsequently, and for which a water rights licensing procedure was also in progress. The municipality justified the rejection of the data request stating that the requested data supported decision-making. In its call, the Authority explained that an organ performing public duties may apply Section 27(5) of the Privacy Act to restrict accessibility only with regard to a procedure aimed at decision-making within its own responsibilities and powers. The Privacy Act disallows an organ performing public duties to restrict access to the data of public interest it processes by reference to a procedure in progress before any authority. Only the head of the organ conducting the procedure is in a position to carry out the balancing test required by Section 30(5) of the Privacy Act to assess whether the restriction of accessibility is necessary for the lawful and professional operation of the organ he heads.

The municipality presented that the data requested by the notifier were also needed for an eventual purchase-and-sale procedure, in which the municipality would be the seller. According to the position of the municipality, the expert opinion contains statements that are difficult to interpret without the appropriate expertise. In its call, the Authority explained that according to the consistent practice of the Authority and of the courts the comprehensibility of the data may not influence the accessibility of data of public interest. In its judgement Pfv. 21.081/2018/5., the Curia declared that *"Even the respondent may contribute to the correct interpretation. Nevertheless, eventual difficulties in interpretation in themselves do not provide grounds for denying the issue of the data."*

The Authority also underlined that the data requested by the notifier qualify as environmental information pursuant to Section 2(a) of Government Decree

311/2005. (XII. 25.) on the order of public access to environmental information. Based on the consistent practice of the Authority and of the courts, the public interest in compliance with requests to access environmental information is particularly significant: *"the appropriate protection of the environment is indispensable for human well-being and the exercise of fundamental human rights, including the right to life. It is a fundamental right that everyone has a right to live in an environment appropriate for his health and well-being, and everyone individually, as well as together with others, has an obligation to protect and improve the environment for the benefit of current and future generations. To ensure this right of citizens and to enable them to meet this obligation, information on environmental affairs must be made accessible to them, they must be granted the right to participate in decision-making, hence in environment-related cases in the given case, the deepening of the accountability and transparency of decision-making is more important than trade secrets, and through this, the reinforcement of the support by the public of decisions. Because of the interest of society in safeguarding the environment, access to data on environmental pollution and the condition of the environment enjoys priority over safeguarding trade secrets"*[8].
In view of the fact that the municipality wished to sell a protective zone designated for the intensive protection of drinking water supply – naturally dependent on the result of the procedure for obtaining a water rights permit – the public interest in the accessibility of the data supporting the municipality's decision concerning the purchase-and-sale was of particular significance in the Authority's view, hence it called upon the municipality to comply with the data request. The municipality acted as called upon, hence the requesting party had access to the requested data. [NAIH-1387/2023.]

In another case, the subject matter of the notifier's data request was the expert opinion, on the basis of which the trees were cut down on Siófok's Silver Beach. The controller, a limited company, rejected the data request based on Section 27(5) of the Privacy Act. According to their position, it was to be feared that the inappropriate publication of the data could either impede the implementation of the decision or make it substantially more difficult and they wanted to avoid any disruption to the works. The Authority established that the data request was answered one day after the trees were cut down. On the day of the submission of the data request, it could have been an acceptable justification for restricting accessibility that "*in other cases, it occurred several times in Hungary that certain individuals attempted to physically prevent the implementation of such decisions*". The decision on the restriction of accessibility was made after the trees

8 Szekszárd Court of Appeal 13.Pf.20.706/2014/6.

were cut down, i.e. after the implementation of the decision. The balancing test according to Section 30(5) of the Privacy Act must be carried out even when restricting the accessibility of data supporting decision-making based on Section 27(5)-(6) of the Privacy Act. The extraordinarily significant public interest in the accessibility of environmental data should have been included with a decisive weight in the balancing test carried out by the company after the trees were cut down, because the decision was made after the cutting of the trees. The company complied with the Authority's call and issued the requested data to the requesting party. [NAIH-575/2023]

Similarly to previous years, the Authority examined non-compliance with the obligation to provide or to transfer information as set forth in Section 12(6) in the Environment Protection Act also in 2023. The requesting party asked for the results of measuring the level of air pollution ordered by a municipality of a city of county rights or any of its municipal companies, the evaluation of the results and the minutes containing these data from the municipality. The municipality justified the rejection by stating that it did not have the requested data at the time of granting the data request. It also stated that it did not transfer the data request to the organ holding the data, because as the principle of the measurement, the municipality as contracting party has a priority right preceding anyone else to access the measurement data. The Authority established that the municipality did not violate the notifier's right to access data of public interest when it failed to comply with the data request as it did not have the requested data, it had not yet received them from the organ carrying out the measurement. However, the municipality acted unlawfully when it failed to forward the data request to the organ holding the data and failed to provide information to the requesting party on the identity of the organ processing the data. According to Section 12(6) of the Environment Protection Act: *"If the contacted organ does not have the requested environmental information, it has to send the request concerning access to the information to the organ that has the environmental information and it has to notify or inform the requesting party about the organ holding the environmental information from which to request that information."*

Neither the Privacy Act, nor the Environment Protection Act contains any provision, which would exempt the organs originally receiving the data request from the obligation to provide information or transfer the data under certain conditions. According to the municipality's position, the data were not yet final, hence the requesting party could not be informed of who to turn to for the measured results of the level of air pollution as requested, nor was it possible to forward the data request to the company producing the data. The Authority informed the

municipality of its contrary position concerning access to raw environmental information. According to Section 51(1) of the Environment Protection Act: *"Data concerning the state and use of the environment should be processed according to the legal regulations concerning data of public interest."*

This means that raw data concerning the level of air pollution yet to be evaluated are also data of public interest because they concerned the state and use of the environment. It may happen that the evaluation or validation of the raw data leads to results different from the original data. It may be a genuine question whether data, which may still change, should be issued. Hungary is party to 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), which was promulgated by Act LXXXI of 2001. According to the implementation guide of the Aarhus Convention, the Compliance Committee of the Convention and the decisions of the European Court of Justice, the notion of environmental information is to be interpreted broadly. The Compliance Committee of the Aarhus Convention found in case ACCC/C/2010/53 that non-compliance with data requests concerning raw data violates Article 4(1) of the Aarhus Convention. According to the Convention, the notion of environmental information is broad, it is not limited to processed data. The Compliance Committee recommends that if an organ discharging public duties has doubts concerning the issue of raw data, they should notify the requesting party that the environmental information made available is raw data, they were not yet processed in accordance with the rules applicable to the processing of raw environmental data when they were issued. Therefore, organs performing environmental duties must issue raw air pollution data to the requesting parties. The Municipality should have forwarded the data request to the organ processing the raw data or it should have informed the requesting party about which organ processes the raw air pollution data. Naturally, the information could have included a warning that the evaluation of the data processed by the organ indicated has not yet been completed. [NAIH-4044/2023]

III.9. Matters of education, the transparency of public education

In 2023, the largest number of data requests was again submitted in relation to the phenomenon of teacher shortage. In addition to the transparency of education, the Authority attaches outstanding importance to taking other fundamental children's rights into account and emphasising them, hence the Authority takes the position that there is an outstanding public interest in accessing the data re-

quested in relation to this subject matter because of the children's right to education. The exploration of problems and challenges related to education affecting the entire society at systemic level and conducting a public debate on these issues are in the interest of the public, in the interest of children, and also in the interest of organs and persons performing public duties involved in educational decision-making.

III.9.1. Statistical data of teachers and vacancies in a school district

The notifier submitted a request for data of public interest to a School District Centre in Budapest, asking for the accurate number of full-time and part-time teachers, teachers of retirement age and retired teachers in a breakdown by age, school subject and educational institution, as well as the number of vacancies unfilled on the first day of the academic year in a breakdown by subject and educational institution. The data request also extended to the number of teachers dismissed in one of the high schools on 30 September 2022, the teachers' teaching qualifications and the impact studies related to their dismissal and the documents supporting decision-making drafted in-house in this context. The investigation revealed that the school district failed to comply with the data request because of an error in administration, but later, after an extension of the deadline, it issued the data it processed to the requesting party. [NAIH-3968/2023]

Parents and parents' organisations pay particular attention to the issue of whether teachers of adequate qualifications teach the students and stand in in classes. The notifier posed questions to the School District Centre concerning the issue of teacher shortage, which partially refused to comply with the data request invoking Constitutional Court Decision 13/2019. (IV. 8.) AB. In the case of the institutions of public education maintained by the school district, the data requested included, among others, the permitted number of the teaching staff, the teaching positions filled in, the number of persons pursuing educational and teaching activities without a tertiary teaching degree and the permanent substitutions (overtime work) assigned to teachers. The request for data of public interest also included questions on how many classes did not have a class breakdown according to the pedagogical programme because of vacancies or the employment of teachers without the necessary qualifications and how many classes were held without professional substitution in the institutions in academic year 2021/2022 based on KRÉTA records.

In the context of the Constitutional Court decision invoked, the Authority underlined that performing simple sums does not qualify as the generation of new,

qualitatively different data. This Constitutional Court decision cannot be applied as an automatic reason for rejection, because the data can be produced without physically finding the requested data one by one, the data are electronically available, and the generation of new, qualitatively different data, explanations and conclusions beyond the data already processed are not needed for compliance with the data request. Compliance with the data request necessarily requires some labour which, however, is concomitant with ensuring the fundamental right to access data of public interest by the institution. Accessibility may be restricted only at the level of the law for the protection of interests specified in the Privacy Act; considerations of convenience may not constitute a basis for rejecting the data request. The requested data – which the requesting party only requested as statistical data without names – are accessible also as personal data accessible on public interest grounds for each teacher. No matter on the basis of what legal regulation or legal relationship teachers are employed, the responsibilities, jobs and other personal data linked to the performance of public duties of each of them is accessible on the basis of Section 26(2) of the Privacy Act.

As to the issue of substitution, the Authority's position was that if, in addition to performing his job, a teacher has to carry out tasks that are part of somebody else's job for a transitory period based on the order of the employer, this affects his tasks, job and performance of public duties, which are also data accessible on public interest grounds based on Section 26(2) of the Privacy Act. Also in the case of teachers substituting for others, the data concerning their qualifications are definitely data accessible on public interest grounds based on Section 26(2) of the Privacy Act, even if the employer of the substitute teacher is another institution. This means that with reference to Section 26(2) of the Privacy Act, requesting parties are entitled to have access to the identity, education and qualifications of substitute teachers.

Beyond requests to access individual data of public interest, another method of accessing data of public interest and data accessible on public interest grounds is the electronic publication obligation of organs performing public duties, in this case, the educational institutions. Pursuant to Section 23 of Government Decree 229/2012 (VIII. 28.) on the implementation of the Act on National Public Education, educational institutions have to publish data on the education and qualifications of teachers, the number of teaching assistants, their education and qualifications based on the jobs filled, on the dedicated site of KIR, as well as on their websites. Requesting parties can find out whether substitution was documented as professional or non-professional in two different ways. If they only wish to have access to summary data, for instance, on the ratio of profession-

al/non-professional substitutions on a given day/week/month, the institution is under an obligation to issue the data as data of public interest. If, however, the data is requested with regard to a specific teacher, as it is personal data, it will be accessible as personal data accessible on public interest grounds based on Section 26(2) of the Privacy Act. In the case of a teacher standing in for another, the fact whether he is standing in as a teacher specialising in the given subject or not, hence the substitution be considered as professional or non-professional, also qualifies as other personal data related to the performance of public duties. It is a separate issue whether, despite the fact that a teacher is substituted by a non-specialist teacher, the institution still books the substitution as a professional substitution. Such data are also accessible as data of public interest because that too is a recorded data processed by the school regarding its activities. As a result of the Authority's call, the School District issued the data it processed, while the requesting party was referred to the respective institution with regard to data whose exclusive controller was the institution of public education concerned. [NAIH-7384/2023]

III.9.2. Accessibility of teachers' education and qualifications

Another notifier wished to know whether the five special needs teachers named in his data request had the remedial educator or conductor qualifications adequate to the type and severity of his child's special needs and what kind of legal relationship the remedial educator had with the school. The Authority took the position that with reference to Section 26(2) of the Privacy Act the requesting party is entitled to have access to the identity and the qualifications of the teachers whether they have the specialised qualifications adequate to the type of special educational needs, the tasks they perform, the tasks they were entrusted with, the contract of assignment itself and, if any, the relevant invoices as well. The Authority also explained that the Privacy Act does not know the notions of personal request for data or data request for private interest. If the subject matter of the data request is data of public interest and data accessible on public interest grounds specified under Section 3(5)-(6) of the Privacy Act, the request qualifies as request for data of public interest, irrespective of the objectives and circumstances of the person requesting the data or of the data request. Such objectives and circumstances cannot be examined when complying with the data request, nor can they constitute an impediment to issuing data, which are otherwise accessible. According to the Authority's position, the use of the personal data accessible on public interest grounds requested in procedures before courts or authorities complies with the principle of purpose limitation. [NAIH-8522/2023.]

III.9.3. The transparency of applications for public education development, accessibility of contracts

The subject matter of another submission was access to all the contracts concluded by the municipality and generated in the course of administering the application for the "*Development of the natural science methodology and instruments of János Arany Primary School and High School*". In this case, both the School District Centre and the Municipality declared that they did not manage the contracts. While under investigation by the Authority, the School District stated that they did not receive the contracts desired to be accessed from the Municipality (they only got them on CD, which was damaged and the documents on them could not be downloaded), hence the School District Centre did not have the requested contracts in its possession either electronically, or signed on hard copy, or in an editable electronic file. According to the answer of the Municipality, the operation of institutions of public education, including the János Arany Primary School and High School, became tasks of the school district as of 1 January 2017, based on legal regulation. Because of this, the performance of tasks related to the application referred to was the responsibility of the School District Centre. In view of the fact that scrapping has not taken place according to Decree 78/2012. (XII.28.) BM on issuing the uniform archiving schedule of municipal offices, the municipality sent the contracts related to the administration of the application to the requesting party by e-mail as a result of the Authority's procedure. [NAIH-3967/2023.]

III.9.4. Accessibility of the division of school subjects

In a request for consultation, it was asked whether school subject divisions could be requested from the School District in a request for data of public interest. According to the Authority's position, the school subject division contains data of public interest and personal data accessible on public interest grounds. Once the school subject division is prepared, it is managed by the school and, after 15 August, by the school and the operator of the school. However, not all data of public interest are accessible. This means that prior to approval by the operator, the document may qualify as a document supporting decision-making according to Section 27(5)-(6) of the Privacy Act, just as is the case after approval, if the data also supports future decision-making, or if access to it would jeopardise the lawful functioning of the organ performing public duties or the performance of its functions and powers without undue external influence. However, in each case, the organ performing public duties has to make reference to the circumstance that restricts accessibility. Based on Section 28-30 of the Privacy Act, the

– approved – school subject division may be requested from the School District. [NAIH-6234/2023]

III.9.5. Issue of the data of class sizes and regular child protection benefits

In another case of consultation, a statement was requested whether a school district is under an obligation to issue data of how many children attend individual junior classes of a primary school and altogether how many children receive regular child protection allowance (hereinafter: RGYK) in the individual classes of the individual grades. It was also asked which organs process the data concerning regular child protection allowance. Earlier, the School District issued the number of children attending the individual classes; however, they stated concerning the regular child protection allowance that they are not controllers with regard to these data and that in their view, a given natural person (student) can be traced back and identified from the cumulated statistical data. The Authority took the position that the cumulated statistical data, which do not contain personal data, are data of public interest, access to which may not be restricted by the provisions of Sections 28-30 of the Privacy Act. Based on the provisions of Act XXXI of 1997 on the Protection of Children and the Administration of Guardianship, the guardianship administration, the municipality or the operator process the data concerning the data on regular child protection allowance with regard to any child. The guardianship administration establishes entitlement to the regular child protection allowance, hence the primary controller of these data is the guardianship administration, so requests for data of public interest with regard to these data should be submitted to the guardianship administration. The municipality and the educational institution itself can provide information on data related to school meals. Since, in practice, tasks related to catering and invoicing are carried out by the educational institution or a local service organisation, (or other organisation providing for public meals or school meals), these organs and organisations also process data on entitlement to meals at preferential rates, hence they are under an obligation to fulfil requests for data of public interest. (A request for data of public interest may also be submitted to the municipality, the school district or the school for the identification for such an organisation.) In the case under investigation, the School District processed the data concerning the regular child protection allowance, while the guardianship administration or the municipality do not process the data on which child attends which class, so they would not be able to answer some of the questions posed in the data request. [NAIH-6566/2023]

III.9.6. Data supporting class division

The Authority took the contrary position in a case when a data request was made for accessing the data supporting the division of class in an anonymous statistical statement. With regard to each student of two classes, the sex, age, place of residence, average study score in the preceding year, the foreign language studied was separately asked for each student and also whether the student benefitted from the regular child protection allowance, whether the student was underprivileged, particularly underprivileged and whether the student had an individual study plan. According to the Authority's position, compliance with a data request of this kind could violate the individual student's right to the protection of personal data, because in this way the individual students could be identified (e.g. if the place of residence of only one student is in a given settlement or the age of only one of them differs from that of the others, etc.) Because of this, the data requested can be accessed only in cumulated form for each class and not separately for the individual students. [NAIH-8194/2023.]

III.9.7. Transparency concerning the E-kréta breach

With regard to the data breach affecting the internal IT systems of eKréta Informatikai Zrt., Educational Development Informatikai Zrt. (because of the change in the name of eKréta Informatikai Zrt. on 20 April 2023) informed the Authority that the company notified every controller of the data breach affecting the company, including the fact that the data breach affected not the KRÉTA system but only the internal IT systems of eKréta Informatikai Zrt. in the form of a message on the "*notice board*"[9] used in the Kréta system. Under its investigation, the Authority established that the company violated the notifier's rights to the protection of personal data and access to data of public interest (two data categories requested) when it has failed to answer the notifier's letter concerning the exercise of data subjects' rights and request for data of public interest since 13 November 2022. When dealing with the large number of requests received in connection with the data breach and due to the workload on the company, they unfortunately failed to answer the notifier's letter. The Authority appreciated the company's argument that it was not in a position to answer certain questions for reasons of data and information security as access to this information and/or their disclosure to the public could greatly increase data security risks and could contribute to malicious activities by persons/organisations planning unauthorized attacks/intrusions. [NAIH-4794/2023]

9 The text of the message was recorded in the data breach report sent by eKRÉTA Informatikai Zrt. on 10.11.2022.

III.9.8. Public evaluation of institutions of public education

In response to a notification submitted in relation to a kindergarten evaluating website, the Authority informed the notifier that having examined the website, the Authority did not find any unlawfully disclosed personal data and the identification and access data of the kindergarten shown in the website objected to corresponded to the data shown on the oktatas.hu website and the kindergarten's own website. The Authority has no powers to take action concerning the publication of opinions on the kindergarten, as such opinions and evaluations belong to the sphere of freedom of expression; the courts have powers to take action in relation to them based on the Acts on the Civil Code and the Criminal Code. [NAIH-8645/2023]

III.9.9. Tertiary education – the accessibility of theses

In one of the cases on tertiary education, the Authority responding to the consultation question of the data protection officer of a university explained its position concerning the accessibility of theses, having invited the opinion of the Ministry of Culture and Innovation (KIM). The regulatory environment changed substantially in 2022 – it is no longer an autonomous decision of the institutions of tertiary education how they publish theses; they must be made accessible without restriction to anyone with regard to theses made after 28 May 2021. According to KIM, the term "without restriction" means that a person wishing to have access to a thesis must not face unreasonable difficulties or costs. An institution of tertiary education may enable access and searchability in other suitable ways, for instance, through a computer installed in its library, if the thesis is otherwise stored in the study system; the rules generally applicable to the use of the library (opening hours, eventual reasonable fee payment obligation for non-students) do not qualify as restrictions. According to the Authority's position, the right to access may be restricted to inspection only in view of the right to intellectual property; the person wishing to access a thesis may not request the institution to make a copy of the paper. [NAIH-5259/2023.]

III.9.10. Contracts concluded by the operator

A notifier objected to the fact that although he submitted a request for data of public interest to the Foundation for […] University asking, inter alia, about the purchase price that the Foundation paid for the […] Medical Center Kft. and the […] Medical Invest Kft., which remained unanswered within the period open for this and beyond.

According to the Authority's position, the foundation as an entity funded from public funds, managing public funds and performing public duties is subject to the scope of the Privacy Act. A trust foundation with a public-service mission (hereinafter: KEKVA) is an organ performing public duties in every case both with a task-oriented and an asset-oriented approach. The assets that KEKVA manages and increases are public assets. Therefore, the Foundation's capacity as an organ performing public duties can be established unconditionally and in every case with an asset-oriented approach. With regard to data of public interest, those subject to the obligation to inform have to do so equally because they perform public tasks and because they manage public funds. In the course of the Authority's investigation, the Foundation declared that although the Foundation was the operator of the University, the University and the Foundation were two separate legal entities and they qualify as two separate controllers with regard to processing data of public interest. It was not the Foundation, but the University that was involved and acted in the legal transaction concerning the purchase of the exclusive business of the Kft., and the indirect property of […] Medical Center Kft., therefore only the University has the data concerning the transaction and the University is the controller. Unfortunately, however, the Foundation failed to notify the requesting party of this fact in a lawful manner and simply left the data request without response. As a result of the Authority's investigation, the Foundation forwarded the data request to the competent organisational units of the University. [NAIH-5650/2023]

III.10. The transparency of the judiciary – data accessibility practice of the courts, MBVK and bailiffs

Among the submission received this year, some consultation submissions affected the courts and complaints against the *Hungarian Association of Judicial Officers*.

III.10.1. Submissions concerning the courts

A consultation request concerning the accessibility of court judgments asked whether a judgement and its justification could be made public without names and addresses with a view to informing the membership of a trade union. The Authority took the position that the statements made by the persons concerned in a court procedure, the testimony they gave, their behaviour in the case at issue (an incident involving wrangling) and the fact that the court qualified their testimony as "*questionable*" are all data, which are not related to their perfor-

mance of public duties, particularly when, as employees, they do not act within the scope of the functions and powers of the organ (e.g., janitors, security guards). The data of a court procedure, which in themselves cannot be associated with natural persons, qualify as data of public interest so long as the data do not/could not become personal data, i.e. a natural person cannot be associated with or by the data and his right to informational self-determination is not infringed through it, or its direct threat cannot arise (e.g., the case number of the lawsuit). A problem may arise from the connection of the data, which enables the identification of natural persons. The connection of an anonymised court decision with natural persons in any way – for instance, by disclosing the name of the respondent company in order to indirectly infer the identity of the persons involved in the lawsuit – would already amount to data processing, which is subject to the objective scope of the GDPR. [NAIH-9453/2023]

It is worthwhile to mention a case of investigation, in which the notifier initiated the investigative procedure of the Authority because a court rejected compliance with his request for data of public interest for sending copies of answers to requests for data of public interest submitted to the court during a given period. The Authority pointed out that upon receipt of the request for data of public interest, the court considered, in view of the provision in the first sentence of Section 86(1) of Decree 14/2002. (VIII.1.) on the rules of court administration (hereinafter: Court Administration Decree), whether the notifier can be regarded as an interested party in accessing the data of public interest, is contrary to the social purpose of the fundamental right because, according to Section 29 of the Privacy Act, *"anyone"* can request data; the controller may not examine his identity or the purpose of requesting the data. In several of its published decisions, the Curia held that the petitioner's request for issuing "documents" related to himself does not constitute a request for data of public interest as it does not and cannot serve the transparency of public affairs, and therefore it does not meet the requirements for a request to access data of public interest. (Pfv.IV.20.419/2021/6., published in: BH2022.16., Pfv.IV.21.269/2022/5., Pfv.IV.20.008/2023/4.) Under Section 1(2) of the Court Administration Decree, its rules are to be applied in the absence of different provisions of separate legal regulations, in view of which the Authority stated that it should be considered in each case whether a different provision of a legal regulation should govern the given case, or the provision of the Court Administration Decree under investigation. The Authority pointed out that in its view it may be established that the restrictive rules in the provisions of Section 86(1) of the Court Administration Decree do not at all govern the granting of requests of data of public interest, i.e. with regard to data of public interest,

because the Privacy Act sets forth different provisions concerning the accessibility of the documents.

Even if the provisions of Section 86(1) of the Court Administration Decree were applicable, these provisions should be applied in view of the provisions of Section 1(3) of the same decree, which requires compliance with the provisions of the Privacy Act in the course of case administration. A different interpretation of the law would lead to the conclusion that the president of the court should decide on granting a request for data of public interest within his discretion according to the last sentence of Section 86(1) of the Court Administration Decree, but the president of the court would naturally be bound by the provisions of the Privacy Act concerning compliance with requests for data of public interest in the course of his deliberations. This means that the president may only refuse to comply with the request for data of public interest, if the reasons for refusal according to the Privacy Act obtain, i.e. similarly to the head of any other organ performing public duties, he may carry out the deliberations only within the provisions of the Privacy Act.

In both of the above interpretations of the law, the president of the court has the discretion to decide whether to grant or reject the request for data, but he may only make his decision on the basis of the provisions of the Privacy Act and not by disregarding them, i.e. not exclusively on the basis of Section 86(1) of the Court Administration Decree. Based on all this, the Authority called upon the court to comply with the data request, which the court did. [NAIH-7830/2023]

III.10.2. Judicial enforcement

This year, again, the Hungarian Association of Judicial Officers (MBVK) was the controller in most cases related to the judiciary. MBVK regularly disputes the positions taken by the Authority supervising the enforcement of the right to access data of public interest, it fails to meet the Authority's calls, or fully leaves its requests unanswered. Unfortunately, most of the cases affecting MBVK end up in court, where the requesting party can have access to the data of public interest desired since the judgment of the court can be enforced through the coercive power of the state. The chapter on court decisions details the court judgments concerning MBVK as respondent in cases related to the freedom of information.

The subject matter of a complaint affecting MBVK was the list of grants and expenditures for the development of MBVK's information systems annually be-

tween 2016 and 2022 and the list of its contracts concluded since 2017 amounting to at least five million forints net.

MBVK rejected the disclosure of the data by stating that it does not keep records on the distribution of the development costs of its various IT systems in an annual breakdown. They stated that they could not comply with the data request as that would require the generation of new data. MBVK rejected the request to issue the list of contracts concluded since 2017 of at least five million forints net and the list of companies with which it concluded contracts in excess of five million forints in 2021 and 2022, declaring that they do not record the requested data as "collected data".

The Authority consistently held that the performance of simple IT queries and mathematical operations (sums) do not qualify as the generation of new data and ordering them in a table does not qualify as "*the generation of new records*". To comply with the data request constituting the subject matter of this case, there is no need to exceed the level of simple IT, mathematical or other operations that do not present any substantial difficulty. Therefore, MBVK has to answer the questions posed in the data request concerning their financial management and spending. The Authority also opined that the data of public interest desired to be accessed would provide important information also for the Hungarian society, promote the transparency of MBVK, whose reputation has been tarnished by corruption and criminal procedures and strengthen public confidence in the functioning of MBVK, the Hungarian state and the judiciary.

With reference to court judgment 69.P.22.423/2023/3, MBVK informed the Authority that it had sent the list of its contracts of at least one million forints net concluded since 2017 in a structure required by the data request. They also stated that they never received any grants to develop their IT systems and with regard to the amounts spent on the development of IT systems, they insisted that the provision of the requested data would involve not merely sums and deductions, that they did not have these data and to comply with the data request, they would have to label all their supplier invoices and wage-type costs in their books, i.e. they would have to indicate the purpose for which any given cost item was used. [NAIH-44-2023.]

In another case affecting MBVK, the requesting party wished to access the data, which would reveal which bailiff positions were vacant at the time of the data request and since when and for how long individual bailiffs have been in their positions.

MBVK informed the requesting party that he can search an up-to-date register of the currently authorised independent bailiffs on mbvk.hu/nevjegyzek. If a position is vacant, an independent bailiff temporarily designated to perform the task takes action as substitute bailiff. In these cases, the person authorised to take action is shown as follows: XY permanent substitute (title of assignment) instead of YX independent bailiff. In addition, they also sent the link to a summary Excel table available under the menu "*Addresses of bailiffs' offices*".

MBVK rejected the part of the data request asking about the date of assigning permanent substitutes, stating that these data are processed in the public register according to Section 250/A(5) of Act LIII of 1994 on Judicial Enforcement (Judicial Enforcement Act). MBVK held the view that based on Section 28(8) of the Privacy Act, the general rules of requests for data of public interest cannot be applied to provide data from the authority records; data from these records may be provided in a manner regulated in a separate act. In view of the fact that the Judicial Enforcement Act only provides for the obligation to forward data as a sectoral rule for cooperating organs with powers to supervise compliance or performing tasks of an authority or court, and according to Section 33 of the General Administrative Procedures Act, a third person may inspect the records if he verifies that his access to the data is necessary for the enforcement of his rights or meeting his obligations based on legal regulation or decision of a court or an authority, the data request in this matter cannot be complied with in MBVK's opinion.

The Authority could not accept the statements made by MBVK in the course of its investigation and it declared in its call that the vacancy of bailiff positions is data of public interest under Section 3(5) of the Privacy Act, while the date of the assignment of permanent substitutes is data accessible on public interest grounds based on Sections 3(6) and 26(2) of the Privacy Act. As the name of the permanent substitute and the date of his assignment qualify as other personal data related to the performance of the public duties of bailiffs, they are accessible as data accessible on public interest grounds. The vacancy of bailiff positions constitutes data of public interest in the service of the transparency of public affairs that are important for public opinion, whose accessibility is not part of providing individual data from the register.

The position of the supervisory organ of MBVK, the Supervisory Authority for Regulated Activities (SZTFH) was also that the data listed in Section 250/A(2) –

except for those specified in Section 250/A(1) of the Judicial Enforcement Act – can be issued when requested.

According to the Authority's position, information concerning data of public interest or data accessible on public interest grounds cannot be refused stating that the requested data otherwise constitute part of a public register. (Similarly, accessibility of data concerning national assets, real estate and business quotas held by the state or a municipality cannot be excluded with reference to the trade register or the land register as public registers, etc.)

In view of the fact that the positions of the Authority and of MBVK have not come any closer with regard to the accessibility of the data constituting the subject matter of this case, the Authority called upon the Supervisory Organ of Regulated Activities to conduct an investigation whether MBVK interprets the relationship between the Judicial Enforcement Act and the Privacy Act in accordance with the legal regulations. Furthermore, the Authority issued a recommendation to the SZTFH, inter alia, on the fact that, as independent bailiffs (and substitute bailiffs) are persons exercising public authority and performing public duties, a law (preferably the Judicial Enforcement Act) should clearly state that they are under the subjective scope of Chapters III and IV of the Privacy Act and they are subject to all the obligations related to the freedom of information, to which organs performing public duties are subject in general (making data of public interest and data accessible on public interest grounds accessible based on individual data request and the publication of data of public interest in accordance with the general publication scheme set forth in Annex 1 of the Privacy Act – expediently on the website of MBVK). [NAIH-5145/2023]

MBVK rejected the issue of data citing similar reasons also in a case inquiring into how many cases were assigned to the individual bailiffs in the independent case assignment system and exactly which bailiffs' offices were supervised in 2019, 2020, 2021 and 2022 and what were the results of these supervisions. In this case, MBVK also stated that the data request was self-serving, however, the Authority resolutely deemed that the data request submitted by the requesting party was not self-serving, it fully met the social purpose of exercising the right to access data of public interest. The corruption and criminal procedures involving MBVK naturally give rise to a great deal of interest on the part of the public, resulting in the public's demand for increased transparency in the operation of MBVK. In the course of its investigation, the Authority found that MBVK processed the data of the independent case assignment system and it should be able to determine by using simple IT query operations how many cases were as-

signed to the individual bailiffs and how many cases were reassigned from the logged data, the electronic public register and the central register of judicial enforcement cases.
MBVK did not state how long these logged data are retained but the fact that it failed to comply with the data request since 30 May 2022 has definitely caused a substantial encroachment on the rights of the requesting party to access data of public interest by infringing the requirement of timeliness and also because of the limited retention period of the data it processes, if some of the data had already been erased.

The responses by neither MBVK, nor SZTFH revealed any justification for restricting accessibility, on the basis of which the data request could be rejected. This means that if the data are electronically available and can be retrieved from the databases processed by MBVK using simple IT query operations, the request for data of public interest must be complied with. To comply with the data request, it suffices, if the data sought in the data request can be queried in MBVK's IT systems; the data request may not be rejected stating that MBVK "*does not keep such records*".

The fact and the results of supervision involving bailiffs qualify as other personal data related the performance of public duties by the bailiffs pursuant to Section 26(2) of the Privacy Act, hence they are accessible as data accessible on public interest grounds. The requesting party did not ask for access to the full documentation of investigations, supervisory reports or disciplinary procedures, together with the personal data of the persons participating in judicial enforcement procedures and those concerned in such procedures as MBVK interpreted. The data request can be complied with just by answering the question of the requesting party by issuing the personal data of the bailiffs accessible on public interest grounds without issuing the personal data of the other participants of judicial enforcement or of the full documentation.

In Hungarian law on transparency, the data principle applies instead of the document principle: under Section 30(1) of the Privacy Act, if a document containing data of public interest contains also data to which access by the requesting party is not permitted, the data that must not be accessed shall be made unrecognizable on the copy, i.e. the issue of the entire document cannot be refused with reference to the fact that it also contains data that must not be accessed.

Contrary to the view of MBVK the fact that sectoral regulation does not set forth an obligation to disclose the audits carried out by MBVK does not mean that the

relevant data would not be accessible and issuable as data of public interest. In view of the fact that the positions of MBVK and the Authority have not come any closer even after the Authority's third call, unfortunately the requesting party has to turn to the courts also in this case in order to have access to data of public interest, which is according to the Authority's position accessible to anyone. [NAIH-4488/2023]

This year, there was a case in which MBVK interpreted the notifier's request for data of public interest as an exercise of data subject's rights.

In his request for data of public interest, the notifier wished to learn how many complaints were submitted to MBVK, because the bailiff failed to return the full auction deposit to unsuccessful bidders after the completion of the auction or its cancellation over the past five years, in a breakdown by years. MBVK interpreted the data request as a request for exercising the data subject's right to access under Article 15 of the GDPR and informed him that on 10 March 2023, he was not shown as a debtor in the electronic public register kept on cases of judicial and administrative enforcement administered by independent bailiffs according to Section 253/E(1) of Act LIII of 1994 on Judicial Enforcement. In the course of the Authority's investigation, MBVK declared that it interpreted the request for data of public interest as exercise of the right to access because of "*an administrative error arising from a filing mistake*" and following the receipt of the Authority's letter, it rectified the erroneous provision of data for the notifier. [NAIH-8721/2023]

The concerns of the Authority related to the portal used by MBVK to comply with data requests are detailed in a separate subsection of the report on this issue.

III.11. Other organs performing public duties, NGOs performing public duties, organisations providing public services

The Authority published information on the organs that are subject to the scope of the Privacy Act accessible through the link https://infoszab.hu/node/183 on the website https://infoszab.hu/, which was created as a result of priority project entitled ADMINISTRATIVE DEVELOPMENT OPERATIONAL PROGRAM"-2.2.6.-COMPETITIVE CENTRAL HUNGARY OPERATIONAL PROGRAM-2019-00001 "SURVEYING AND IMPROVING THE EFFICIENCY OF THE DOMESTIC PRACTICE OF THE FREEDOM OF INFORMATION". This information was published in view of the fact that the Authority received a substantial number of notifications every year on non-administrative organisations

performing public duties and/or managing public funds because certain business organisations held by the state or municipalities, other non-profit organisations backed by the state or municipalities, public bodies, public foundations and institutions of tertiary education failed to meet requests for data of public interest because in their view, the provisions of the Privacy Act governing compliance with requests for data of public interest do not apply to them.

The Authority found the following in relation to requests for data of public interest submitted to a limited company (hereinafter: Ltd) functioning as the sole shareholder of a foundation (hereinafter: Foundation) founded by the state subject to Act IX of 2021 on Trust Foundations with Public-service Mission (hereinafter: Trust Foundations Act).

Based on the data in the trade register, the Hungarian state used to be the sole shareholder of the Ltd; then, the Foundation became the sole shareholder of the Ltd. The Foundation performs public duties according Annex 1 to the Trust Foundations Act, it is founded with public funds, it manages public funds and performs public duties, hence it is subject to the Privacy Act. The same applies to the Ltd, as it was also founded with public funds, it has been managing public funds and it is involved in the performance of public duties to be carried out by the Foundation. In view of this, it is the Authority's position that if the Ltd receives a request for data of public interest and the company processes the data requested, it has to comply with the data request; if, however, the data request submitted to the Ltd is for data which can only be found in possession of the Foundation, the company has to provide information about the identity of the controller. [NAIH-5917/2023; NAIH-7325/2023]

In another case, a company also failed to comply with a request for data of public interest for sending copies of contracts concluded by and between the company and the Foundation, because in their view, they did not qualify as an organ performing public duties under the Privacy Act. The Authority pointed out that the Foundation's church background was irrelevant, because it performed public duties though its activities, while the company was involved in the performance of this public task through the contract concluded with the Foundation. The financial background for the company's operation stems not only from its commercial activities, but partly from performing the contracts concluded with the Foundation. According to the Authority's position explained in this case, it was not necessary to "transfer" the public duties from the Foundation to the company, it suffices that the company collaborated in the performance of the public duty for

having to make the data related to the performance of the public duties available to the requesting party based on the Privacy Act. [NAIH-5436/2023]

In another case, the Authority pointed out with respect to a Foundation that pursuant to Section 2(6) of Act III of 1993 on Social Governance and Social Benefits (hereinafter: Welfare Act), the development and provision of the framework of operation for the system of welfare institutions and measures are tasks of the state and of the municipality. When performing their duties related to providing the conditions of welfare care, the state and the municipality cooperate with church organisations and NGOs. Pursuant to Section 120 of the Welfare Act, a municipality may provide welfare services or services to enforce the right to rest also by way of contracts of care concluded with church organisations, other non-state organs, church or non-state operators. A Foundation was authorised through a contract of care concluded with a municipality to operate a home for the elderly providing comprehensive care for them in a property held by the municipality whereby the Foundation took over the performance of this municipal task. In the course of providing welfare services, the municipality and the Foundation – the latter up to its tasks taken over from the municipality based on contract – are under an obligation to guarantee the enforcement of the freedom of information, i.e. to make data of public interest and data accessible on public interest grounds accessible to anyone. In view of all this, the Authority called upon the Foundation to comply with the request for data of public interest. [NAIH-86/2023]

In the context of a data request lodged with another Foundation, the Authority agreed with the Foundation that the requesting party misinterpreted a legal regulation, which was the reason for his opinion that the Foundation inadequately complied with his data request. The reason for this is that the framework agreement specified under Section 20(1) of the Trust Foundations Act is not the same as the contract financing public duties under Section 18(1)(e) of the same act. Finally, the Foundation sent copies of both agreements to the requesting party. In the same case, the Authority established in the context of compliance with a data request for decisions of the Board that the Foundation violated the requesting party's right to access data of public interest when it wished to ensure access to them exclusively by way of inspection stating that the decisions also contained data concerning its commercial and business activities. The Authority pointed out that the accessibility of full documents cannot be restricted under the document principle and the requesting party is entitled to request a copy of the documents according to Section 29(3) of the Privacy Act in view of its Section 30(1). [NAIH-29/2023]

A company rejected a request for data of public interest submitted concerning the use of a priority state sports facility asking for the detailed presentation of the revenues of the facility for several years in a breakdown by events and the detailed presentation of warranty repairs, citing its market interests and possible competitive disadvantage. The Authority pointed out that, in general, reference to a competitive disadvantage is inacceptable in the context of the utilization of facilities operated by the state. There is an outstanding interest in learning what revenues result from the utilisation of facilities operated by the state. If the company is worried that the requesting party would incorrectly evaluate the revenue data by themselves, it has the opportunity to send supplementary information, so as to enable the requesting party to evaluate the totality of the data made available to him and develop his position in this way. Drawing correct or, according to the controller, incorrect conclusions from the data may not influence the controller in issuing or withholding information. The company has to disclose all the data available to it in a recorded form on warranty repairs even if the value of the warranty repairs is not included in its records, given that the repairs were carried out under warranty. [NAIH-46/2023]

Certain public transportation companies performing public duties did not comply with requests for data of public interest asking for daily and ad hoc reports (hereinafter: reports) citing various reasons for rejection. [The reporting obligation towards the Transport Safety Body (hereinafter: KBSZ) is imposed on the companies by Act CLXXXIV of 2005 on the Technical Investigation of Aviation, Railway and Marine Accidents and Incidents, Act CLXXXIII of 2005 on Railway Transportation and Decree 24/2012. (V.8.) NFM on the detailed rules of the technical investigation of serious railway accidents, railway accidents and unexpected railway incidents and of the operator's examination.]

In the opinion of one of the companies, the daily reports do not include data of public interest as, in terms of extraordinary events, they contain information related to several railway companies, undertakings and natural persons who cannot be associated with the state. The Authority found that the company qualifies as an organ performing public duties, the daily/ad hoc reports produced by it are held by the company and they relate to its activities and, furthermore, they were generated in the context of performing public duties, consequently they contain data of public interest.

The companies also stated that the reports were internal technical documents, work documents and they qualify as correspondence with KBSZ. According to the Authority's finding, the requested documents were clearly not work docu-

ments, they were not made for internal use as they were sent to KBSZ. Sending the reports could not be regarded as correspondence as legal regulation requires that they be drafted and sent, they were not drafted in a letter format and they contained data of merit required by legal regulation.
The controllers also cited that the reports supported decision-making as they contained data required for the companies' procedures, used for drafting the railway safety strategy, the annual testing schedule and the development of the business plan and their content also appeared in the documents on investigating accidents. The Authority pointed out that for this restriction to comply with constitutional requirement, the relationship between the data supporting decision-making and the future decision must be specific and direct, an abstract relationship to a decision cannot serve as a reason for restricting freedom of information.

One of the controllers stated that the reports were available in a format, which also included personal data. The Authority called attention to the provisions of Section 30(1) of the Privacy Act, according to which, if a document containing data of public interest contains also data to which access by the requesting party is not permitted, the data that must not be accessed shall be made unrecognisable on the copy. The Authority pointed out that the name and the unit dispatcher making the notification indicated in the reports, the railway safety duty officer and the person receiving the report on the part of KBSZ qualify as data accessible on public interest grounds, which can be disseminated if the principle of purpose limitation is respected. In view of the fact that the data request was for the content of the reports and not the persons making and receiving the notification, in view of the purpose-limited processing of personal data accessible on public interest grounds, the Authority recommended the blocking of the names of the notifier and the recipient in the documents. However, the Authority also called the attention of the company to the fact that if a data request is expressly aimed at the names of the notifier and the recipient, it is necessary to issue the required information calling on the requesting party to abide by purpose-limited processing. [NAIH-4613/2023; NAIH-4615/2023; NAIH-4529/2023]

In another case, the notifier initiated an investigation by the Authority in view of the rejection of a data request for accessing an internal auditor's report closing an internal audit launched because of the delayed commissioning of a renewed facility. The controller answered the data request stating that all the current communications, news and information of the controller are available on the website, but the answer did not include any internet link and according to the finding of the Authority – which the controller also acknowledged – the requested data

were accessible on the website. Then, the controller cited that they did not identify the notifier's letter as a request for data of public interest, in view of which the Authority called the controller's attention to the need for assessing requests according to their content. After the Authority's call, the controller rejected the data request with regard to the entire document citing Section 27(5) and (6) of the Privacy Act. The Authority then pointed out that: first, the two reasons for rejection exclude one another, second, it is not permitted to cite these reasons in general, and third, the entire document cannot be qualified as data supporting decision-making. According to the repeated statement, the controller rejected the request in view of Section 27(6) of the Privacy Act, because issuing the results of the internal audit to be accessed would jeopardise the performance of its functions and powers without undue external influence, in particular, the free expression of its views during the preparatory stage of decision-making concerning "various" renewals and investments. This means that in their repeated statement, the controller again cited "various" future decisions in general, they were unable to justify that access to the various data one-by-one would jeopardise their lawful operation or performance of their functions and powers without undue external influence, in view of which the Authority did not accept the controller's answer. [NAIH-1279/2023]

Another company (hereinafter: controller) rejected compliance with requests for data of public interest concerning the operation of two of its terminated offices (financial management data, labour situation) also with reference to Section 27(6) of the Privacy Act and trade secrets. As, according to the controller's statement, the financial data are accessible in the reports published on its website and the company provided the Authority with the requested information concerning the financial data and the data on the labour force not published on the website and gave reasons acceptable from the viewpoint of restricting the freedom of information and provided justification for the necessary and proportionate restriction of the freedom of information, the Authority accepted the controller's answer and terminated the investigation based on Section 53(5)(b) of the Privacy Act. [NAIH-961/2023]

In his request for data of public interest submitted to a company pursuing media activities (hereinafter: controller) the requesting party asked for the sound recording of an interview of a mayor broadcast live on a radio channel (hereinafter: sound recording). As grounds for rejection, the controller argued that the sound recording of the broadcast enjoys protection under copyright against its use by the requesting party with an unspecified purpose and content, possibly by highlighting certain parts of the text in a different context. In response, the Authority

pointed out that an organ or person performing public duties may not examine the purpose of the data request, hence it cannot be rejected on the grounds of the potential use of the data provided to the requesting party. The controller also cited that some of the broadcast information did not relate to the performance of the mayor's public duties and were not accessible on public interest grounds. The Authority pointed out that when meeting requests, the data principle is enforced, which means that the parts of the sound recording with regard to which there are justified reasons for excluding access as substantiated by the controller had to be edited or distorted by the controller prior to disclosure. The controller also argued that, with the possible editing of the sound recording, the content structure of the interview would be damaged, as a result of which the information in it would be distorted. The Authority pointed out that the Privacy Act – in view of the enforcement of the data principle – does not recognise damage to the integrity of a document, in this case a sound recording, as an impediment to access data of public interest or data accessible on public interest grounds. In view of all this, the Authority called upon the controller to meet the request for data of public interest in accordance with the requirements of the Privacy Act, and if the sound recording to be accessed also contains data subject to a restriction of access, those should be removed from the sound recording and the requesting party should be informed of the reasons for such removal. After this, the controller notified the Authority that according to Section 155(10) of Act CLXXXV of 2010 on Media Services and Mass Communications, it had to retain the sound recording for 60 days, hence in line with the controller's practice it might have been erased during the procedure in progress before the Authority; however, this did not take place as a sign of its bona fide action. According to its notification, the controller following the Authority's call ensured wider access than that required by the call and published a sound recording at a URL address accessible to anyone; however, after two weeks of accessibility it finally erased it. However, the controller failed to notify either the requesting party or the Authority of having made the sound recording public. In view of the above, the Authority issued a report concerning the controller's infringement of the freedom of information because the controller not only failed to grant the requesting party's fundamental right to access data of public interest or data accessible on public interest grounds, but it made it impossible to have any access to the data to be accessed by the requesting part. [NAIH-2665/2023]

III.12. Consultative procedures

III.12.1. Access to data of public interest generated while exercising the powers conferred on a mayor

A citizen requested information from the Authority whether a municipal representative of the settlement or the body of representatives may request specific information and regular reports from the mayor on the relevant procedures conducted by him if the body of representatives delegates its powers defined in Act LXXIV of 2016 on the Protection of the Visual Environment of Settlements to the mayor by municipal decree.

The Authority informed the petitioner that Section 42 of Act CLXXXIX of 2011 on Local Governments of Hungary (hereinafter the Municipalities Act) provides for the non-transferable powers of the body of representatives. However, according to Section 41(4) of the Municipalities Act, "*the body of representatives may delegate its powers to the mayor, its committee, the body of the sub-government, the municipal executive, its association, with the exceptions provided for in this Act. It may give instructions for the exercise of these powers and it may revoke these powers.*" In the Authority's view, therefore, if the body of representatives wishes to request information or a report from the mayor on the procedures carried out by the mayor in the field of applying the instruments for the protection of the visual environment of the settlement, it may lawfully do so. [NAIH-5605-2/2023]

III.12.2. Making video and audio recordings at the meetings of municipal representatives

The Authority was asked in a consultation submission for its opinion on making video recordings of public meetings of the body of municipal representatives. The Authority is of the opinion that participation in public meetings of the body of representatives or committees and in an official capacity constitutes appearance in public within the meaning of Section 2:48(2) of the Civil Code, which does not require the consent of the person concerned for making and using the recording under the legal provisions quoted. Similar treatment applies to third persons who may speak at a public meeting, such as invited persons, persons concerned and the audience itself. It should also be emphasised that pursuant to Section 46(1) of the Municipalities Act, the meetings of the body of representatives are open to the public. Derogation from this may only be possible pursuant to Section 46(2) and (3). Section 52(1) and (2) of the Municipalities Act, minutes

shall be taken of the meetings of the body of representatives, which minutes shall be signed by the mayor and the municipal executive. The minutes constitute a public document. The following provision is also contained in Section 46(3): *"The voters may inspect the proposals and minutes of the meetings of the body of representatives, except in the case of closed meetings. The opportunity to inspect data of public interest and data accessible on public interest grounds shall also be provided in the case of a closed meeting. The decision of the body of representatives taken in a closed session shall also be public".* Pursuant to Section 2(2) of the Municipalities Act, local self-government expresses and implements local public will in local public affairs in a democratic manner by creating broad publicity. This includes the right to make visual and/or audio recordings and that the participants must tolerate the making of visual and/or audio recordings at the public meetings of the body of municipal representative and at the committee meetings.

The events of the public meetings of the body of representatives and the committees, as well as the minutes, visual and audio recordings of the meetings constitute data of public interest and data accessible on public interest grounds, which may be accessed by anyone, pursuant to Section 3(5) and (6) of the Privacy Act. Therefore, from the point of view of freedom of information, the minutes and the visual and/or sound recordings are treated in the same way, i.e. they are public and may be published on the Internet or on bulletin boards. Statements made by the municipal representatives at a public session of the body of representatives, as well as other personal statements, are also public statements, so in the case of public sessions, the contributions are also public. [NAIH-3232-2/2023]

III.12.3. Access to payment vouchers for a person performing public duties

An applicant has repeatedly requested information from the Authority on whether a municipal executive of a large village has lawfully refused to respond to a request for data of public interest. The complainant requested the Mayor's Office to send an electronic copy of the receipt for the repayment of the funeral allowance to the Office's cashier, indicating the legal title for the repayment. The municipal executive refused to reply to the request for data of public interest, on the grounds that the data requested did not constitute budgetary support within the meaning of Section 1(14) of Act CXCV of 2011 on Public Finances (hereinafter the Public Finances Act) and were therefore not data accessible on public interest grounds. The Authority has provided information on the fact that Section 179 of the civil Servants Act classifies the personal data of a government official as data accessible on public interest grounds. The amount of regular, ad hoc, cash

and in-kind benefits paid to managers, such as allowance in lieu of leave, bonuses, substitution payments, earnings supplements and special benefits, are personal data generated in connection with the performance of public duties, and can be accessed by anyone, so the controller is obliged to fulfil this part of the data request, broken down as requested. However, the allowances provided under Section 152(1) of the Civil Servants Act are paid to the government official by the organ performing public duties with regard to events and life situations that may be related to the private sphere, so they may only be disclosed in a breakdown by name with the consent of the persons concerned and, therefore, in the absence of consent, they may only be disclosed in aggregate form, as data of public interest related to the management of the organ performing public duties. Following the consultation response, the complainant initiated an investigation procedure. [NAIH-9371/2023]

III.12.4. Grating access to and disclosing asset declarations

A citizen asked the Authority whether it was lawful for the municipality not to send him a copy of the declaration of assets of the municipal representatives and the mayor in response to his request for data in the public interest, but he would have been given access to review the requested documents at a pre-arranged time.

In the Authority's view, pursuant to Section 29(3) of the Privacy Act, the notifier may receive a copy of a document or part of a document containing the data, regardless of the mode in which it is stored. The organ performing public duties that handles the data may set a reimbursement for the fulfilment of the data request up to the amount of the costs incurred in connection with the request, if the costs incurred exceed the lowest amount of the reimbursement set in the Government Decree, provided that the amount of the reimbursement so set may not exceed the highest amount set in the Government Decree. The amount of the reimbursement and the options for fulfilling the request for data not requiring copying shall be communicated to the notifier within 15 days of receipt of the request.

With a view to Section 29(3) of the Privacy Act, it is only possible to fulfil a request for data of public interest by inspection if it is accepted by the applicant. However, the Authority also drew the complainant's attention to the fact that, pursuant to Section 29(1a) of the Privacy Act, the organ performing public duties that handles the data is not obliged to comply with the part of the data request which is identical to a data request for the same data set submitted by the same

applicant within one year, provided that there has been no change in the data in the same data set. [NAIH-6676/2023]

III.12.5. The mayor's representation account

Has the municipal executive acted lawfully when he did not send the data requested by the notifier as requested? The complainant requested the disclosure of the costs of representation for a specific period in a table format, broken down by year, indicating the issuer, date and amount of the invoice or receipt. The municipal executive did not reply in the form, with the breakdown and the data content requested, within the legal deadline.

The Authority informed the complainant that, as this concerns the use of public funds, transparency and verifiability are of paramount importance as a matter of public interest. At the same time, freedom of information and the right to informational self-determination must be enforced in relation to each other, so in determining the scope of other personal data relating to the performance of public duties [Section 26(2) of the Privacy Act], it must be taken into account whether their disclosure would not disproportionately infringe the right to privacy. The amount of regular and ad hoc benefits paid to managers in cash and in kind, such as allowance in lieu of leave, bonuses, substitution payments, earnings supplements and special allowances, are personal data generated in connection with the performance of a public duty and can be accessed by anyone, so the controller is obliged to fulfil this part of the data request, broken down as requested. [NAIH-7093/2023]

III.12.6. Right of access to data by municipality representatives in the context of financial management

Two municipal representatives asked the civil servant of the branch office to make copies of all the bank account statements and related documents of the municipality for the period from January to September 2023 and to hand them over to them. The request for a decision was to ask whether a copy of the full financial documentation could be released to the representatives and, if so, under what conditions or with what restrictions. Also, an objection was made to the fact that the representatives made their request for data orally to the civil servant and not to the mayor "*in accordance with the provisions of Section 32(1)(f) of Act CLXXXIX of 2011 on the Municipalities of Hungary*".

In the Authority's view, pursuant to Section 32(2)(b) of the Municipalities Act, a municipal representative may request information on matters of the municipality from the mayor (deputy mayor), the municipal executive and the chairman of the committee, to which a substantive reply must be given at the meeting of representatives or in writing within thirty days at the latest, and he may request information necessary for the work of the representative from the mayor pursuant to Section 32(2)(f). In matters of public interest, he may request the mayor to take action, to which he must reply in substance within thirty days.

The mayor is therefore obliged to give the representative a substantive answer to the questions addressed to him in accordance with the law, and in the event of failure to do so, the competent Government Office exercising legal supervisory powers pursuant to Section 1(2) and 127 of the Municipalities Act may initiate measures pursuant to Section 132 of the Municipalities Act.

On the other hand, under the provisions of the Privacy Act, municipal representatives have no extra rights, i.e. they can access data of public interest or data accessible on public interest grounds under the same conditions as anyone else. Personal data, with the exception of personal data accessible on public interest grounds, cannot be disclosed to them at all in the absence of a legal basis. In the present case, it is not the right of access to data of public interest that has been infringed, but the specific right of access of municipal representatives, as detailed above. In the light of the foregoing, the Authority is not entitled to determine the scope of the right of access of municipal representatives, it is a matter for the Government Office to assess. [NAIH-8976-2/2023]

III.12.7. Access to extracts from the general ledger of a publicly owned company

A municipal representative submitted a complaint to the Authority because a company wholly owned by the municipality failed to comply with its requests for data of public interest concerning the company's general ledger extracts and general ledger files for the years 2021 and 2022, which he considers to be entitled to receive as a municipal representative, as he would be able to review the company's financial management in detail on the basis of the requested data.

Pursuant to Section 30(7) of the Privacy Act, the provisions of separate laws apply to the disclosure of data for the purpose of comprehensive, account-level or itemised audit of the financial management of organs performing public duties. In the present case, the Authority came to the conclusion that the data in question, which, according to the notifying party's declaration, was also requested in order

to obtain full knowledge of the financial management of the company, constitute a comprehensive, itemised audit as it covers the entire financial management of the company over two years. Since the request for data must be fulfilled pursuant to Section 30(7) of the Privacy Act only if the request can be distinguished from the checks on the expediency, efficiency and legality of the financial management of organs performing public duties – since separate bodies are entitled to carry out such checks – the Authority found it lawful to reject the request for data of public interest. The full text of the resolution is available on the website. [NAIH-6367-2/2023]

III.12.8. Criminal information that may be provided by the mayor

The mayor of a municipality requested information from the Authority on the lawful way of informing the body of representatives and the public. In 2019, after his election, a series of indications of misappropriation were uncovered in the Office, and the municipality filed a report against an unknown perpetrator. According to the District Court, a former employee of the Office was convicted of the crime of continuous embezzlement and the former mayor and his associates were charged by the District Prosecutor's Office with the crime of budget fraud causing substantial financial loss.

Section 179 of the Civil Servants Act classifies the name and other personal data of a government official as public data accessible on public interest grounds. The freedom of information and the right to informational self-determination must be enforced with respect to each other, so when determining the scope of other personal data in connection with the performance of a public task [Section 26(2) of the Privacy Act], it must be taken into account whether their disclosure would not disproportionately infringe the right to privacy. The Authority also drew the Office's attention to the fact that, where another person is involved in the proceedings or in the judgment at first instance, disclosure of personal data beyond those generated in the context of the performance of the public task of the person performing the public task and of personal data relating to a third party is unlawful. In providing information and disclosing data, attention should also be paid to whether judgments have become final, whether the processing and disclosure of personal data accessible on public interest grounds in the course of ongoing proceedings does not violate the presumption of innocence, and to the necessity and proportionality of the processing of personal data of the data subjects. The responsibility for the lawfulness of the processing of personal data lies with the controller (the person who takes and implements the decision) and it is not replaced by a position of the Authority.

While the information provided to the body of representatives – in the case of a closed meeting – can be considered as *transmission of data*, the information provided to the public constitutes *disclosure of data*. It follows from the above that in the case of a request for data of public interest, the Office is obliged to process and provide information on the data it holds in accordance with the relevant provisions of the Privacy Act and the GDPR. [NAIH-9210/2023]

III.12.9. Use of images, exercise of data subject rights in the context of freedom of the press

A citizen requested information from the Authority regarding a complaint about data processing by the editorial board of a major news portal, in which the Authority did not launch an investigation and the notification was rejected without examining the merits of the case on the basis of Section 53(3)(a) of the Privacy Act in view of the pending legal action concerning personality rights.

A natural person's face, likeness, image and audio and video recordings of him or her are personal data and their collection, recording, storage and use (including publication) constitute processing. As the complainant is clearly identifiable in the video footage in question, the editorial board is processing data. The Authority recommended that, in respect of the processing complained of, the complainant should contact the controller (the publisher) in a justifiable manner under Article 21 (right to object) of the General Data Protection Regulation and request that his/her image be made unrecognisable, stating his/her reasons. If the controller does not comply with or refuses the data subject's request, he or she may lodge another complaint with the Authority. [NAIH-6297/2023]

III.12.10. Those subject to publication obligation in the Central Information Register of Public Data

It was raised as a consultation question whether the obligation to provide data on the website of the Central Information Register of Public Data applies to companies held by municipalities – as business entities which perform public duties that are not listed in the general register of the Hungarian State Treasury but in the trade register.

The Authority pointed out in connection with the case that the publication obligation applies to all budgetary bodies except the national security services. Consequently, it does not apply to non-budgetary bodies, i.e. only budgetary bodies are subject to the obligation to publish specific financial management data

on a bi-monthly basis on the newly created Central Information Register of Public Data (hereinafter "the Platform"). The method and content of the publication are set out in Section 37/C of the Privacy Act and in Government Decree 499/2022 (XII. 8.) on the detailed rules of the Central Information Register of Public Data. The publication obligation applies to data generated on or after 29 November 2022. The Authority also pointed out that a company listed in the trade register may perform public duties, but it is not a budgetary organ under Act CXCV of 2011 on Public Finances (Act on Public Finances), and therefore, based on the provisions of the Central Information Register of Public Data established under Chapter 24/B of the Privacy Act, it is not a body required to publish data on the Platform. In view of this, it is not required to publish data of public interest relating to its financial management in this area. However, it is important that the obligation to publish on its own website or on the website of its supervisory body or on the central website (kozadat.hu) [Section 33(3) of the Privacy Act], as well as the obligation to publish under Act CXXII of 2009 on the more economical operation of publicly owned companies, continues to apply to companies performing public duties, as was the case previously. [NAIH-1221-2/2023]

III.12.11. Retention period of a disclosure unit on financial management

A university requested the Authority's views in its submission for consultation on which legislation defines the retention period for disclosure items 2 and 6 of disclosure unit III. Financial management data of the General Disclosure Schedule. According to the Authority's position, neither Annex 1 of the Privacy Act, nor Decree 18/2005 (XII. 27.) IHM contain any provision on the retention period of the data disclosed in the disclosure units indicated in the submission. With regard to the retention of disclosed data of public interest and data accessible on public interest grounds, the Authority is of the consistent opinion that the transparency of the operation of an organ performing public duties is facilitated if not only current data of public interest and data accessible on public interest grounds are disclosed, but data previously disclosed remain accessible in the disclosure scheme by keeping the data in the archive. The Authority drew attention to the fact that requests for data of public interest may be submitted for archived data even after one year from the date of disclosure, which the data controller is obliged to comply with according to the provisions of the Privacy Act. In the case where the data to be accessed are available in the archive of the general disclosure scheme, the data request may also be lawfully fulfilled by sending a link to the data in the archive. [NAIH-1588/2023.]

III.13. Authority procedures for the supervision of classification in the field of the freedom of information

III.13.1. Authority procedure for the supervision of classification in connection with the classification of the investigation report based on OBHE Decision 6.Sz/2022 (I.28.) on the targeted investigation of the Metropolitan Court of Budapest

Transparency International Hungary Foundation brought an action before the Metropolitan Court of Budapest against the National Office for the Judiciary (hereinafter: OBH) *for the disclosure of the investigation report based on OBHE Decision 6.Sz/2022 (28.I) on the targeted investigation to be conducted at the Metropolitan Court of Budapest, as well as any other documents or data containing the findings of the persons appointed to conduct the targeted investigation, their conclusions or positions in connection with the targeted investigation*.

The OBH, as the respondent in the litigation, stated that the *'any other documents or data containing the findings of the persons appointed to carry out the targeted investigation, their conclusions or positions in connection with the targeted investigation'* subject to the request for data and referred to in the petition do not exist, because *they are contained in the investigation report based on OBHE Decision 6.Sz/2022 (28.I) of 28.I. on the targeted investigation to be carried out at the Metropolitan Court of Budapest*, referred to in point 1 of the petition.

The president of the OBH classified the referenced investigation report as "Restricted" national classified information with a validity period of 10 years. In view of this, he refused to comply with the data request on the basis of Section 27(1) of the Privacy Act. The Metropolitan Court of Budapest initiated the authority procedure for the supervision of classification with regard to the lawfulness of the classification of the data subject to the litigation.

As a result of the authority procedure for the supervision of classification, the Authority established the breach of the following with regard to the classification of the report generated in the course of the targeted investigation ordered by Decision 6.SZ/2022.(I.28.) OBHE pursuant to Section 63(1)(a) of the Privacy Act;

- Section 5(1) of the Classified Data Protection Act[10],
- Section 5(3) of the Classified Data Protection Act,
- Section 6(1), (2), (3) and (4) of the Classified Data Protection Act and
- Section 38(3) of Government Decree 90/2010. (III.26.) on the Roles of the National Security Authority and the Handling of Classified Information, therefore it called upon the classifier to terminate the classification in accordance with Section 63(1)(a)(aa) of the Privacy Act.

Pursuant to Section 63(2) of the Privacy Act, the Authority applied a repeated classification marking with regard to the content of the justification of the decision in view of the possibility of legal remedy against the decision adopted in the authority procedure for the supervision of classification and its suspensive effect. As the decision was challenged by the classifier in an administrative appeal, which is still pending, the classification still stands. [NAIH-503/2023]

III.13.2. "Pseudo" authority procedures for the supervision of classification

According to the essence of Section 31(6a) of the Privacy Act, if the controller refuses to grant a request for access to data of public interest because the data of public interest or data accessible on public interest grounds cannot be disclosed because it is classified data under the Classified Data Protection Act, and the data subject goes to the court for review of the refusal to disclose the data of public interest, the court shall initiate an authority procedure for the supervision of classification by the Authority. Pursuant to Section 62(1a) of the Privacy Act, if the court initiates an authority procedure for the supervision of classification as defined in Section 31(6a), the Authority shall initiate the authority procedure for the supervision of classification. Therefore, the Authority has no discretionary power to initiate proceedings under the provision of Section 62(1a) of the Privacy Act, and if the court initiates the launch of the authority procedure for the supervision of classification on the basis of this provision, the Authority is obliged to initiate the procedure. It follows from Section 62(1) of the Privacy Act that the Authority may, in the course of its authority procedure for the supervision of classification, examine the lawfulness of the classification or the repetition of the classification marking of national classified information, i.e. in order for the procedure to be conducted, there must be classified information which has been created prior to the procedure and which can therefore be examined as to the lawfulness of the classification. If classified information exists, there must also be a classifier (or a person repeating the classification marking), since classified information can be

10 Act CLV of 2009 on the Protection of Classified Information

lawfully created as a result of the classification procedure. Only the classifier (or the person repeating the classification marking) can be a client of the authority procedure for the supervision of classification before the Authority.

It is important to emphasise the above because the Authority has recently received several submissions in which the court initiated the launch of authority procedure for the supervision of classification with reference to Section 62(1a) of the Privacy Act, but based on the examination of the transcripts sent by the courts and the attached documents, it was likely that no classified data had been generated in the main case before the procedure was initiated. In these cases, although the Authority found that the conditions for starting the authority procedure for the supervision of classification – such as the existence of classified information and the existence of a classifier – were not met, it had to start the authority procedure for the supervision of classification as it had no discretion.

In the course of the fact-finding it was established that, in the cases referred to, there was no classified data among the data that were the subject of the litigation, therefore the continuation of the authority procedure for the supervision of classification became pointless due to the lack of classified data, therefore the Authority decided to terminate these authority procedures for the supervision of classification pursuant to Section 47(1)c) of the Act on General Administrative Procedures.

In these cases, the Authority was therefore obliged to initiate authority procedures for the supervision of classification in the absence of classified information, i.e., it had to initiate and conduct the procedure despite the fact that there was no national classified information to be examined. In the absence of classified information, it would also be meaningless to identify the classifier (or the person repeating the classification marking), who is the client of the authority procedure for the supervision of classification.

The number of such “pseudo” procedures for the supervision of classification would presumably be reduced by interpreting the provisions of Section 62(1) and (1a) of the Privacy Act in the same way as intended by the legislator. In applying these rules, the starting point is that the data which are the subject of litigation before the courts under Section 31(6a) of the Privacy Act include classified data and that it is likely that the classification of these national classified data or the repetition of their classification marking is unlawful. According to the Authority’s position it is only under these conditions that the initiation of a procedure for the supervision of classification by the courts on the basis of Section 62(1a) of the Privacy Act can be interpreted. The purpose of the authority procedure for the

supervision of classification initiated under Section 62(1a) of the Privacy Act is not to establish whether the data which are the subject of the litigation contain classified information at all, but to establish whether or not the classification of the national classified information designated by the court or the repetition of the classification marking is unlawful. The Authority considers it important to call attention to the fact that in cases where a court has initiated the launch of authority procedures for the supervision of classification, it is for the court to determine as precisely as possible the scope of the classified information to be examined in the context of the authority procedure for the supervision of classification. [NAIH-7114/2023]

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

2023 saw important developments in terms of international and EU law – we are providing an update on these in the renewed international cooperation section of the NAIH website.

For the third time since its establishment, the Hungarian DPA invited the EU DPAs to Budapest on 10-12 May 2023 for the so-called Spring Conference (https://springconference2023.hu/). Altogether, 138 accredited representatives from 39 countries registered for the closed sessions (covering new technologies, competition law and data protection, decisions of the Luxembourg and Strasbourg courts and good practices), while 358 external participants (including for the first time Hungarian DPOs, with a special focus on the DPOs' key issues) registered for the open day. The Conference adopted three resolutions on the need for enhanced cooperation with competition authorities, on the accreditation of the San Marino DPA and on the revision of the Rules of Procedure of the Spring Conference.

The drafting of procedural regulation to complement the GDPR is still in progress in the EU; it will only detail procedural rules for cases involving cross-border data processing, for example guaranteeing stronger procedural rights for parties, in particular the right to make a statement. At the same time, significant progress has been made in the context of the EU digital package.

IV.1. Digital sovereignty and the digital strategy of the European Union

IV.1.1. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a single market for digital devices and amending Directive 2000/31/EC

[(Digital Services Act, DSA), in force from 16 November 2022, generally applicable from 17 February 2024]

The DSA aims to ensure a safe, predictable and trustworthy online environment; its immediate predecessor is Directive 2000/31/EC on electronic commerce, which remains in force but the DSA supplements it with significantly expanded provisions. The Regulation applies to so-called 'intermediary services' such as ISPs, cloud hosting providers, messaging applications, online forums, but does not apply where the intermediary service is an integral part of another, non-intermediary service (such as Uber). Due to its horizontal nature, unlawful content is defined by separate EU and national norms, but intermediary service providers can be exempted from liability if they can prove that they acted in good faith and with due care. The service providers operating the online platform are not allowed to display advertisements based on profiling within the meaning of the GDPR to underage users and the use of special categories of personal data is also prohibited. Service providers can be sources of different social risks due to their size and form, so providers operating a giant online platform or a very popular online search engine (with more than 45 million users) are subject to specific rules. The designated digital service coordinator in Hungary is the National Media and Infocommunications Authority.

IV.1.2. Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724

[(Data Governance Act, DGA), in force from 23 June 2022, generally applicable from 24 September 2023]

The aim of the Regulation is to facilitate data-driven innovation, i.e. data sharing across strategic areas, sectors and EU countries, in order to harness the potential of data for the benefit of European citizens and businesses. The Regulation supports the creation of common European data spaces in strategic areas, involving private and public actors in sectors such as healthcare, environment, energy, agriculture, mobility, finances, manufacturing and public administration. The Regulation defines "data" as any digital representation or compilation of actions, facts or information, covering both personal and non-personal data. It also sets out the conditions for the re-use of data held by bodies in the public sector within the EU. New actors are data intermediaries and data altruism organisations. Data intermediary services are entities that establish commercial relationships for the purpose of data sharing between an unspecified number of data subjects and data owners on the one hand, and data users on the other. Data intermediaries enable the sharing of data of public interest provided by public bodies and facilitate access to data by businesses. They must notify the competent

authority of the EU Member State of their intention to do so before they start their activities. They must not use the data subject to their intermediary services for their own purposes and they must distinguish their data-sharing services from their other commercial activities. They must charge a fair price for their services. Data altruism organisations include all organisations that carry out activities related to voluntary data sharing, operate on a non-profit basis and are registered with the authorities of the competent Member State. These organisations may voluntarily disclose data for broader benefits of society, based on the consent of the data subjects. Such benefits include health research, combating climate change, improving mobility or improving the delivery of public services.

The Regulation established the European Data Innovation Board, which is an advisory body to the Commission. It works with the participation of the competent authorities of the Member States responsible for data intermediary services, the competent authorities responsible for the registration of data altruism organisations, the European Data Protection Board, the European Data Protection Supervisor, ENISA and Commission representatives, as well as the representatives of SMEs and those of relevant bodies in specific sectors. The Regulation also establishes new tasks for NAIH, as the tasks and powers assigned to the competent authority responsible for data intermediary services and the competent authority responsible for the registration of data altruism organisations are exercised by NAIH in respect of entities under the jurisdiction of Hungary, as defined in the Data Governance Act and the Privacy Act. The Authority, upon request of the data intermediary service provider, certifies with an official certificate that the registered data intermediary service provider complies with the conditions set out in the Data Governance Act. The Authority notifies the European Commission without delay of any changes to the registered data and of the cessation of the activity.

IV.1.3. Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and the amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828

[(Data Act, data sharing law in the translation of a previous draft) in force from 11 January 2024, most of its provisions are directly applicable from 12 September 2025]

As a “counterpart” to the Data Governance Act, it mainly regulates the sharing of data between private parties (B2B), in particular in the case of jointly gener-

ated data (such as Internet of Things-IoT). It sets obligations for the following data controllers:

- (i) those that sell a product or provide a service that generate or collect data within the European Union;
- (ii) which are legally obliged to provide data;
- (iii) in exceptional cases, public sector bodies and any data controller operating in the European Union, where public sector bodies request data from private sector data controllers for the purpose of managing a public emergency (e.g. flood, pandemic).

The Data Act specifies and extends the right of data portability under Article 20 of the GDPR in the case of personal data (but does not apply only to personal data). Access to data generated by products or services covered by the Data Act must be granted to the data controller at the request of the user who generated the data (in the case of personal data, the data subject), or to a third party designated by the user. Previously, access to these data was often limited to the producer or service provider, which significantly distorted free competition.

Supervision of the application of the Data Act in cases involving personal data is the responsibility of the national data protection authorities (in Hungary, the NAIH), while the designation of the competent authority for non-personal data requires national legislation, which is still underway in all Member States. The EDPS supervises the application of the Data Act in relation to the Commission, the European Central Bank and other EU bodies. Member State legislation still in the pipeline should also regulate the rules for the division of tasks and cooperation between other authorities acting under sectoral legislation and supervisory authorities.

IV.1.4. Draft of the Artificial Intelligence Act

(Legislation in progress, envisaged adoption: 2024)

Artificial intelligence (AI) is not a new legal institution that has come out of nowhere, it is merely a qualitatively new tool for data management and processing, including the processing of personal data, that will define the future. The difference – and the degree of risk – stems from the processing of large volumes of data at high speed and with hardly any human intervention. Both during the training phase of AI and during its operation, it is typical to handle a significant volume of data, including but not necessarily personal data. The pioneer-

ing European approach is to create a regulation that ensures the functioning of both the markets and the public sector, as well as the security and fundamental rights of individuals (the issue of supervision is still a matter of future legislative decision).

However, AI systems are not “ex lex” even today, as – inter alia – Recital 15 of the GDPR explicitly sets out the principle of technological neutrality in the regulation and Article 22 provides for the application of the GDPR to all automated processing.

The risk is that such an application, if not properly designed and applied, can easily become a “black box” about which no one can tell what exactly is happening inside, and this is particularly problematic when processing personal data. The transparency of data processing and the accountability of the data controller are important data protection requirements, which are mainly design issues and a responsibility of the system creator – among other things, the Act is intended to clarify the division of this responsibility among the different actors in the AI ecosystem (developer, importer, user, end-user). One of the hardest challenges for the legislator is the definition of AI, but it is important to note that even if the related data processing falls outside the scope of the Act, the provisions of the GDPR will still be enforceable.

EU legislation applies an unacceptable-high-constrained risk-based classification system, with different levels of risk accompanied by different rules and requirements. However, the list of prohibited and high-risk purposes of processing with AI is not exhaustive and it does not mean that unlawfulness or disproportionate risk of processing cannot be sanctioned under other legislation. Under both the new Act and the GDPR, the controller must be able to demonstrate effective compliance, among others, by guaranteeing the principles, a valid legal basis and data subject rights. The new rules are also likely to provide guidance on the qualification of controllers and in particular joint controllers, as the use of AIs is often the result of the involvement of several actors.

It is not yet clear what the status of the authority will be that will oversee compliance with the AI Act and how it will fit in with the numerous authorities set up as part of the EU’s digital package – this will require decisions and legislation both by the EU and the Member States. However, it is also expected that an EU-level body will be set up, including a representative from each of the designated authorities in the Member States, as well as representatives of civil society. Its role

will be to support the uniform application of the law and legal compliance, and to issue opinions.

Outside the EU, there are regulatory initiatives also that interact with each other – for example, the Council of Europe is working on a convention on AI, human rights, democracy and the rule of law, the content of which has many similarities with the draft regulation.

IV.2. Data protection related decisions of the Court of Justice of the European Union

Of the 18 judgments of the Court of Justice of the European Union (CJEU, Luxembourg) on data protection delivered in 2023, the Authority considers that several are of particular interest, and their conclusions are briefly presented below.

IV.2.1. Judgment of the Court of 12 January 2023 in Case C-132/21, NAIH v Budapesti Elektromos Művek (ECLI:EU:C:2023:2)

If the data subject exercises both their right to lodge a complaint under Article 77(1) of the GDPR and their right to judicial remedy under Article 79(1) of the GDPR, the supervisory authority and the court are obliged to examine the breach independently of each other and they may reach different results, because the procedures may be conducted in parallel in order to ensure a high level of protection for natural persons within the Union with regard to the processing of personal data. Parallel and independent remedies should not, however, jeopardise the effective exercise and protection of the rights guaranteed by this Regulation, and therefore it is for the Member States to lay down detailed rules in national procedural law governing the relationship between those remedies, in accordance with the principle of procedural autonomy.

IV.2.2. Judgment of the Court of 12 January 2023 in Case C-154/21, RW v Österreichische Post AG (ECLI:EU:C:2023:3)

Article 15(1)(c) of the General Data Protection Regulation should be interpreted as meaning that the right of access of the data subject implies that, where personal data have been or will be disclosed to recipients, the controller is, as a general rule, obliged to provide the data subject with the specific identity of the recipients. Exceptions include if the recipients cannot be identified or where the

said controller demonstrates that the identity of the specific recipients cannot be disclosed for reasons of protection, the data subject's request is clearly unfounded or excessive within the meaning of Article 12(5) of the GDPR.

IV.2.3. Judgment of the Court of 4 May 2023 in Case C-300/21, UI v Österreichische Post AG (ECLI:EU:C:2023:370)

The right to compensation provided for by the GDPR requires three conditions to be met: the breach of the Regulation, the material or non-material damage resulting from that breach, and the causal link between the damage and the breach. Thus, a breach of the provisions of the GDPR does not in itself confer a right to compensation.

According to the recitals of the GDPR, a breach of the Regulation does not necessarily entail damage and it does not always give rise to a right to compensation, as there must be a causal link between the breach and the damage sustained. As a result, a claim for damages is different from other remedies under the GDPR, in particular those that allow for the imposition of administrative fines and do not require verification of concrete damage. The right to compensation is not limited to non-pecuniary damage above a certain threshold of severity. The GDPR does not impose such a requirement and such a limitation would be contrary to the broad interpretation of the concept of "damage" adopted by the EU legislator. In addition, to link non-material damage to a threshold of severity would jeopardise the coherence of the regime introduced by the GDPR. The determination of the level of compensation is a matter for the legal systems of individual Member States, in particular with regard to the aspects that allow for full and effective compensation under the GDPR, while respecting the principles of equivalence and effectiveness.

IV.2.4. Judgment of the Court of 4 May 2023 in Case C-487/21, FF v Austrian DPA (ECLI:EU:C:2023:369)

The decision interpreted the first sentence of Article 15(3) of the GDPR literally, systematically and teleologically, which gives the data subject the right to request a copy of their personal data that are the subject of the processing. Although this provision does not contain a definition of "copy", the usual meaning is a reproduction or a true transcription of the original, i.e. a general description of the data subject to processing or a reference to the categories of personal data is not sufficient. As regards the purposes pursued by Article 15 of the Regulation, the Court of Justice stressed that the right of access granted by that

Article must enable the data subject to ascertain that the personal data relating to them are accurate and are being processed lawfully. So, in order to ensure that the information thus provided is easily understandable, it may be essential to reproduce extracts from documents, or even entire documents, or even extracts from databases, which contain, inter alia, the personal data which are the subject of the processing. In particular, where personal data are generated from other data or where these data are derived from free text fields, i.e. where there is no indication revealing information about the data subject, the context in which these data are processed is considered indispensable to allow the data subject to have transparent access to these data and to make the presentation of these data intelligible. Where there is a conflict between, the exercise of the right of full access to personal data on the one hand, and, the rights or freedoms of others on the other hand, the Court considers that a balance must be struck between the rights and freedoms in question. Wherever possible, the method of communicating personal data must be chosen in a way which does not infringe the rights or freedoms of others, but it must be borne in mind that such considerations must not have the effect of denying the data subject all information.

IV.2.5. Judgment of the Court of 22 June 2023 in Case C-579/21, JM v the deputy data protection officer, Finland (ECLI:EU:C:2023:501)

Article 15(1) of the GDPR does not grant a data subject the right to obtain access to information from the controller concerning the identity of employees of the controller who have handled access under the direction and in accordance with the instructions of the controller, unless that information is necessary to enable the data subject to effectively exercise the rights granted to them by the Regulation, provided that the rights and freedoms of those employees are also taken into account.

IV.2.6. Judgment of the Court of 26 October 2023 in Case C-307/22, FT v DW. (ECLI:EU:C:2023:811)

The controller is also under an obligation to provide the data subject with a first copy of the personal data which are the subject of the processing, free of charge, if the request is justified for a purpose other than that referred to in the first sentence of Recital 63 of the GDPR. The right to request a copy of the personal data which are the subject of the processing in the context of a doctor-patient relationship implies that the data subject should be provided with a faithful and intelligible reproduction of all those data. It is presumed that the data subject should be provided with a full copy of the documents in the medical records, including

– among others – the data referred to above, where the provision of such a copy is indispensable to enable the data subject to verify their accuracy and completeness and to ensure their intelligibility. In any event, as far as the health data of the data subject are concerned, this right includes the right to obtain a copy of the medical records containing information such as the diagnosis, examination findings, opinions of treating physicians and any treatment or intervention carried out on the data subject.

Article 23(1) of the General Data Protection Regulation does not allow for the adoption of national legislation which, in order to protect the economic interests of the controller, imposes the cost of the first copy of their personal data subject to processing on the data subject.

IV.2.7. Judgment of the Court of 7 December 2023 in Case C-634/21, OQ v Land Hessen

Article 22(1) of the General Data Protection Regulation must be interpreted as meaning that the automated determination by a company providing business information of a probability value based on an individual's personal data concerning that individual's ability to meet future payment obligations constitutes an 'automated individual decision' within the meaning of that provision, where the establishment, performance or termination of a contractual relationship with that individual by a third party to whom that probability value is communicated depends predominantly on that probability value.

IV.3. Activities of the European Data Protection Board

In 2023, the European Data Protection Board (Board, EDPB) adopted 12 guidelines on a wide range of topics, such as data breach notification, the recognition of deceptive patterns on interfaces of social media platforms, but of particular importance are Guidelines 04/2022 on the calculation of administrative fines under the GDPR and Guidelines 01/2022 on the right of access. All the guidelines are accessible in English or Hungarian on our website [11].

11 https://naih.hu/europai-adatvedelmi-testulet-edpb/edpb-iranymutatasai

IV.3.1. Guidelines 04/2022 on the calculation of administrative fines under the General Data Protection Regulation

The European Data Protection Board (EDPB) endeavours to harmonise the methodology applied by supervisory authorities in calculating the amount of fines. For this purpose, it adopted and issued for public consultation Guidelines 04/2022[12] These guidelines supplement the earlier guidelines on the application and setting of administrative fines (WP253)[13], which focuses on the valuation criteria to be taken into account when imposing a fine.

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

First, in accordance with Article 83(3) of the General Data Protection Regulation, the processing operations to be assessed and the interrelationship between eventual simultaneous infringements have to be determined. The second step is the identification of the starting point for the calculation of the amount of the fine according to the following criteria: the classification of the infringement in accordance with the General Data Protection Regulation, the severity of the infringement and the size of the undertaking. The third step is the evaluation of the aggravating and mitigating circumstances related to the past or present behaviour of the controller/processor and increasing or decreasing the fine accordingly. The fourth step is identifying the relevant legal maximums for the different infringements. Increases applied in the previous or subsequent steps may not exceed this maximum amount. Finally, it needs to be analysed whether the calculated final amount meets the requirements of effectiveness, deterrence and proportionality. The fine can still be adjusted accordingly, however without exceeding the relevant legal maximum.

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

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

In 2023, the Board took binding decisions in three cases, which are presented below.

IV.3.2. EDPB binding decision 1/2023 in the Meta case

The Irish Supervisory Authority, as the Lead Supervisory Authority (LSA), has submitted a request for a dispute settlement procedure under Article 65(1)(a) of the GDPR regarding a draft decision on the international transfers of personal data, in particular to the US, in connection with the Facebook service operated by Meta Platforms Ireland Limited ("Meta IE"). The objections to the decision of the Irish supervisory authority by the Austrian, French, German and Spanish supervisory authorities were deemed relevant and well-founded on the basis of Article 4(24) of the GDPR and EDPB Guidelines 09/2020 on Relevant and Well-Founded Objections. It is important that the dispute was only about the further remedial actions to be applied, as the objecting supervisory authorities concerned would have considered it necessary to delete or return to the user the data transmitted in an unlawful way, and to impose an administrative fine. In its decision[14] issued on 13 April 2023, the EDPB instructed the Irish authority to impose an administrative fine for breach of Article 46(1) of the GDPR, to take into account the aggravating circumstances under Article 83(2)(a), (b), (g) and (k) of the GDPR and provided that the basic amount of the fine should be set between 20% and 100% of the maximum amount of the fine that can be imposed, based on the Guidelines on the method of setting administrative fines, due to the gravity of the breach. The EDPB also instructed the Irish authority to include in its final decision an order that Meta IE cease processing, including storing, personal data unlawfully transferred to the US within 6 months.

IV.3.3. EDPB binding decision 2/2023 in the case of TikTok Ireland Limited

The procedure was initiated following a request by the Irish Supervisory Authority as the lead supervisory authority in relation to its draft decision on TikTok Technology Limited ("TTL") on its compliance with Articles 5, 12, 13, 24 and 25 of the GDPR in relation to the TikTok platform for the period from 29 July 2020 to 31 December 2020 ("relevant period"). The EDPB agreed with the German authorities that the registration and video-sharing practices used by TTL are not compatible with the principle of fair processing and therefore justified its identification as an infringement. Based on the Italian authority's objection, the EDPB expressed serious concerns about the effectiveness of the TTL's age verification

14 https://edpb.europa.eu/system/files/2024-01/edpb_bindingdecision_202301_ie_sa_facebooktransfers_hu.pdf

methodology (13 years of age or older) during the relevant period. After a thorough discussion of the issue, the EDPB concluded in a binding decision[15] adopted on 2 August 2023 that there was insufficient information available to assess this in the course of the procedure. In response to the EDPB's binding decision, the Irish supervisory authority amended its draft decision and, in its final decision[16], ordered TTL to bring its processing into compliance with the GDPR on the basis of Article 58(2)(d) of the GDPR, fined the controller for breach of the GDPR on the basis of Article 58(2)(b) of the GDPR and imposed a total fine of €345 million for the TTL's breaches.

IV.3.4. EDPB urgent binding decision 1/2023 in the case of Meta Platforms Ireland Limited

On 31 December 2022, the Irish supervisory authority issued Decisions IN-18-5-5 (Facebook Decision) and IN 18-5-7 (Instagram Decision) (together "the Irish Decisions"), in which it found that the legal basis – Article 6(1)(b) of the GDPR – used by Meta Platforms Ireland, which operates Facebook and Instagram, in relation to behaviour-based advertising, was inappropriate and it ordered Meta to bring its processing of these data in line with Article 6(1) of the GDPR within three months. The Irish decisions were based on the EDPB's binding decisions of 3/2022 and 4/2022, which were issued by the EDPB after dispute settlement procedures. On 5 April 2023, Meta informed the Irish authority and the Irish authority informed the supervisory authorities concerned that Meta would mostly base its processing in connection with behaviour-based advertising data from 5 April 2023, which was the last day of the period provided for in the Irish decisions, on Article 6(1)(f) of the GDPR instead of Article 6(1)(b). However, according to feedback from several supervisory authorities concerned, the reference to Point (f) was not lawful either and the Norwegian authority requested the Irish authority on 5 May 2023, in the context of the mandatory mutual assistance under Article 61(1) of the GDPR, to temporarily prohibit Meta from processing personal data relating to behaviour-based advertising based on Article 6(1)(f) of the GDPR in relation to Instagram and Facebook services and to provide information on how it was going to ensure the adequacy of the legal basis for processing by Meta. The Irish authority replied that it "cannot comply with the request", that it would be in a position to complete the assessment of Meta's compliance reports by the end of June 2023 and that it wished to wait for the so-called Bundeskartellamt judg-

15 https://edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-22023-dispute-submitted_en

16 https://edpb.europa.eu/our-work-tools/consistency-findings/register-decisions/2023/decision-matter-tiktok-technology_en

ment of the Court of Justice of the European Union, which was delivered on 4 July 2023 in CJEU Case C-252/21 (the judgment held that the processing of behaviour-based advertising cannot be based on Article 6(1)(f)). On 14 July 2023, the Norwegian authority issued an interim measure temporarily prohibiting Meta and Facebook Norway AS from basing their processing of behaviour-based advertising affecting data subjects in Norway on Article 6(1)(b) or (f) of the GDPR, so the interim measure was only applicable in Norway and was in force from 4 August to 3 November 2023. On 27 July 2023, Meta informed the supervisory authorities that it would base its processing of behaviour-based advertising on Article 6(1)(a) within three months, and it attached a timetable, clarifying it later (on 14 August) that it would make the transition by 24 November 2023. On 18 August 2023, the Irish supervisory authority shared with the supervisory authorities concerned its final position that Meta had not complied with the obligations contained in the Irish decisions. The Norwegian Supervisory Authority's request of 26 September 2023 for a binding decision to be issued in an emergency procedure concerned the adoption of a binding decision by the EDPB, as it considered that final measures should be adopted urgently.

On the basis of Articles 70(1)(t) and 66(2) of the GDPR, the EDPB adopted the following binding decision on 27 October 2023[17]: Meta IE's processing of data continues to infringe Article 6(1) of the GDPR by relying without basis and in breach of Article 6(1)(b) of the GDPR for the purposes of processing data relating to behaviour-based advertising, including data relating to the geographic location of users and data relating to users' response to an advertisement, and by relying without basis and in breach of Article 6(1)(f) of the GDPR for the processing of personal data collected through Meta's products for the purposes of behaviour-based advertising. As regards the existence of an urgent situation, the EDPB considers that it is clear that the urgent adoption of final measures was necessary due to the risks threatening data subjects' rights. In addition to the above, the failure of the Irish authority to provide the requested information within the one-month deadline under Article 61(5) of the GDPR, by failing to respond to the Norwegian supervisory authority's request for mandatory mutual assistance, made the presumption under Article 61(8) GDPR applicable in the present case, further supporting the need to depart from the normal course of the cooperation and consistency mechanism. In EDPB's view, the situation that arose required the adoption of additional corrective measures.

17 https://edpb.europa.eu/our-work-tools/our-documents/urgent-binding-decision-board-art-66/urgent-binding-decision-012023_en

The Irish supervisory authority complied with the EDPB's urgent final decision[18] 1/2023 in its final decision of 10 November 2023 by applying the instructions addressed to the Irish authority in the binding decision. In the meantime, Meta has shifted its processing of behaviour-based advertising to the consent of the data subject, in such a way that if the user consented to the display of such ads on Facebook and Instagram, they do not have to pay for the services, otherwise they have to pay a monthly fee (the so-called "pay or ok" model, which the EDPB started to examine in 2024).

IV.4. Review of the cooperation procedures conducted pursuant to GDPR

Since the application of GDPR beginning in 2018, the Authority has taken an active part in the cooperation procedures according to Article 60 conducted with the Member States of the EEA. The one-stop-shop procedure[19] serves the investigation of cases launched on the basis of complaints concerning trans-border processing or ex officio. Communication among the authorities related to the cooperation procedures is conducted via an interface specifically transformed for these procedures in the Internal Market Information System (hereinafter: IMI system). As an important step of this procedure, the authority in the Member State where the complaint against a controller pursuing trans-border processing is received (hereinafter: initiating authority) launches an Article 56 procedure in IMI to identify the lead supervisory authority and the supervisory authorities concerned. The initiating authority may presume the role of the lead supervisory authority on the basis of the controller/processor's centre of activity or single place of activity[20], which may accept or, with appropriate justification, reject the role[21]). In addition, the Member States in which the controller/processor does not have an operation centre or place of activity may designate themselves as authorities concerned, if the processing under investigation was likely to affect a large number of data subjects who are residents in their countries.

In 2023, the Authority received 672 cases from the authorities of other Member States through the IMI system. Of these, we were involved in more than 200 cas-

18 https://edpb.europa.eu/our-work-tools/consistency-findings/register-decisions/2023/enforcement-notice-matter-meta_en

19 GDPR Article 60

20 For controllers or processors not established in the Union under Article 27 of the GDPR.

21 Article 56(3) of the GDPR

es as an authority concerned, we acted as lead supervisory authority in 5 proceedings and we opened 12 of our own Article 56 proceedings.

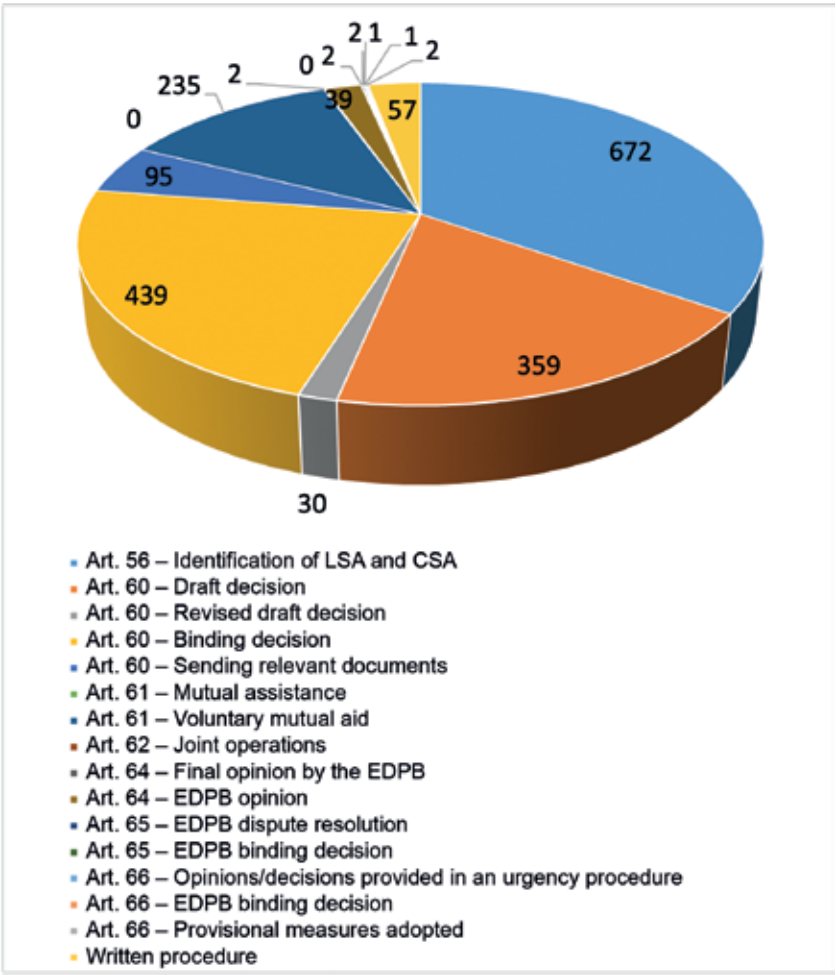


Figure 1: Procedures received by NAIH in 2023

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

Where a relevant and reasoned objection to the draft decision or a proposal for amendments is submitted by a supervisory authority concerned and the lead supervisory authority wishes to uphold the relevant and reasoned objection, it submits an amended draft decision to the other supervisory authorities concerned for them to comment on. Opinions concerning the draft amended decision are to be submitted within two weeks. In the case of mere proposals for amendments or comments, the lead supervisory authority is not obliged to amend its decision. The lead supervisory authority may modify its draft decision as long as all the authorities concerned accept it, after which it can be sent to all the Member State authorities in the form of a binding decision.

In 2023, the Authority received 359 draft decisions to be studied, 32 revised draft decisions, 439 final decisions and 50 requests for informal consultation facilitation cooperation under Article 60. During the same period, the Authority sent 3 draft decisions and 3 binding decisions to the other authorities under the cooperation procedure.

In the event that a lead supervisory authority disagrees with the relevant and reasoned objections of the authorities concerned, it may request that through a dispute settlement procedure according to Article 65, the Board resolve the conflict and decide on the disputed issues (no dispute settlement procedure has ever been launched against any draft decision by NAIH). In 2023, 2 such procedures were started against draft decisions by the Irish authority, the Board closed both procedures with a binding decision according to Article 65.

Cooperation procedures include mutual assistance procedures and voluntary mutual assistance procedures according to Article 61. While the former is a procedure subject to stringent formal requirements to be performed within a given period of time and generally conducted between two Member States, the latter is a more lenient procedure in terms of form and content, which the Member State authorities use, inter alia, for giving and obtaining information, expressing interest in relation to investigative procedures and general consultation. In 2023, the Authority received 235 requests for mutual voluntary assistance, and none for

mutual (mandatory) assistance. In the same period, the Authority initiated 48 mutual voluntary assistance procedures.

Some topics of keener interest:

- The issue of video recordings remains “evergreen”: discussions have taken place in the context of in-vehicle cameras and surveillance in public places (in Sweden, for example, a special permit is required under separate law).
- Several enquiries asked whether and how EU legislation had been transposed/implemented by national authorities, and if yes, how? An example is Directive 2009/103/EC relating to insurance against civil liability in respect of the use of motor vehicles, and the enforcement of the obligation to insure against such liability, the provisions of which have been duly transposed by the Hungarian legislator into Act LXII of 2009 on compulsory motor insurance.
- On the practical side of data breaches, the question has been raised whether the loss or theft of a bank card or the use of manipulation techniques to obtain card data could be considered a data breach. In such cases, the conceptual elements of a data breach are met if the bank fails to comply with the general data security requirements for the handling of card data as set out in the GDPR. Since in the vast majority of cases card misuse is not due to a security flaw on the part of the bank, but the data are obtained directly from the data subject (typically by deception), no data breach occurs on the part of the bank most of the time. Regardless of this, of course, the criminal liability of the perpetrators who obtain the card data will be established in such cases, but the bank will not be liable for data protection/data security.
- Another question is whether a system failure or technical problem that makes bank information inaccessible to data subjects constitutes a data breach. If the unavailability of personal data is due to a security incident on the bank’s side (e.g. a denial-of-service attack on the bank’s website), the conceptual elements of a data breach are present. In this case, the data controller must be able to handle the incident in accordance with the GDPR and, as a result, must also ensure the recoverability and accessibility of the data.
- Another recurrent topic is the recording of telephone conversations with insurers, which is a data controller activity regulated by law in Hungary.

Although they are not strictly related to the Article 60 procedure of the GDPR, the Board's Article 64 opinions, of which 39 were received by the Authority in 2023, are also worth mentioning.

Also noteworthy are the 57 written procedures managed by the Authority in 2023 in relation to cooperation between national authorities, which are votes in IMI to simplify the agenda of the Board's plenary meetings.

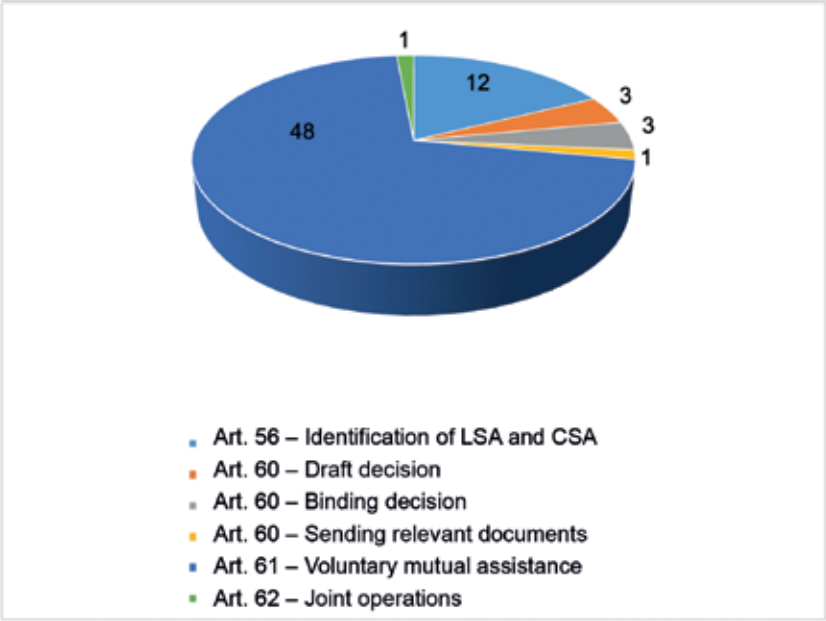


Figure 2: Procedures launched by NAIH in 2023

Based on the statistics kept since GDPR became applicable in May 2018, it can be established that the previous trend is continuing according to which the main emphasis of the procedures among Member State authorities is shifting from the identification of the lead supervisory authority towards cooperation and the exchange of information.

IV.5. Activities of the Authority within the Coordinated Enforcement Framework (CEF)

Each year, the European Data Protection Board (EDPB) identifies a priority issue to be addressed within the Coordinated Enforcement Framework. In 2023, the coordinated action of the supervisory authorities was focused on the designation and status of DPOs.

As part of the coordinated action, the Authority conducted a survey among DPOs in a subset of domestic public sector data controllers (those performing public tasks) using a standardised online questionnaire for participants in the action (which can be adapted to national specificities).

After receiving the responses, the supervisory authorities prepared their national reports using the template provided. These were collated by the Secretariat and compiled in a document adopted by the Board at its plenary meeting on 16 January.

The report summarises the findings of all the supervisory authorities participating in CEF and presents the current status of their work.

The first part of the report provides statistics on the answers to each question, while the second part analyses the challenges DPOs and the organisations nominating them (controllers or processors) are faced with, and how these may affect compliance with the GDPR. For each of the challenges identified, the specific problem is briefly described, indicating the specific provision of the GDPR, and the report includes some points of attention and/or recommendations for each of the challenges identified. Among the recommendations made, the recommendation to revise WP243 of the Article 29 Data Protection Working Party, the predecessor of the EDPB, on the guidelines for DPOs, maintained by the EDPB after the GDPR became applicable, should be highlighted.

The report also provides an overview of the measures already implemented or ongoing by supervisory authorities, including any guidelines issued by them, as well as enforcement and other measures taken by supervisory authorities.

National reports from the participating supervisory authorities, including the Authority, providing further details on the results obtained and on the analyses and observations at national level, are annexed to the document adopted by the Board.

In connection with the 2023 CEF, at its launch and following the adoption of the report by the EDPB, both the EDPB and the Authority published announcements on their websites.

IV.6. Review of GDPR after four years – NAIH's position in the Union-wide comparison[22]

The GDPR (four-year) Evaluation Report 2023 was prepared on the initiative of the European Commission, based on data provided by the data protection authorities; it was commented on by the EDPB, and also included the experience of the first year and a half of reporting after 2018[23]. According to the overall assessment, the GDPR has modernised and harmonised data protection principles at EU level, and awareness of data protection rights and obligations has increased significantly among data subjects and public and private organisations. Supervisory authorities frequently make use of their powers of investigation and correction, and cooperation in joint procedures and operations has been strengthened over the past years, with the EDPB playing a central role (of EDPB Guidelines on cooperation, see 09/2020 on relevant and reasoned objection under the GDPR; 2/2022 on the application of 60 GDPR; 6/2022 on the practical implementation of amicable settlement; of GDPR documents, see 1/2021 on joint operations; 6/2020 on preliminary steps to handle a complaint; 1/2019 on handling cases with only local impacts under Article 56.2 GDPR).

Based on the case statistics extracted from the IMI system, the Evaluation Report shows that the NAIH is in the middle of the field among Member States in all respects:

22 The entire Evaluation Report is accessible here: https://edpb.europa.eu/system/files/2023-12/edpb_contributiongdprevaluation_20231212_en.pdf

23 https://edpb.europa.eu/our-work-tools/our-documents/other/contribution-edpb-evaluation-gdpr-under-article-97_en

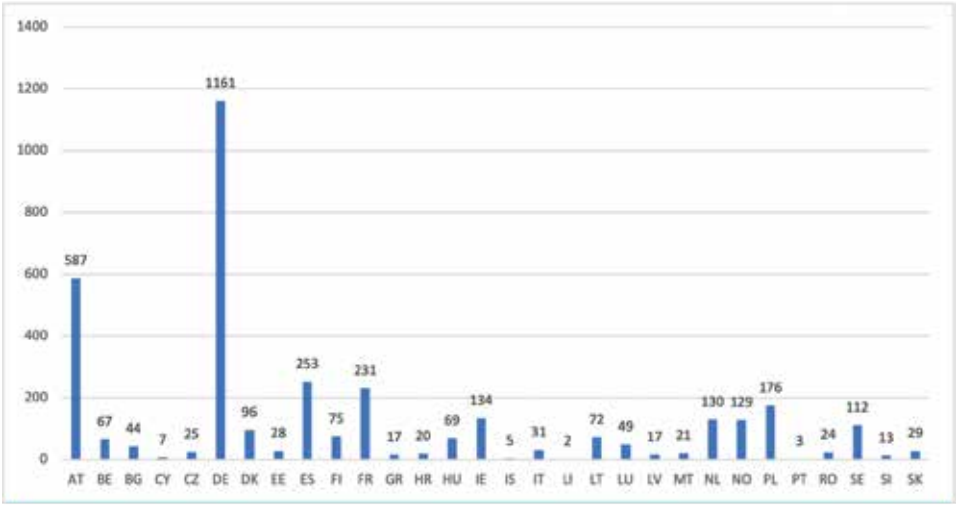


Figure 3: Number of procedures launched to identify the lead and concerned supervisory authorities, 2018-2023

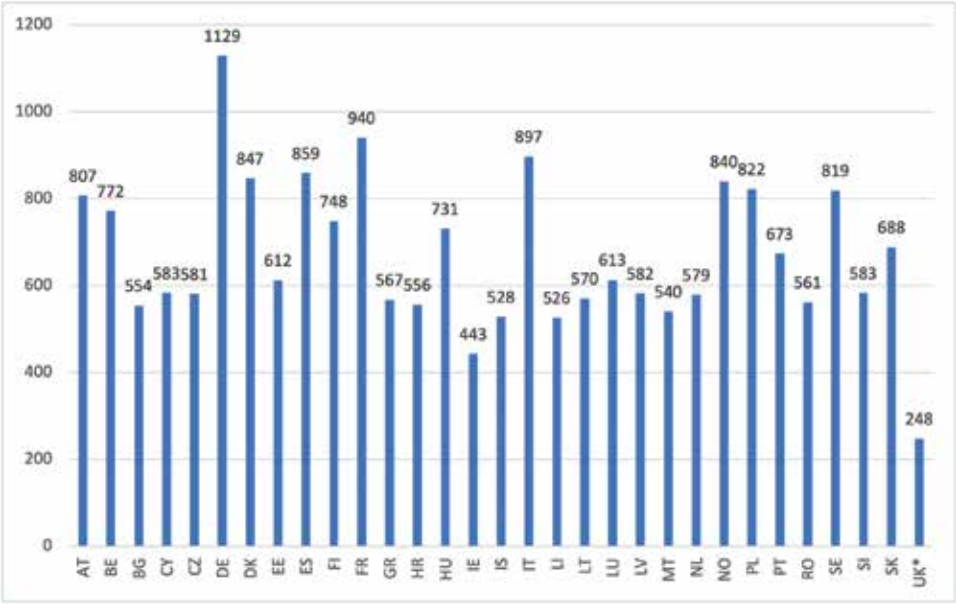


Figure 4: Number of Article 60 draft decisions received per concerned supervisory authority

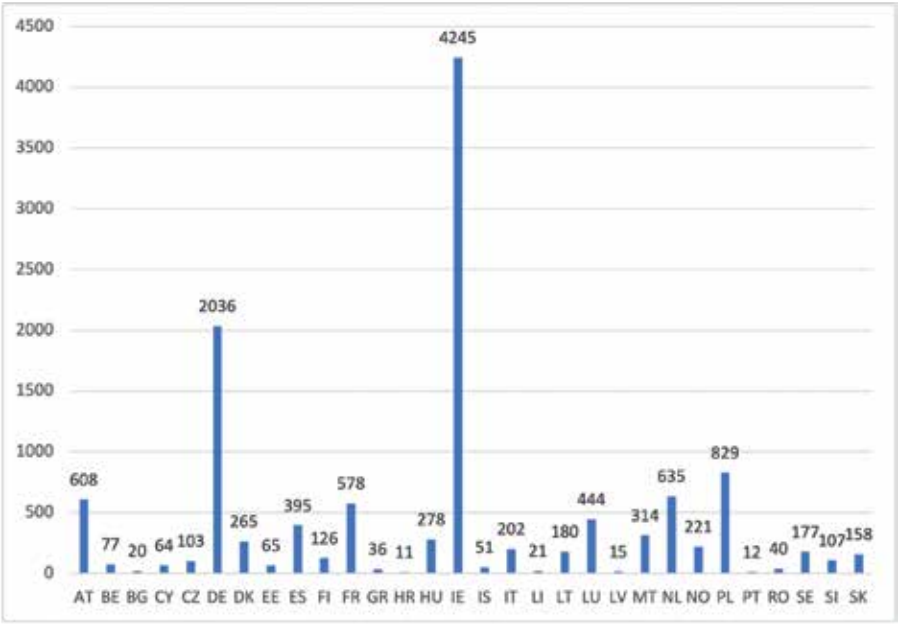
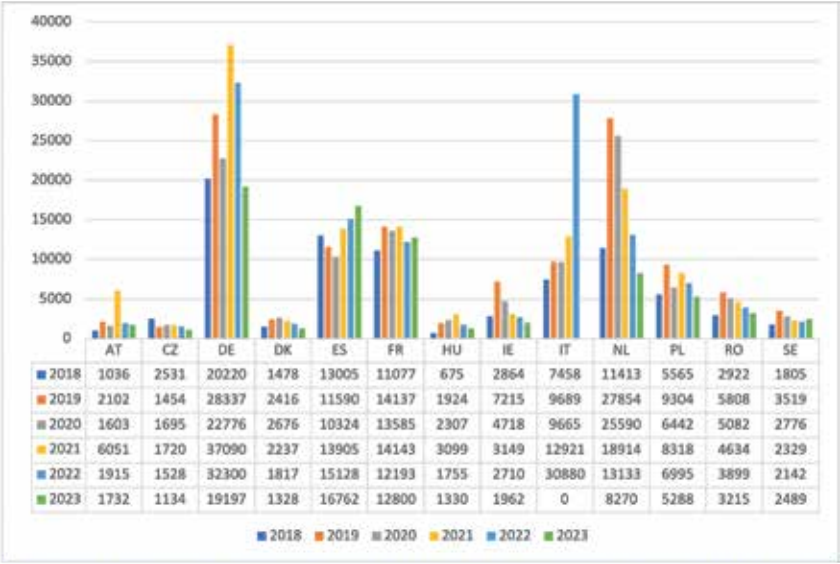


Figure 5: Article 61 - Voluntary mutual assistance procedure



	AT	CZ	DE	DK	ES	FR	HU	IE	IT	NL	PL	RO	SE
2018	1036	2531	20220	1478	13005	11077	675	2864	7458	11413	5565	2922	1805
2019	2102	1454	28337	2416	11590	14137	1924	7215	9689	27854	9304	5808	3519
2020	1603	1695	22776	2676	10324	13585	2307	4718	9665	25590	6442	5082	2776
2021	6051	1720	37090	2237	13905	14143	3099	3149	12921	18914	8318	4634	2329
2022	1915	1528	32300	1817	15128	12193	1755	2710	30880	13133	6995	3899	2142
2023	1732	1134	19197	1328	16762	12800	1330	1962	0	8270	5288	3215	2489

Figure 5: Annual breakdown of complaints received by the DPA (excluding requests for consultation) – Above 2,000 complaints

SA	2018	2019	2020	2021	2022	2023	TOTAL
IE	€0,00	€0,00	€785.000,00	€225.261.500,00	€1.077.583.000,00	€1.551.782.500,00	€2.855.412.000,00
LU	€0,00	€0,00	€0,00	€746.319.500,00	€48.375,00	€6.500,00	€746.374.375,00
IT	€2.992.675,00	€15.904.790,00	€60.635.147,00	€50.015.863,00	€42.850.782,00	€24.658.900,62	€197.058.157,62
FR	€1.196.000,00	€51.370.000,00	€3.489.300,00	€3.856.000,00	€25.122.900,00	€46.834.500,00	€131.868.700,00
ES	€13.180.655,00	€6.295.923,00	€8.018.800,00	€35.074.800,00	€20.775.361,00	€16.828.710,00	€100.174.249,00
DE[10]	€142.083,50	€16.783.838,05	€48.168.314,88	€2.676.162,14	€5.894.641,20	€6.177.051,50	€79.842.091,27
AT[10]	€9.500,00	€18.106.700,00	€17.650,00	€24.730.660,00	€50.650,00	€26.350,00	€42.941.510,00
GR	€625.000,00	€777.000,00	€48.000,00	€364.000,00	€30.060.000,00	€541.000,00	€32.415.000,00
SE	€0,00	€51.900,00	€12.700.000,00	€2.751.000,00	€823.000,00	€10.133.037,00	€26.458.937,00
NL	€0,00	€2.535.000,00	€2.043.500,00	€5.280.000,00	€4.840.000,00	€1.975.000,00	€16.673.500,00
NO	€0,00	€279.000,00	€506.000,00	€6.961.000,00	€1.550.000,00	€8.123.000,00	€17.419.000,00
HR	€0,00	€0,00	€145.995,09	€103.191,99	€528.369,49	€8.261.000,00	€9.038.556,57
PT	€400.000,00	€12.000,00	€2.000,00	€131.200,00	€4.496.500,00	€261.950,00	€5.303.650,00
BG	€186.775,00	€3.633.340,00	€530.414,00	€274.023,00	€652.971,00	€70.756,00	€5.298.179,00
PL	€0,00	€958.654,26	€805.440,06	€482.923,61	€1.669.304,28	€115.398,28	€4.031.720,49
HU	€0,00	€298.016,00	€808.098,00	€178.307,00	€1.297.355,00	€1.024.074,00	€3.605.850,00
FI	€0,00	€0,00	€207.500,00	€780.000,00	€1.195.300,00	€464.600,00	€2.647.400,00
BE[11]	€0,00	€39.000,00	€885.000,00	€301.000,00	€738.900,00	€80.000,00	€2.043.900,00
CY	€113.300,00	€142.600,00	€103.000,00	€1.069.500,00	€105.750,00	€65.750,00	€1.599.900,00
LV	€10.230,00	€163.522,59	€92.894,80	€109.627,18	€1.223.059,13	€22.600,00	€1.621.933,70
RO	€0,00	€489.000,00	€184.550,00	€66.900,00	€212.200,00	€268.900,00	€1.221.550,00
IS	€0,00	€0,00	€28.471,00	€132.424,00	€46.659,00	€537.356,00	€744.910,00
CZ[11]	€151.582,00	€58.191,00	€84.347,00	€243.147,00	€8.516,00	€122.141,00	€667.924,00

Figure 7: Total value of fines imposed per supervisory authority in an annual breakdown of fines

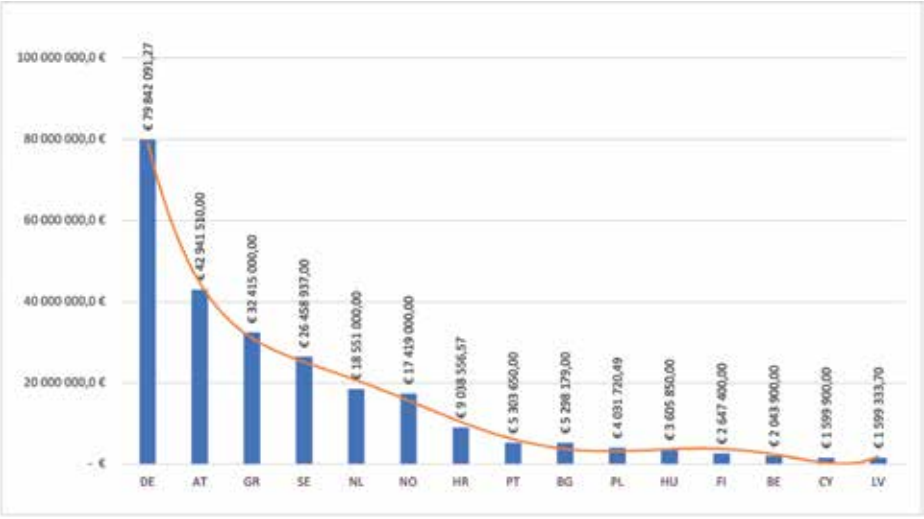


Figure 8: Total amount of fines in 2018-2023 – Between € 1 and 100 million

IV.7. New adequacy decision for transatlantic data transfers

The legal framework for the transfer of data from the EU to the US was first provided by the Safe Harbour agreement between 2013 and 2015, but in October 2015 the Court of Justice of the European Union ruled it invalid, following an objection by Max Schrems and the NOYB.EU (None Of Your Business) association behind him. The new framework, known as the Privacy Shield, was in place from 2016-2020, but following a new complaint by Max Schrems, the Court of Justice of the European Union again ruled on 16 July 2020 that the EU Commission decision under the agreement was invalid. Therefore, the European Commission adopted a new adequacy decision on the new EU-US Data Privacy Framework (DPF) on 10 July 2023.

On the one hand, the DPF covers processing for business purposes – so American companies can join on a voluntary basis, provided they commit themselves to implement and maintain data protection safeguards in line with the GDPR[24]. On the other hand, US authorities can only access EU citizens' personal data for law enforcement and national security purposes subject to the safeguards indicated, but beyond that they must also bear in mind the criteria of necessity and proportionality. European citizens will have two levels of redress available to them: they can send their complaints to the Civil Liberties Protection Officer (CLPO) employed by the US National Security Services and submit an appeal against their refusal to the independent, three-member Data Protection Review Court.

When redress mechanisms are to be used, both the national data protection authorities and the EDPB are also involved in filtering and forwarding complaints. At the time of writing this report, the EDPB is still working on a document on the procedure and a standard notification form, which, once adopted, will be publicly available on the websites of the Board and the DPAs.

24 List of participant US companies: https://www.dataprivacyframework.gov/s/participant-search

IV.8. Criminal/Justice cooperation

IV.8.1. Borders, Travel and Law Enforcement Expert Group (BTLE)

Law Enforcement Directive (LED, PD) Article 37 Guidelines

In March 2020, the EDPB mandated the BTLE expert subgroup to develop guidelines on Articles 36 and 37 LED. Following the completion of the work on Article 36 LED (Transfers on the basis of an adequacy decision), a new working group within the BTLE expert subgroup was established to draft and prepare guidelines on Article 37 (Transfers with adequate safeguards). The draft guidelines were discussed by the BTLE expert sub-group in several meetings in 2023, also using the opportunity to submit written comments. The BTLE expert subgroup also consulted the Commission on the individual discussion points. In the end, the working group responsible for drafting the working document and the Commission were able to reach a full consensus on the draft guidelines, which were finalised in August 2023.

Draft EU-US agreement on electronic evidence

The Commission presented the EU-US agreement that allows authorities to access electronic evidence directly through service providers in other jurisdictions for the purposes of criminal proceedings at the BTLE expert sub-group meeting. In particular, the agreement covers content data and aims to remove the conflicts of interest that currently prevent service providers from accessing and responding to requests from foreign law enforcement authorities. On the US side, it takes the form of an implementing agreement under the U.S. Cloud Act, while on the EU side, it takes the form of a separate international agreement. The negotiations started back in 2019 and the EDPS issued an opinion on the negotiating mandate.

The Head of the Commission's negotiating team met the President of the European Data Protection Board in early November 2023 and addressed the December plenary session to present the current situation.

Regarding the United Nations Cybercrime Treaty, the Commission informed the members of the BTLE expert sub-group that negotiations are at an advanced stage and that the draft text will be submitted for adoption in September 2024. This will be an international instrument on cooperation between central extradition authorities and it will provide assistance in legal matters. It will include a pro-

vision under which cooperation may be refused in the absence of adequate data protection safeguards.

IV.8.2. Coordinated Supervision Committee – CSC

The CSC, which coordinates the data protection supervision of the Schengen Information System (SIS), the Internal Market Information System (IMI), Europol, Eurojust and the European Public Prosecutor's Office (EPPO), met four times in 2023. In the near future, the CSC's tasks will be further extended to include data protection supervision activities related to the large-scale information systems developed for border, asylum and migration cooperation and police and judicial cooperation (EES, ETIAS, VIS, ECRIS-TCN).

The Schengen Information System (SIS) Supervision Coordination Group, which used to meet separately, has been put under the CSC since March 2023 as a result of the SIS Recast, so the tasks of the SIS SCG have been transferred to the CSC. The CSC secretariat tries to set the agenda of the meetings each time, taking into account that the membership of the different formations is different, not all Member States are members of the EPPO, for example, and some Member States are not full members of the SIS, and they can only participate in the meetings as observers.

As part of its work programme for 2022-2024, the CSC has decided to engage in a regular dialogue with civil society organisations on their possible involvement in issues such as migration, which are relevant to the CSC's mandate. As a first step, representatives of the CSC consulted three NGOs (EDRi, Access Now, Statewatch). One idea is to organise joint awareness-raising campaigns to inform citizens about their rights, on the one hand, and to support the competent authorities in the fight against discrimination in the field of digital rights, on the other hand. Potential cooperation could also involve parties drawing each other's attention to new relevant documents and developments, including those which are, for example, unlikely to come to the attention of data protection authorities.

The Dutch DPA organised a workshop in September 2023 to exchange experiences in order to give colleagues a better understanding of how each DPA is strategically preparing to deal with the new supervisory tasks at national level in relation to the enlargement of EU information systems, data flows and interoperability. The workshop was also attended by staff from the Authority

In connection with Eurojust, the issue of secure communication channels and the use of encryption for the transmission of personal data from national authorities to the national units of Eurojust has been raised. Most of the EDPS recommendations have been implemented. The new legal framework for Eurojust – the amendment of the Eurojust Regulation – is expected to settle a number of issues in 2025. Eurojust would also receive a new CMS, inter alia to enable the processing of electronic evidence.

The EDPS presented its main findings of the Annual Audit Report 2022 on Europol. The report concerned the processing of personal data of minors, with a specific focus on those under 15 years of age. The investigation concentrated on the transfer of data from third countries and international organisations, which sometimes apply lower standards for the processing of minors' data than EU Member States. In particular, the EDPS noted that Europol should make its own assessment of the lawfulness of the processing of data received. The EDPS also informed the CSC of ongoing proceedings against Europol, which were initiated on the basis of complaints, either because there were insufficient grounds for refusing data subjects' requests for access or because Europol was late in responding to data subjects' requests for access. According to Europol, the delay stems from a structural problem in the Europol Regulation, which provides for a short time limit of three months for responding to access requests, as this period may not be sufficient to allow Europol to receive information from national law enforcement authorities.

The EDPS also shared some findings on the 2023 annual PNR data audit. In particular, the EDPS shared the observation that the assessment and the way of action at national level differ significantly between Member States. CSC members agreed that the issue of PNR data falls under the remit of the BTLE expert subgroup and therefore agreed that the Deputy Coordinator is to refer to the BTLE expert sub-group for the clarification and identification of possible actions.

IV.8.3. Scheval training for experts

Since the entry into force in October 2022 of Regulation (EU) No 2022/922 on the establishment and operation of an evaluation and monitoring mechanism to verify the application of the Schengen acquis (hereinafter: Scheval Regulation), periodic evaluations are carried out by experts on the basis of a new approach. The so-called Scheval 3.0 takes a country-specific rather than a domain-specific approach to assessing the performance of individual Member States in applying the Schengen acquis. Periodic pre-announced inspections are complemented by

unannounced evaluations and thematic inspections. Periodic audits switch from the previous five-year period to seven-year periods and regular follow-up, including repeat and monitoring visits, are going to play a key role. Regular training is required to ensure that the expert team carrying out the Scheval controls can perform their work to a sufficiently high standard. Accordingly, the Commission has developed a training plan for the experts in the so-called "expert pool". As a first step in this training plan, training in the area of data protection was launched in 2023, in which the Authority's staff was also participating.

IV.8.4. The working group supervising data protection of the Visa Information System (VIS Supervision Coordination Group)

In 2023, the VIS SCG developed a common audit plan to assist the supervisory authorities' work and to standardise to some extent the way in which audits are carried out at national level, thus allowing for a more efficient analysis and comparison of results. The joint audit plan will support the authorities as supervisory bodies in carrying out audits, taking into account that the procedural rules and audit methods at national level may vary considerably. Therefore, each DPA can adapt the audit plan to its own procedures, as the methods and questions described in the plan will serve as a guide for the authority carrying out the audit. The common audit plan contains a set of questions (checklists) that are relevant for the audit of the Visa Information System (VIS) from a data protection perspective. The thematic checklist of questions is intended to explore compliance with the requirements of Regulation (EC) 767/2008 (VIS Regulation), Regulation (EC) 810/2009 (Visa Code) and Council Decision 2008/633/JHA (VIS Decision). The set of questions is divided into distinct sections depending on the actor of data processing to which the questions refer, e.g. controller, processor, external service provider. In preparing the joint audit plan, the VIS SCG has also taken into account previous recommendations made in the framework of the Schengen evaluation of VIS (SCHEVAL) carried out in different Member States.

The Authority prepared for the upcoming Schengen audit of Hungary in 2024 by using the common audit plan in 2023. Similarly to previous years, the Authority's staff carried out audits at the Ministry of Foreign Affairs and Trade and the National Directorate-General for Aliens Policing as controllers of the Visa Information System.

IV.8.5. The working group supervising the data protection of the Eurodac System (Eurodac Supervision Coordination Group)

In its work plan for the period from 2022 to 2024, one of the main tasks set by the Eurodac SCG was the definition at national level of the bodies that would have access to the Eurodac system for law enforcement purposes and the verification of the lawfulness of such access. Chapter VI of the Eurodac Regulation currently in force provides for a procedure to allow the comparison of fingerprints with those stored in Eurodac and their transmission for law enforcement purposes. However, because of the fundamental right to privacy, law enforcement authorities may only use Eurodac for comparison if they have no other means available to them for the prevention, detection or investigation of a terrorist offence or serious crime. In the light of future changes to the Eurodac Regulation, the Eurodac SCG considered that it would be important to examine the current use of this procedure by Europol and national law enforcement authorities. In order to allow authorities to monitor the practice at national level, the Eurodac SCG has developed a common review methodology.

In 2023, the Authority launched an ex officio investigation at national level into the processing of data in the context of the implementation of the Eurodac Regulation. Based on the questions drawn up by the Eurodac SCG, the Authority first examined in writing and then on the spot the processing of fingerprint data by the Hungarian Institute for Forensic Sciences and the National Directorate-General for Aliens Policing.

IV.9. Ratification by Hungary of the "modernised" Convention 108+

The *Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data, signed in Strasbourg on 28 January 1981* (known as Convention 108 or the Data Protection Convention) is the first and to date the only instrument with binding force in international law that comprehensively regulates the framework of the right to the protection of personal data. Its importance extends well beyond the European continent, as the parties to the Convention are not only members of the Council of Europe, but also non-member non-European States (e.g. Argentina, Uruguay, Morocco, Tunisia, Mexico, Senegal).

The revision and the "modernisation" of the Convention's rules was carried out in parallel with the European Union's data protection reform. As a result of the revision process, the Member States of the Council of Europe agreed on the text of

an Additional Protocol amending the Convention (ETS 223 Additional Protocol), which was adopted by the Council of Europe's Committee of Ministers on 18 May 2018 and is open for signature as of 25 June 2018. Thirty-one States have ratified the Additional Protocol by January 2023, but its entry into force in international law – the conditions for such entry into force as set out in the Additional Protocol – still have to be met. Hungary signed the Additional Protocol amending the Convention on 9 January 2019, and it was promulgated by Act XLIII of 2023 on the promulgation of the Amending Protocol signed at Strasbourg on 10 October 2018 to the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data, signed at Strasbourg on 28 January 1981, and ratified on 19 October 2023. After its entry into force in international law, which is expected in the course of 2024, the "modernised" Data Protection Convention will certainly have an even greater global impact on the protection of personal data than before, becoming a standard to which the subjects of international law will have to conform in the future, and they will develop their own legislation on the protection of personal data in the light of the legal provisions of this instrument.

IV.10. The Council of Europe Convention on access to documents containing data of public interest

The Council of Europe Convention on access to official documents entered into force on 1 December 2020. Currently, there are 15 parties to the Convention: Albania, Armenia, Bosnia and Herzegovina, Estonia, Finland, Hungary, Iceland, Lithuania, Montenegro, Norway, the Republic of Moldova, Slovenia, Spain, Sweden and the Ukraine.

The Tromsø Convention was the first binding international legal instrument to give anyone, without discrimination, the right of access to documents containing data of public interest held by a public authority, regardless of the status of the applicant or the purpose of the request. Under the Convention, all documents containing data of public interest are, as a general rule, accessible and may be disclosed, and this may be restricted only in order to protect the rights and legitimate interests specifically listed in the Convention, unless there is an overriding public interest in disclosure. There are also rules which must be respected in any event concerning the speed and fairness with which public authorities process requests for access to official documents, the cost of access and the right to legal remedy before a court or other independent body in the event of the refusal of the request.

The two monitoring bodies established under the Convention are a group of experts on access to documents containing data of public interest or the Access Info Group (AIG) and the Consultative Council of the Parties. The AIG is a body of independent and impartial experts with the highest level of integrity in the field of access to official documents, which evaluates and reports on the legislative and other measures adopted by the Parties to implement the provisions of the Convention. In carrying out its tasks, the Access Info Group may seek information and opinions from civil society. One of the ten members of the Expert Group is the President of the NAIH.

Over the past three years, the Parties to the Convention submitted reports under Article 14 of the Convention, setting out the legislative and other measures they have taken to implement the Convention. The country reports have been the subject of preliminary draft assessment reports prepared by the officers assigned to each Party, and in the final stage of the process the Secretariat, on the instructions of the Group of Experts, has prepared a draft core assessment report on the basis of the reports. Recently, changes were made in the legislation on the freedom of information in several Member States which have resulted in the need to amend the Article 14 country reports. Inter alia, these amendments and the evaluation reports of Bosnia and Herzegovina, Moldova and Lithuania were on the agenda of the last meeting of the Group of Experts.

The Convention entered into force in Spain on 1 January 2024, so the Secretariat called upon the Spanish Party to complete a questionnaire on legislative and other measures to implement the provisions of the Convention. The Convention continues to be open to accession by any State that meets the accession requirements set out in Article 17 of the Convention.

V. Cases of litigation for the Authority

In 2023, the Authority had altogether 47 finally closed cases of litigation at the Municipal Court of Budapest and at the Curia.

Of these, the Authority was 100% successful in 29 cases, the Authority was overwhelmingly successful in 6 cases, the court dismissed the petition in 1 case, the court dismissed 3 cases and the Authority lost a total of 8 cases. Almost without exception, the guidelines issued by the judges in the Authority's repeat proceedings concern the correction of procedural errors or a more precise determination of the amount of the fine.

In 2023, the Authority imposed fines of HUF 524,375,000, of which HUF 518,500,000 was data protection fines, HUF 5,345,000 was procedural fines and HUF 530,000 was enforcement fines. Of the fines imposed, including late payment penalties, HUF 325,502,768 were paid voluntarily by the liable parties, while enforcement action by the NAV was taken in connection with fines amounting to HUF 89,015,000.00, i.e. about 62% of the fines imposed were paid voluntarily by the liable parties.

Based on the Authority's experiences with litigation, it can be stated that the emphasis of litigation shifted towards administrative lawsuits following data protection procedures launched upon request. In the fifth year of the application of the General Data Protection Regulation, it can be said that the Authority has to respond to increasingly complex data protection legal issues, both in terms of factual and legal content, and the same is true for the application of the law in court. There is also a clear trend towards a rise in litigation, which is also linked to the increasing amount of fines imposed by the Authority.

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

V.1. Claims against Meta Platforms Ireland Limited for breach of rights to the protection of personal data

The facts of the case

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

Clause 4.2 of the Facebook Terms of Use (hereinafter "Terms of Use") provided the possibility for the Respondent to suspend or permanently block a user's access to their account in case of a clear, serious or repeated violation of the Terms of Use or other policies of the Respondent, including in particular the so-called Community Principles. In case of breaching the provisions of Clause 3.2. 1-3.a of the Terms of Use, if Facebook removes any content shared by the user due to a violation of the Community Principles, it will inform the user and explain the options available to request a review, unless the user is in serious or repeated violation of the Terms of Use, or if doing so would expose Facebook or others to legal liability, harm the user community, hinder or interfere with the operation or integrity of Facebook's service, system or product, or where there are technological limitations that prevent it from doing so, or where it is prohibited from doing so by law. Once deleted in accordance with Clause 3.1 of the Terms of Use, the content will no longer be visible to other users; if, due to technical limitations, immediate deletion is not possible, it will be actually deleted within a maximum of 90 days from the date of deletion.

Similar rights were granted not only to the Respondent, but also to the operator of the site concerned. The persons who managed the specific Facebook page (three roles are relevant to the dispute: the administrator, the editor and the moderator) were all entitled to reply to comments and posts on the page, to delete them from the page or to "ban" or "block" another Facebook user from the page. Beyond that, the administrator and the editor also have the right to create and delete posts on behalf of the page, and to edit the page. Moreover, administrators also have the ability to manage roles and settings for the page. Once a Facebook user creates a page, they automatically become its administrator.

When a user's profile is "blocked", the blocked user is unable to see the content posted by the user blocking him, he is unable to access it, and is unable to find the page and view the posts posted there. When a user is "blocked", the blocked user can view the content of the page, but has no possibility to comment on the posts. Users banned or blocked by another user are not notified of the action.
Facebook's Privacy Policy (15/A/3) indicated the contact details of the data controller and the data protection officer, and specified the data that the Respondent processes in support of the services it offers. In this context, the Respondent collects information and content provided by the user when using Facebook, it collects data on the people, accounts, Facebook pages and groups to which the user is connected, the way in which the user interacts with them, and the intensity of the interactions. It collects information about how the user uses the service, such as what types of content are viewed; it logs when the service is used, which posts and content are viewed. According to the Privacy Policy, the Respondent may use these data to provide access to and support the Respondent's products and services, as defined in the Terms of Use, to the user. The Privacy Policy also includes the manner in which such data may be used and shared, the legal basis for processing and a warning of the possibility to exercise the rights granted by the GDPR.

Only the so-called "help centre" provided information about the types of roles (five different roles) associated with each page, and that if a user blocks another user's profile, the blocked person does not get notified that the profile has been blocked. The "activity log" is a Facebook feature that allows users to review and manage their activity, including posts they have made, activity on pages, posts, messages and other activity posted by others.

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

The petition
In his petition, the Petitioner asked for a declaration, pursuant to Section 2:51(1)(a) of the Civil Code, that the Respondent, as data controller, had infringed his

rights to freedom of expression and human dignity, and his rights to the protection of personal data and human dignity.

Due to the above infringements, pursuant to Section 2:51 (1)(b) of the Civil Code, the Petitioner requested that the court prohibit the Respondent from similar infringements in the future, so that users who identify themselves as public figures in the Facebook system as representatives of the Facebook page in question (editor, moderator, administrator), as decision-makers, could apply a decision (blocking) resulting in the restriction or ban of the right to express one's opinion or the erasure of one's comments made in the past or to be made in the future. Pursuant to Article 2:51(1)(d) of the Civil Code, he asked that the Respondent be ordered to remedy the grievous situation by restoring access to the public figure's Facebook page and his deleted posts within 15 days and by restoring all his subsequently deleted posts (110+436).

According to the Petitioner's argument, the Respondent is not only a passive hosting provider, but also a data controller in its own right (but at least in common with the "administrators" of the sites blocking it) (Article 4(7) of the GDPR; Article 26 of the GDPR). He is himself a "data subject" within the meaning of Article 4(1) of the GDPR, and his posts are "sensitive personal data" within the meaning of Article 9(1) of the GDPR. The deletion of his personal data (the comments) stored on the system operated by the Respondent is data processing within the meaning of Article 4(2) of the GDPR. Even if the Respondent did not delete the comments itself, the hosting and the system developed and operated by the Respondent allowed third parties (administrators, editors and moderators) to delete the comments, and is therefore a data controller. The Respondent is solely responsible for the deletion of his posts, not only from the Facebook pages accessible to all, but also from his activity log. In the absence of the conditions set out in Article 6(1) of the GDPR, the Respondent's processing is unlawful. By virtue of the applicable (reverse) burden of proof rule under Articles 5, 24 and 82 of the GDPR, it is for the Respondent to prove that it was not at fault. By accepting the Terms of Use (which cannot be considered as a waiver), he only accepted the legal consequences of lawful blocking and deletion, but not the restriction in the case at hand. Any content of the Terms of Use contrary to the GDPR shall be disregarded. In relation to the public figure's page, the Respondent should not have provided third parties (administrators, editors and moderators) with the possibility of deletion and blocking in the first place, but if it had done so, it would have been obliged to operate the system in a GDPR-compliant manner under Articles 24(1) and 25(1)-(2) of the GDPR.

The Respondent's non-compliant data processing and the shortcomings in the supply of information led to the fact that he was unable to exercise his rights properly as a data subject. The Data Protection Policy only identifies the Respondent, it carries no reference to the processing of data by the administrators of each site, the relationship between the Respondent and these administrators, and the division of responsibilities and rights. The possibilities for the exercise of data subject rights are not transparent, such processing is unfair.

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

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

The Authority has drawn attention to the European Data Protection Board (EDPB) Guideline 7/2020 on the correct interpretation of the GDPR. It pointed out that the capacity of data controller does not require that the controller has access to the data subject to the processing, and that joint processing can take the form of joint decisions, resulting from coordinated decisions, if the decisions are complementary and inseparable. It pointed out that the Respondent's status as controller has been established by the Court of Justice of the European Union (CJEU) in

several judgments (CJEU C-319/20; C-645/19). In its judgment in Case C-210/16 Wirtschaftsakademie Schleswig-Holstein (paragraph 26 et seq.), the CJEU held that the administrator of a site of the social network and the Respondent were joint controllers. The CJEU also confirmed in its judgment C-40/17 (Fashion ID) that the decision of an organisation to use for its own purposes a tool or other system developed by another organisation which allows the processing of personal data is likely to constitute a joint decision on the mode in which those organisations process personal data.

Judgment of the court of first instance
The court did not share the Petitioner's view that the Respondent was a data controller (or joint controller) in relation to the acts subject to litigation. The Respondent's data processing activities had a different content and purpose from those subject to the complaint, essentially consisting of the collection of data in support of other products and functions it offered. The Respondent did not have any control over the exercise of the user rights granted by Facebook's system (deleting another user's post or blocking another user). Only by applying the so-called "decisive influence test" can the existence of joint controller status under Article 26 of the GDPR be decided. The Respondent had no influence on the data processing activities in the case, in terms of the deletion of data, the purpose of the deletion, the scope of the posts to be deleted and the management of the data processing practices. The mere fact that the Respondent gave users of Facebook pages (in the role of administrator, editor or moderator) the possibility to delete other users' posts on the page in question or to block (ban) other users from the page does not in itself result in a common definition of the purposes and means of the processing. The administrators of the Facebook page in question exercised their discretion independently of the Respondent, necessarily using the tools provided by the Respondent, but deciding themselves, within the limits of the possibilities provided by the tools, which tools to use. The facts of the cases referred to by the entity intervening on the Petitioner's behalf to justify joint processing are different from those in this litigation and are therefore not applicable.

As it is known to all, the Terms of Use must be accepted during the registration process as part of the legal relationship between the parties, and their acceptance constitutes consent to the processing of data pursuant to Article 6(1) and Article 9(2) of the GDPR. Indeed, the Terms of Use do not address the roles related to the individual pages, but the relevant information is available in the so-called Help Centre, and the Petitioner should have been aware that the administrator (administrator, editor or moderator) of a given page is entitled to de-

lete posts on that page and to block or ban other users on that page. The fact that the Petitioner's posts deleted by other users are not available in the Petitioner's own activity log does not violate the data controller's obligations under Articles 24(1) and 32 of the GDPR, because the Respondent has not made any undertaking to ensure that the deleted posts remain available in the activity log, despite their deletion.

Both the Petitioner and the Authority, which intervened on behalf of the Petitioner, submitted an appeal against the judgment of the court of first instance.
Judgment of the court of second instance

Contrary to the judgment of the court of first instance, the Respondent was found to have breached certain provisions on data processing in connection with the erasure of the Petitioner's comments from the activity log. At the same time, since the Petitioner's action as a whole was aimed at enforcing sanctions under the law to protect privacy (and not specific data protection provisions under the Privacy Act), the court of appeal did not establish that the Respondent had breached the privacy rights that were the subject of the action despite the data processing infringements, so no ground was found for repeating the procedure of first instance either by the examination of the adequacy of the Respondent's information or the fact that pursuant to Section 23(2) of the Privacy Act the Respondent would have been required to prove the lawfulness of data processing during the proceedings at first instance, but no such proof was provided.

The court of first instance correctly found that the Respondent was not a data controller (joint controller) in relation to the "first stage of processing", i.e. the erasure of the Petitioner's posts on another user's page and the blocking of the Petitioner by another user. The court of first instance correctly recognised that the processing of data by the Respondent and the individual user was of a different nature and for different purposes, and that those purposes were not closely related or complementary (EDPB 07/2020, paragraph 60). By registering in Facebook's system and by accepting the Terms of Use (as a general contractual condition), the parties also became part of a legal relationship with each other, as a whole, by granting each other the rights that they enjoyed in relation to their own pages. The user who is the data controller of their own site (the site administrator) has become entitled to the processing operation complained of. The operator of the site (administrator, editor, moderator) necessarily used the system developed by the Respondent. However, the use of a common data processing system or infrastructure does not necessarily lead to joint data processing (EDPB Guidelines No 7/2020, paragraph 68), in particular where there is no joint

data processing in relation to the consequences of the system settings which are not foreseeable by the operator of the site.

With regard to the first phase of data processing, it was significant that the operator of the Facebook page in question had the sole control – based on the assessment of the content of the post and the commenter's rating – over the content of the post and the users who were banned from the page, i.e. he alone had "decisive influence" over the publicity and content of the page, and the Respondent had no influence on this at all. In terms of the "influence" of the controller (the purpose and the basic means of data processing), there was no joint decision (or a decision taken jointly or not alone) or a coordinated decision. Because of this, contrary to what is alleged in the appeal, the Respondent did not have to conclude a legal agreement with each user on the sharing of responsibility (EDPB Guideline 07/2020, summary and paragraphs 39, 40, 55, 59). The use of the first person, plural in the Terms of Use does not refer to joint processing, it is merely a(n un-Hungarian) linguistic formula intended to apply only to the Respondent. The Respondent's system does not (and cannot) distinguish between the rights of public and non-public Facebook users. It is consistent with the purposes of data processing that the operator of the Facebook page concerned may, within the Facebook system, remove the publicity of its page, either by limiting it to the posts of another user or by limiting it to the other user's entire activity. In the case of blocking a profile, the erasure of the blocked user's entire activity publicly expressed on that page is consistent with the rights of the operator of that page, as well as the purposes and the publicity of processing.

However, the Court of First Instance erred in not establishing the Respondent's status as a data controller for the "second stage of processing", the processing of the activity log. Of the data processing provisions identified in the petition, only those relating to the outcome attributable to the Respondent, namely the erasure of the posts from the activity log, had relevance. The Respondent rightly argued that it was essentially a hosting provider (Article 2(lc) of the Act on Electronic Commercial Services). In addition, it is also an application provider (Article 2(m) of the Act on Electronic Commercial Services), because it has developed and made available to users a system which allows the creation of a wide communication network (network of connections) among individual users. The Petitioner's argument is correct in so far as it is unlawful that resulting from Facebook's system, which is exclusively determined by the Respondent and which is consistent with the data processing purposes, the posts containing the Petitioner's specific personal data are deleted automatically and without prior information to the user concerned after 90 days from the activity log of the user's own page – as the

Petitioner's storage space – and after a further 90 days from the entire system operated by the Respondent (the backup interface).

The Petitioner correctly argued that neither the operator of the comments page nor the Petitioner could have been aware from the Terms of Use and the Privacy Policy alone of the effect that the blocking of the profile would have on the Petitioner's activity log. The Terms of Use did not contain any information on the consequence for the activity log, but only on the consequences of the Petitioner' erasure of the shared content and the deletion of the user's own page. The Respondent itself – indirectly – admitted this at the appeal hearing. Contrary to the Respondent's argument, the partial information displayed on the "help" interface is also irrelevant because, apart from the fact that it is not part of the parties' contract (GDPR, Recital 32) without the user's activity (by putting an x in the relevant box), it does not imply a legal consequence covering the activity log. The erasure of personal data from the activity log (as storage space), which is managed and accessed exclusively by the Petitioner, can no longer be considered as processing necessary for the performance of the contract without further ado [Article 6(1)(b) of the GDPR]. The Petitioner did not even consent to this, so the processing is unlawful and lacks a basis under Article 6 of the GDPR. The Respondent is not a joint controller with the operator of the other Facebook page with regard to the content of the activity log (Article 26 of the GDPR). The consequences of the decision of the other controller on the activity log were determined by the Respondent – independently of the controller of the page concerned – already before the erasure or blocking, by considering the processing unnecessary already at the level of the activity log after the erasure/blocking, and thus it is an independent controller in this respect.

The principle of data minimisation, if proper information is provided about it, could justify the lawfulness of the Respondent's decision as data controller. Had proper information been provided, the Petitioner could also have been prepared to create backups of the comments stored in his activity log on a regular basis, which constitutes a material form of his 'sense of mission'. According to this principle, the scope of the data stored should be limited to the minimum necessary for the purpose. To this end, it must be ensured that the storage of personal data be limited to the shortest possible period of time, and the controller must therefore set time limits for erasure or periodic review (GDPR, Recital 39). In accordance with Article 5(1)(c) and (e) of the GDPR, the Respondent could have required that public data which ceased to be public as a result of the action of the operator of the page concerned be deleted from the activity log immediately or within a specified period of time. However, neither the Terms of Use nor the

Privacy Policy contain such a provision (on this ground). Clause 3.2 of the Terms of Use only sets out the legal consequence of Facebook itself (as the hosting provider) removing content shared by a user, but it does not address the further consequences of deletion or blocking by another user.

The Respondent breached Articles 12(1), 13(2)(a), 24(1) and 25(1) of the GDPR and its actions were not consistent with the principles of Article 5(1)(a) and (f) of the GDPR. The obligation to provide information under Articles 12 and 13 of the GDPR was imposed on the Respondent irrespective of the data subject's request. However, the Respondent rightly argued that the exercise of the rights under Articles 15, 16 and 20 of the GDPR presupposes a request by the data subject and that it was not established that the Petitioner had made a request, so the Respondent could not be held liable for the infringement of those provisions. As explained above, the breach of any data processing rule does serve as a basis for the infringement of personality rights.

The right to the protection of personal data provides external protection for personal data, protecting them from the outside (the public), and basically providing protection in the event of unauthorised acquisition, communication to an unauthorised person or disclosure. The very opposite is the case in the present litigation. In the case of the deletion from the Petitioner's activity log of personal data lawfully deprived of their publicity by the operator of the Facebook page, who has the right to delete and block them, it is not the external protection of the personal data which is the protected legal object, but the storage of the data itself (as information of some value to the Petitioner from some respect) in the activity log which acts as a repository for the Petitioner.

By its very nature, this infringement does not constitute a breach of the right to the protection of personal data or of another personal right (human dignity) which is the subject of the action. *(Győr Court of Appeals Pf.III.20.070/2023/11-I.).*

V.2. The Budapesti Elektromos Művek Zrt. case at the Court of Justice of the European Union and its domestic aftermath (C-132/21.)

In this case the Municipal Court of Budapest referred the following questions to the Court of Justice of the European Union (hereinafter: CJEU):

Must Articles 77(1) and 79(1) of Regulation 2016/679 of the European Parliament and of the Council be interpreted as meaning that the administrative appeal provided for in Article 77 constitutes an instrument for the exercise of public rights, whereas the legal action provided for in Article 79 constitutes an instrument for the exercise of private rights? If so, does this support the inference that the supervisory authority, which is responsible for hearing and determining administrative appeals has primary competence to determine the existence of an infringement? If the data subject – in whose opinion the processing of personal data relating to them has breached the General Data Protection Regulation – simultaneously exercises their right to lodge a complaint under Article 77(1) and their right to bring a legal action under Article 79(1) of the General Data Protection Regulation, which interpretation is consistent with Article 47 of the Charter of Fundamental Rights:

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

b) the supervisory authority's decision takes precedence when it comes to assessing as to whether a breach has been committed regarding the powers provided under Article 51(1) of the GDPR and those conferred by Article 58(2)(b) and (d) of the GDPR

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

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

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

After the Respondent's decision, the relationship between the final judgment of the Civil Chamber of the Metropolitan Court of Appeal and the Respondent's decision was examined by the Metropolitan Court of Budapest on the basis of the administrative procedure and the judgment of the CJEU. With regard to administrative jurisdiction and civil jurisdiction, the CJEU judgment did not rule out parallelism in the opinion of the Municipal Court of Budapest, but, in accordance with the principle of procedural autonomy, considered it to be a matter for the Member States to lay down detailed rules governing the relationship between the means of redress, taking into account the obligation to ensure effective legal protection. In this respect, the court could only state that there is no such detailed regulation in Hungarian law, and no individual review procedure may be initiated by a judge for the discontinuation of a breach of fundamental law caused by an omission, in the light of Section 25 of Act CLI of 2011 on the Constitutional Court.

However, according to the Metropolitan Court of Budapest, paragraphs [54]-[56] of the CJEU judgment are relevant for the resolution of the case insofar as it states in the relationship between Articles 78 and 79 of the GDPR that conflicting court decisions would weaken the protection of natural persons with regard to the processing of their personal data, which would lead to legal uncertainty due to the lack of consistency. The obligation of protection as formulated by the CJEU is also reflected in the provision of the CJEU judgment, emphasizing the effectiveness of the legal protection and the requirement of consistent and uniform application of the law. With regard to Section 85(6) of the Act on Public Administration Procedure, the final judgment was not binding on the court in the administrative proceedings, but the content of the final judgment – in view of the highlighted part of the CJEU judgment – was not in itself decisive, but was taken into account by the Metropolitan Court of Budapest as a fact relevant to the case. Therefore, the Municipal Court of Budapest decided to annul the Authority's de-

cision and order the Authority to start a new procedure, and instead of adopting the Authority's interpretation of the law, it followed the final judgment of the Municipal Court of Appeal in the parallel civil proceedings also on the substantive data protection issue.

In the above-mentioned question of principle, the Curia found, on the basis of the facts of the case, that the CJEU judgment responded to the parallelism of the civil judicial remedy, jurisdiction and the administrative remedy (competence of the Respondent, administrative remedy, jurisdiction) by stating that the question falls within the competence of the Member States. The administrative court of first instance, i.e. the Metropolitan Court of Budapest, therefore correctly found that –- although the CJEU judgment considered it to be a matter for the Member States to lay down detailed rules on the relationship between parallel legal remedies in accordance with the principle of procedural autonomy – there is no such detailed regulation in the Hungarian legal system. However, having established the existence of Member State jurisdiction and the absence of detailed national legislation, the judgment made the wrong conclusion from paragraphs [54]-[56] of the CJEU judgment (which, as regards the relationship between Articles 78 and 79 of the GDPR, held that conflicting judicial decisions would weaken the protection of natural persons with regard to the processing of their personal data, and it would create legal uncertainty due to the lack of consistency).

It is up to Member State law enforcement and Member State courts to interpret EU law. In the present case, the GDPR is a regulation directly applicable in the Member States. Consequently, if, as a result of legal remedy running in parallel, the final judgment of the civil court in a given case precedes the final judgment of the administrative court in time, but the interpretation or application of EU law according to the civil judgment is incorrect, as believed by the Curia in the present case, the administrative court that subsequently rules may depart from the final judgment of the civil court. In the present case, the administrative court, i.e. the court of first instance, could have departed from the judgment of the civil court. This would have been just in the interests of legal certainty, contrary to the position of the judgment, which would have given priority to the consistency between the civil and administrative judgments, irrespective of the correctness of the interpretation of the law. According to the Curia, the Authority rightly pointed out in its request for review that the procedure of the court of first instance did not meet the goal of resolving legal uncertainty: it is not acceptable that, although there is consistency between the judgments of the civil court and the administrative court, EU law is interpreted in the same way, but the law is misinterpreted, and it is raised to the level of a final judgment. The Authority also complained,

with good reason, that the court of first instance disregarded the Respondent's statement in this context, which challenged the correctness of the final judgment of the civil court, but this was not the decisive factor in the review procedure, but the incorrect solution chosen by the court of first instance and its consequence. On the basis of the foregoing, the Curia repealed the final judgment of the Metropolitan Court of Budapest and ordered the court of first instance to conduct a new procedure. (Curia Kfv.V.37.595/2023/6.).

V.3. Use of voice analysis software, analysis of emotions, artificial intelligence and the prevalence of data subject rights

The Authority examined the Petitioner credit institution's data processing, according to which the Petitioner automatically analyses the recorded material of customer service calls based on the emotional status of the calling customer and the customer service employee and other characteristics of the conversation, and uses the result to decide which customer need to be called back. The Petitioner introduced the voice analysis application (the software) on 26 May 2017, stating that its purpose was to make the work of its staff more efficient, to prevent complaints by proactively calling the customer, to help shorten call times, to reduce the number of incorrect banking transactions, to ensure efficient customer service and to support the effectiveness of control procedures. It explained that the software prioritises calls in a closed system without storing any individual data suitable for identification, calls to be assessed are filtered according to defined rules and keywords, then calls are selected at random by senior staff from the list of calls proposed by the software for call-back, the software allows for individual replay of prioritised calls by clicking through them; caller identification is necessary for the handling of complaints.

In the contested decision, the Authority found that the Petitioner's data processing practices in relation to the analysis of the audio recordings under investigation infringed Articles 5(1)(a) and (b), 6(1) and (4), 12(1), 13, 21(1) and (2), 24(1) and 25(1)-(2) of the GDPR. It instructed the Petitioner to modify its data processing practices in accordance with the GDPR, i.e. 'not to analyse emotions in the analysis of the voice recordings and to ensure that the data subject's rights in relation to the processing are adequately safeguarded, in particular, but not limited to, the right to be informed and to object. With regard to employees, processing should be limited to what is necessary for the purposes for which it is intended and appropriate information should be provided to them, indicating the assessment criteria and consequences. A specific balancing of interests in relation to

the processing of data relating to employees for different purposes should address the vulnerable position arising from this dependence and appropriate internal safeguards should be specified in view of this. The applicant was also ordered ex officio to pay a data protection fine of HUF 250,000,000

As to the processing of data relating to the analysis of captured voice recordings, the Authority found that speech signal processing based on artificial intelligence is used to automatically analyse the emotional/mood status of the speaker; the processing is personal and sensitive, but does not relate to special categories of data within the meaning of Article 9(1) of the GDPR. In relation to the application of the GDPR, it was found that both parties to the call can be clearly identified in the system under investigation – customer service employees directly due to the storage of their names and the third party due to the identification of the person which is part of every call. Reference was made to the judgment of the Court of Justice of the European Union (CJEU) in Case C-582/14 and it was found that the emotional status recognised by the software and the data linked to the call identifier and telephone number also used in the software are personal data that can be linked to an individual person, and thus the GDPR applies to the processing of data using the software. With regard to the artificial intelligence used in the software, it referred to information available on the English and Hungarian websites of the company developing the software, stating that the software is capable of automatically evaluating received and initiated calls according to predefined rules, and therefore the software uses artificial intelligence to automatically process personal data, and consequently Article 21 of the GDPR also applies to the data processing in question. It also found profiling under Article 4(4), as dissatisfied customers are prioritised for call-back based on keywords and emotions.

Examining the information provided to the data subjects and the right to object, the Authority established that the data subjects were not given any information at the beginning of the conversation on the voice analysis, the automatic analysis and evaluation of emotions and the resulting possibility of a call-back, the Petitioner does not provide any information according to Article 13 of the GDPR, except for the legal basis, but the designation of the purpose was not complete either, because no reference was made to quality assurance, prevention of complaints or increasing internal efficiency. Due to the total absence of the right to object, there exists a breach of Article 21 of the GDPR, and thus consent would not be acceptable as a legal basis; the Petitioner infringed the provisions of Articles 5, 12-13 and 21 of the GDPR, as set out in the operative part of the decision.

With regard to the qualification of the balancing of interests, it pointed out that the lack of adequate prior information and the absence of a right to object renders the data subject's rights meaningless. The Petitioner has conflated the purposes of the processing and failed to confirm the effective examination of the alternatives, with special regard to the possibility for employees to object. The invalidity of the Petitioner's balancing of interests means that it is not possible to establish the primacy of legitimate interest in data processing. However, the application of the rules of automated processing according to Article 22(1) of the GDPR could not be established by the Authority. Due to the invalidity of the balancing of interests, it found that the processing by software was unlawful because there was no legal basis under Article 6(1)(f) of GDPR and no other legal basis exists, thereby also infringing Article 6(4) GDPR. In the context of the systemic breach of the rights of data subjects, with reference to Recital 47 of the GDPR, it pointed out that the conditions of foreseeability and guarantee were not met at systemic level because of the method of implementation chosen by the Petitioner. The Petitioner carried out data processing solely for its own commercial interests, excluding the possibility of choice for the data subjects, and it was unable to provide the complainant even basic information; thus, the data processing practice was also contrary to the provisions of Articles 12 and 24-25 of the GDPR, as highlighted in the operative part.

On 9 March 2023, the Metropolitan Court of Budapest delivered a final judgment in the case and, agreeing with the factual and legal position of the Authority, dismissed the Petitioner's action in its entirety, and the Curia refused to accept the petition for review submitted by the Petitioner.

V.4. Data protection implications of camera surveillance in a beauty centre

The core activity of the Petitioner company includes "services to improve physical well-being". The Petitioner offers its customers various beauty services in a beauty centre at its headquarters, where facial and body treatments and aesthetic medical procedures are carried out in two diagnostic rooms and fifteen treatment rooms. In total, 32 cameras were installed in the beauty centre during the period subject to litigation: two in the reception area, four in the corridors, one at the rear entrance, one in each of the two diagnostic examination rooms, one in each of the 10 treatment rooms and in each of the 5 VIP treatment rooms, one in the storage room, one in each of the two customer service rooms, one in the training room and two in the control office. The control office is a double room

with a camera in the other part of the room. The training room is used for company events and meetings and many of the employees also spend their lunch break in this room. There was another camera in the office of the labour manager and yet another in the so-called “interview” room. There was no information leaflet on camera surveillance at the reception. The cameras were accessible by software, which could be accessed by workers via an icon on the desktop of their computers. The recordings stored in the camera system could be exported in AVI format, which could be downloaded by any user who had access to the system using the software. The software could be opened on the business manager’s computer and live images from the installed cameras could be viewed continuously, and 24 hours of saved footage could be accessed by downloading for 7 days. The usernames - and passwords - of the managers’ computers were displayed on a piece of paper taped to the monitor. The saved camera footage showed the workers’ workstations, so that workers at each location could be seen and heard as they worked. The cameras in the treatment rooms showed the cosmetic beds in their entirety, without being covered, with the clients lying on these beds during treatment, with their upper bodies covered by a bath towel. The cameras also recorded sound in the treatment rooms.

By its decision, the Authority established that the Petitioner (1) infringed Article 5(1)(a) and (b) and Article 6(1) of the GDPR by continuously recording the work performed and monitoring the guests; (2) infringed Article 13(1)-(2) of the GDPR by providing incorrect and misleading information to data subjects in its prospectus and consultation form about the processing of their personal data; and (3) by failing to provide default settings for the operation of the camera system which minimise data processing, and the means necessary to ensure the highest possible level of protection of personal data, it infringed Articles 5(1), 24 and 25 of the GDPR and Article 32(1)(b) and (2) of the GDPR by failing to take system security measures; (4) by recording the health data of guests, it infringed Article 6 and Article 9(2) of the GDPR. The Authority ordered the Petitioner to pay a data protection fine of HUF 30,000,000 for infringements (1) to (4).

By its final judgment of 21 November 2023, the Metropolitan Court of Budapest dismissed the action brought by the Petitioner against the decision.

V.5. Curia judgment on the paramount moral and legal responsibility of the press and the domestic data protection law treatment of paparazzi activities

In its final judgment of 18 October 2023, the Curia also adopted a position in principle on the data protection issues related to those referred to in the title above. The Curia stressed that one of the consequences of social engagement and participation in public affairs is a lower level of the protection of privacy. However, the fact that the Petitioner in the case has been a prominent public figure for many years does not mean that their right to privacy can be disproportionately restricted and that all the data concerning their private life are public data in the public interest. Public figures also have a right to privacy.

According to the Curia, the person of a public figure or former public figure cannot in itself constitute a public or political debate, the nature of the article published in the press must be examined on a case-by-case basis in every instance, since the public figure's public role does not deprive them of their protection of privacy. According to the Curia, the publication of photographs and articles whose sole purpose is to satisfy idle curiosity or gossip hunger by disclosing the private life of the well-known Petitioner cannot be regarded as content which contributes towards a social debate in the public interest. In line with the relevant decisions of the Constitutional Court, the Curia has held that photographs of the Petitioner in the course of their private life, while doing housework in the garden, the description of this activity and of the Petitioner's appearance, current lifestyle and place of residence (private property) do not contain content of public interest contributing to the discussion of public affairs. A public figure is obliged to tolerate only in the context of their public activities.

In relation to the role of the press, the Curia expounded that increased protection for the communication of facts and information relating to public affairs applies in particular to the operation of the press, since the press has a constitutional mission to reveal events, circumstances and interrelationships that influence the development of public affairs and to bring them to the attention of the public. The free information activity of the media is the most important component of the modern democratic public sphere, and it is therefore of central importance that the press is able to carry out this task without uncertainty, compromise or fear. This is not to say that the press should not be subject to legal provisions. The activities of the press are extremely diverse, ranging from political reporting to sports, news on science and public affairs and even gossip. Journalism is different from any other activity. There is no single yardstick by which to judge

press products. According to the Curia, the data processing in question in the litigation at hand served the publication of a press product that clearly satisfied a “gossip hunger”. The Curia expressly emphasised that the Petitioner, as such a press product, essentially performs data processing operations, handling personal data. Therefore, it must make compliance with data protection rules part of its general practice and it must take into account the degree of compliance with data protection rules in all of its activities. This is of particular importance because of the key role of the written and electronic press in shaping the morals of society and of its individual members.

The Curia emphasised that if the press oversteps the limits set by law, it cannot be considered unlawful if the authorities and courts include this activity in their scope of investigation, and even prohibit and sanction the given conduct accordingly.

On the basis of the above, the Curia therefore agreed with the final judgment of the Metropolitan Court of Budapest in the first instance dismissing the Petitioner’s action, upheld it, including the HUF 10 million data protection fine imposed by the Authority on the Petitioner.

VI. The Authority's legislation-related activities

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

The number of the Authority's opinions stated in connection with legal regulations by the level of the legal source

Level of legislation/year	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
Act	33	79	85	82	72	61	73	77	68	78
Government decree	63	133	98	89	47	49	52	74	56	55
Ministerial decree	85	126	83	94	55	41	27	15	16	49
Government decision	21	61	29	33	40	34	22	14	4	8
Other (Parliament decision, instruction, etc.)	7	27	20	23	17	29	10	16	19	16
Total	**209**	**426**	**315**	**321**	**231**	**214**	**184**	**196**	**163**	**206**

Statistics of substantial observations made in the opinion of legal regulations

Nature of observations	Number of observations									
	2014	2015	2016	2017	2018	2019	2020	**2021**	**2022**	**2023**
Related to data protection	145	298	461	461	487	323	436	488	311	341
Information related to freedom of information	21	53	28	28	22	39	80	89	40	97
Other	53	137	92	92	79	78	37	9	26	36
Total	**219**	**488**	**581**	**581**	**588**	**440**	**553**	**586**	**377**	**474**

Pursuant to Section 8 of Act CXXXI of 2010 on Public Participation in Developing Legislation arranging for general consultation is mandatory in each case and the drafts issued for public consultation must be published on the dedicated website maintained by the government. The summary of the prior impact study specified in the Act on Legislation will have to be published together with the draft. Section 38(4)(a) of the Privacy Act authorises the Authority to make recommendations with respect to new laws and to the amendment of laws pertaining to the processing of personal data, the access to data of public interest and to data accessible on public interest grounds.

Unfortunately, in 2023, the Authority found on numerous occasions that the ministry preparing the draft law sent the proposal for an opinion only after it had been submitted to Parliament and put on its agenda. In such cases, even if there were serious objections to the proposal from a data protection point of view, the possibilities to amend the content of the proposal are limited to much narrower circle than before its submission.

Such a belated request for an opinion clearly does not comply with the Authority's right under the Privacy Act.

VI.2. Priority issues

VI.2.1. The amendment of the Privacy Act

In 2023, Parliament adopted several laws that amended the Privacy Act on a matter of substance. These included the following:

Act XXXII of 2023 on the amendment of Act CLV of 2009 on the protection of classified data and Act CXII of 2011 on the informational self-determination and the freedom of information re-regulates the provisions concerning the possible content of decisions adopted in authority procedures for the protection of confidential information. According to this, the Authority may examine the lawfulness of the repetition of the classification marking, and the law also provides for legal consequences in this respect. The Authority may find that the classification of national classified data has not been lawfully established, and in this case it may call upon the classifier to take appropriate measures to remedy the unlawful situation, i.e. to remove the unlawfully applied classification marking from the file.

The amendment also allows for the suspension of the procedure. Pursuant to Section 48(2) of Act CL of 2016 on the General Public Administration Procedure (hereinafter General Public Administration Procedure Act), the law may allow for the suspension of proceedings if the preliminary question falls within the competence of another body or if it cannot be decided on a well-founded basis without another decision of the same authority closely related to the given case. Previously, the Privacy Act did not provide for the possibility of suspension of the administrative authority procedure for the review of the data classification. If the Authority conducts an administrative authority procedure for the review of the data classification in a reclassification case, the outcome of the procedure may in some cases depend on the validity and lawfulness of the classification, which cannot be decided in the administrative authority procedure for the review of the data classification in the case of a reclassification, in which case the Authority will decide to suspend the procedure until another – separate – procedure on the lawfulness of the classification is conducted. Once this has been completed, the suspension of the reclassification procedure may be lifted and the procedure may resume. [NAIH-3370/2023]

Act CI of 2023 on the system for the utilisation of national data assets and certain services

The EU Digital Governance Act (DGA), which aims to regulate access to large public databases at European level, applies directly from 24 September 2023. Following the amendment introduced by Act CI of 2023, the Privacy Act designates the Authority as the competent authority responsible for the implementation of the DGA. In accordance with the provisions of the DGA, the Authority complies with the requirements that it is independent in the performance of its tasks, it is subject only to the law, it cannot be instructed in the performance of its tasks, it cannot seek guidance from any other person or body in the performance of its tasks, and it performs its tasks separately from other bodies and it is free from any influence.

The Act has laid down the basic procedures, together with their details, to be conducted under the DGA, with regard to the rights of the clients and the rules on competence, which complement the provisions of Act CL of 2016 on the General Public Administration Procedure. The Authority, upon request, registers data intermediation services providers, issues them with a certificate of compliance with the DGA and registers data altruism organisations, and, both upon request and ex officio, verifies the compliance of data intermediation services providers

and data altruism organisations with the DGA in an authority supervisory procedure.

This Act also added a new paragraph (2a) to Article 30 of the Privacy Act, according to which in the course of a request for data of public interest submitted to a public body, the public body may not be obliged to collect data not in its possession or to produce qualitatively new data in respect of data in its possession in order to fulfil the data request.

The Act has also supplemented the provisions on the procedure of the Authority in order to exercise its powers more effectively. In order to strengthen transparency and practices concerning access to information of public interest, the Authority carries out at least twice a year as well as in the event of a complaint, an audit of public and municipal entities under its supervision to determine whether they comply with the requirements on transparency of public data and access to information of public interest.

Act CXV of 2023 on certain authority issues

Act CXV of 2023 added a new paragraph (7) to Section 61 of the Privacy Act on the destruction of data affected by a decision of the Authority identifying unlawful data processing. Pursuant to Article 61(6) of the Privacy Act, the data concerned by the contested processing may not be erased or destroyed until the expiry of the time limit for bringing an action to challenge the decision or, in the event of administrative proceedings, until the final decision of the court. The reasoning behind this rule is that, in accordance with the general rule of the Act on the General Rules of Administrative Procedure, an action brought against a decision of the Authority does not have suspending effect, but it is an important interest that – according to the legislator's justification – the data concerned by the processing could not be erased or destroyed "in order to allow the dispute to be settled before a court".

The new paragraph (7) aims to provide for the fate of these data in the course of the implementation of decisions, i.e. if the availability of the data concerned by the erasure or destruction is still necessary for some other constitutional interest. Due to the implementing rules of the Act on the General Public Administration Procedure applicable to the Authority's proceedings, the statute of limitation for the execution of decisions is subject to a subjective time limit of 3 years and an objective time limit of 6 years. However, in practice, other proceedings of public

authority are often initiated in parallel with the proceedings of the Authority, either on the basis of the same facts of the case but under a different area of law (e.g. criminal law), or the availability of the data concerned by the erasure or destruction as evidence after the above time limits is still of fundamental interest either for the authorities (courts) or for the persons subject to the proceedings or the litigants. However, the duration of proceedings in other areas of law may well exceed the statute of limitation laid down in the General Public Administration Procedures for the Authority to order and implement enforcement. The new paragraph 7 ensures that no action concerning destruction or erasure of data in the course of enforcement would be necessary if such data were otherwise still needed in pending cases, which could even mean the destruction of evidence.

VI.2.2. Body camera on baggage handlers

The amendment to Act XCVII of 1995 on Air Transport, in force from 1 January 2024, provides for the mandatory processing of data by ground handlers at civilian airports through the use of body cameras worn by baggage handlers in the immediate vicinity of aircraft during baggage loading in order to protect air transport and to detect and prove infringements of the law affecting passenger property, in the vicinity of cargo doors, and in the cargo hold, during the baggage loading process. According to the justification of the law, if baggage handlers have unattended and free access to prohibited items checked in for transport in baggage by passengers in the hold, the airport area loses its safe designation. This makes it necessary to monitor the baggage handling process with cameras to ensure the sterility of the most sensitive internal security areas of airports, the so-called “security restricted areas”, and to guarantee the lawful handling of baggage, thus compliance with international and EU requirements.

In its opinion on the draft law, the Authority noted that, taking into account the purpose of data processing, it does not support the recording of sound, as it is not necessary or appropriate to achieve its purpose. [NAIH-9136/2023]

VI.2.3. Access to the post-mortem and autopsy report

The Hungarian Medical Chamber approached the Authority with a legislative proposal and asked for its support to further represent the proposal. The proposal, which has caused serious problems for general practitioners, concerns the accessibility of autopsy and post-mortem examination reports, and is based on the principle that the autopsy and post-mortem examination reports of deceased

patients should be accessible only to a person authorised by the deceased or, failing this, to the first close relative who so requests.

Paragraph (11) of Section 24 of Act CLIV of 1997 on Healthcare provides that in the event of the death of a patient, his/her legal representative, close relatives and heirs are entitled to get to know health data that are or may be related to the death and are in connection with the medical treatment that preceded the death, to inspect medical records and to make extracts and copies thereof, as well as to receive copies thereof at their own expense in the manner provided for by the Act on the Management and Protection of Health and Related Personal Data.

However, the Authority did not support the proposal as it would significantly restrict the rights of the deceased's relatives. It is easy to see that the adoption of the proposal would be a considerable relief for GPs, as the obligation to inform could be fulfilled in a single act after a minimum of verification of eligibility (verification of the power of attorney or of the status of close relatives), and this is undoubtedly in favour of the proposal. However, it would impose a restriction on the right holders which is legally unjustified, unnecessary and disproportionate to the objective pursued. It may be in the legitimate interest of other persons concerned to have access to the health data of the deceased after death, and this group of persons concerned is defined in the Healthcare Act as the legal representative, close relatives and heirs. There is no other interest on the basis of which the exercise of the right could be restricted, in contrast to the legitimate interest presumed by law. And the fact that, as the proposal states, the first of the close relatives – in practice, the first to arrive – should only be informed is expressly incompatible with the right to informational self-determination. [NAIH-3090/2023]

VI.2.4. Construction of a new penitentiary in Csenger

In November, the National Headquarters of Penitentiary Institutions informed the Authority that it was making a new investment. A penitentiary institution is to be built in the municipality of Csenger that will surpass the radical security developments of previous years. The unique penitentiary institution, equipped with modern technical, IT and security solutions, is scheduled to start its operation on 1 September 2024.

The Authority received the following information on the envisaged data processing solutions:

The primary means of identification of staff, detainees and other persons entering the facility will be a facial recognition system capable of tracking persons on the premises. The workload resulting from monitoring contacts, including phone calls and e-mails, would be reduced by using artificial intelligence, voice analysis, keyword monitoring, text analysis and facial image analysis. This would also require recording the voice of the detainee and the contact person. At the discretion of the commander of the penitentiary, detainee e-mailing could be authorised. This would both prevent the introduction of prohibited articles by mail and ensure that this method of contact can be easily monitored by IT.

Due to the proliferation of the use of drones, it is planned to detect unmanned aerial vehicles in the vicinity of the penitentiary institution and to prevent them from entering the airspace of the penitentiary in order to ensure the security of the penitentiary institution.

To support the work of staff, camera-equipped robot monitors could be used to monitor specific areas, prisoner wards, by following pre-programmed routes. The staff on duty would be provided with a transponder wristband, a specialised personal protection device, which would allow accurate positioning, and is capable of sending alarms and detecting health data. The wristband worn by detainees can be used for identification, but can also be equipped with other specific functions such as the detection of vital signs and location, and possibly later the supply of electronic signature.

For the time being, the Authority has only had the opportunity to familiarise itself with these innovations through a single presentation, while the analysis of the planned data processing has not yet been carried out. However, it is clear from the outset that the current legal environment does not allow for the introduction of all the planned innovations, and that the review and amendment of the legislation is essential for these.

VII. Annexes

VII.1. The financial management of the Authority in 2023

We have passed the 12th year of the operation and financial management of the Hungarian National Authority for Data Protection and Freedom of Information as of 31 December 2023. Below, we provide a brief presentation of the data related to its financial management.

VII.1.1. Revenue estimate and the data of its performance in 2023

The Authority received and accounted for other aid for operation and accumulation to finance the priority project "Mapping out the practice of the freedom of information in Hungary and enhancing its effectiveness".

Of the revenue data, the operating revenue of the Authority does not show any substantive change either in its composition or in its value relative to the financial year 2022.

Most of the non-operating revenues of the Authority arose from the sale of one official vehicle.

Converting the budget fund remaining from 2022 into a revenue estimate increased the original revenue estimate by HUF 92,976,000.
In addition to the initial budget support, the Authority received an additional HUF 145,000,000 from the central budget during the year to cover its staff and administrative expenditure, in approximately equal proportions.

VII.1.2. Expenditure estimates and the data of its performance in 2023

Based on the amendment to the Privacy Act at the beginning of 2023, the Authority's core activities have been extended to include a new task: it conducts transparency authority proceedings on the basis of notification and ex officio. The Authority has therefore received additional budget support to cover the additional expenditure. Payments to personnel and the expenditure on the related employers' contributions exceeded last year's data by no more than 6.7%. This increase has been influenced by further staff recruitment and an optimised, balanced and responsible wage management.

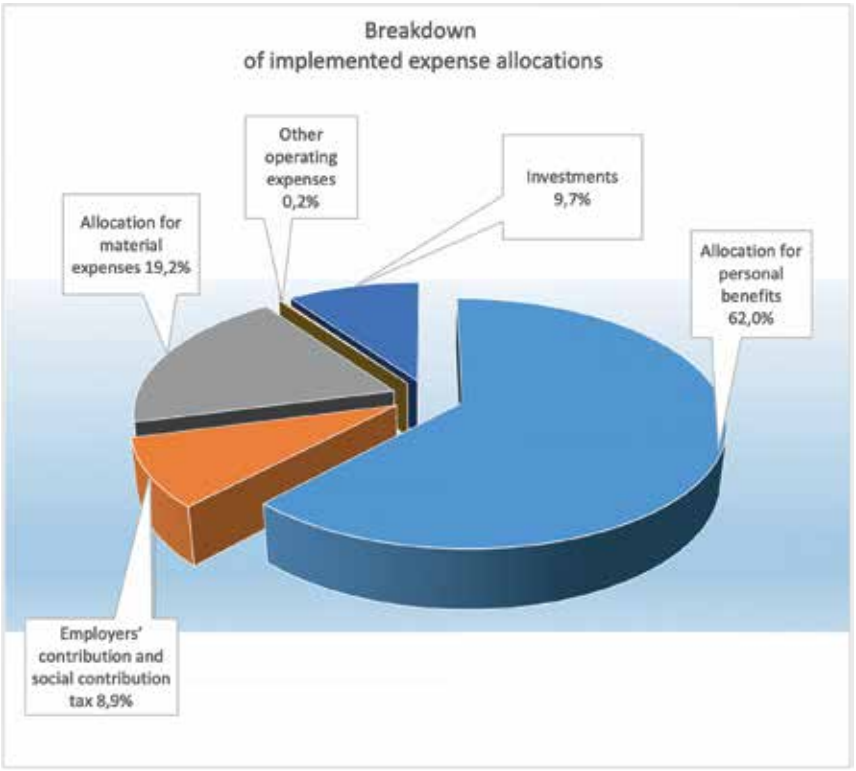
In 2023, two factors were of particular importance for the Authority's budget: the financing of expenditure on works upped by the rate of inflation and closely related cost savings that were constantly monitored. This year, several operational and maintenance expenses were incurred that did not arise in the previous budget year. Furthermore, it is worth highlighting that overheads have also multiplied for the Authority, which has been a major challenge in operational management. In 2023, NAIH hosted the European Data Protection Authorities Congress in Budapest with great success. The previously envisaged budget could be kept even though prices increased dramatically during this period.

Overall it can be stated that, based on the experience of previous years, particular attention has been paid to the cost optimisation of all contracts concluded, and negotiations have been held to recalculate prices where necessary.The analysis of accumulation expenditure shows that the Authority scheduled several works to restore the original condition of the building and value-adding investments, serving the safe and satisfactory operation of the Authority's basic activities for the long term for 2023. These activities were carried out with the permission of Magyar Nemzeti Vagyonkezelő Zrt.

Funds remaining from the Authority's budget related to its basic activities in 2023 amounted to HUF 98,823,000, the entire amount of which is subject to liabilities. The following table presents the figures for NAIH's 2023 budget (in HUF '000):

Description	Original estimate	Amended estimate	Per-for-mance	2023 re-mainder from basic activity
Operational other support from chapter		23,460	23,460	
Cumulation other support from chapter		48,077	48,077	
Value for mediated services		7	7	
Invoiced VAT		91	91	
Exchange rate gain		46	46	
Other operational revenues		3,812	3,812	
Reimbursement of expenses		7,696	7,696	
Sale of tangible assets		7,116	7,116	
Recovery of loan for non-operational purposes		1,629	1,629	
Funds remaining from the 2022 budget		92,976	92,976	
Grant from central budget from Managing Authority	1,624,500	1,769,899	1,769,899	
Revenue estimates total:	1,624,500	1,954,809	1,954,809	-
Estimates for payments to personnel	1,089,800	1,150,983	1,150,983	-
Employers' contribution and social contribution tax	146,700	165,358	165,358	-
Estimate for material expenses	388,000	454,351	355,528	98,823
Other operational expenses		3,735	3,735	-
Investment		180,382	180,382	-
Expenditure estimate total:	*1,624,500*	*1,954,809*	*1,855,986*	*98,823*

The following graph shows the actual expenditures of the modified estimates in a percentage distribution:



VII.1.3. Changes in the headcount of the Authority

As of 31 December 2023, the Authority's headcount according to labour law was 120.

Human resource management is based on positions according to the Act on Organs of Special Legal Standing, namely the Authority has four administrative job categories (councillor, lead councillor, main councillor I, main councillor II, head main councillor), and two managerial job categories (one heading an independent organisational unit and one heading a non-independent organisational

unit). Although the Authority has sought to provide competitive salaries for its staff since the introduction of the Act on Organs of Special Standing, high inflation and a difficult economic environment have led to high turnover in our organisation. During the year, 16 people left the Authority and 21 new colleagues entered. In 2023, 11 people were on long-term leave, and 1 returned from long-term leave.

VII.1.4. Changes in receipts from fines

The amount of the fines paid to the Authority's account totalled HUF 366,838,000, which was close to the record amount collected in the previous year. It should, however, be noted that receipts from fines constitute the revenues of the central budget, not of the Authority.

VII.2. Participation of the President of the Authority in Hungarian and international conferences and events of the profession in 2023

- 1 March 2023 – The opening event of the Energy Efficiency Green Project of the Hungarian University of Agriculture and Life Sciences Centre of Analysis for the Circular Economy - Gödöllő, Szent István Campus – *Data protection aspects of Artificial Intelligence*
- 18-21 April 2023 – Privacy Symposium – Venice, Italy – "*Two sides of the coin" - privacy and the right to freedom of information in the Hungarian legislation*
- 4 May 2023 – ELTE JOTOKI 50 Café Conference on Current issues of data protection – Budapest, Eötvös Lóránt University, Faculty of Law Institute for Postgraduate Legal Studies – *Data protection updates*
- 11 May 2023 – As part of the Spring Conference 2023 „Vulnerable individuals: tools for online protection. Children and age verification" workshop hosted by the Italian DPA – Budapest, Italian Institute of Culture – *opening address*
- 24 May 2023 – 3 ARB Data Protection Conference, 5 years of GDPR – Budapest, Stefánia Palace – *„GDPR turns 5" unconventional online interview*
- 31 May 2023 – A professional event hosted by the Association of the Hungarian Data Protection Awareness Society on the new generation of data protection professionals, the challenges and effectiveness of training – Budapest, MÁV Baross Gábor Training Centre – *roundtable discussion*

- 31 May 2023 – "Man amid the latest technologies" conference hosted by the Constitutional Court, the National Authority for Data Protection and Freedom of Information and the Information Society Research Institute of the National University of Public Service – Budapest, National University of Public Service, Training Centre – *Artificial intelligence and data protection: authority experiences*
- 5-7 September 2023 – 32nd Economic Forum „New Values for the Old Continent – Europe on the Threshold of Change" conference – Karpacz, Poland – *„Two sides of the coin" – privacy and the right to freedom of information in the Hungarian legislation*
- 27 September 2023 – "Parliaments at the gateway to artificial intelligence" conference hosted by the Legislative Directorate of the Parliament's Office – Budapest, the Delegation Chamber of Parliament – *Data protection aspects of AI*
- 4 October 2023 – Semmelweis Data Protection Forum – Budapest, Semmelweis University – *NAIH's procedures*
- 17 October 2023 –Compliance Conference hosted by the University of Debrecen – Debrecen, University of Debrecen – *Data protection and freedom of information in the corporate culture*
- 20 November 2023 – The online DPO conference of National Authority for Data Protection and Freedom of Information – Budapest, NAIH – *Novelties in information rights, 2023 statistics*
- 7 December 2023 – Acta Humana – The sustainability paradigm conference hosted by the National University of Public Service Environmental Sustainability Institute and the Editorial Board of Acta Humana – Budapest, National University of Public Service Orczy Street College – *opening address*
- 11 December 2023 – Human Rights Conference: In the grip of cancel culture and the woke movement – Budapest, Petőfi Literary Museum – *panel discussion*

VII.3. Winners of the NAIH medallion

Based on NAIH's rules 19/2012 on the Donation of the "*Medallion of the National Data Protection and Freedom of information Authority*", this medallion can be donated to whoever has reached high-level, exemplary achievements in the field of data protection, the right to informational self-determination and the freedom of information or has substantially contributed to the achievement of such results. The medallion made of silver is the work of Tamás Szabó goldsmith. It is

donated annually on the occasion of the Day of Data Protection and Freedom of Information.

In 2023, the medallion was awarded to *Hajnalka Szilvia Ledvina*, a teacher of mathematics, informatics and digital culture at the Baar-Madas Református Gimnázium for her dedicated and committed work in the field of children's privacy education and awareness.

VII.4. List of legal regulations and abbreviations mentioned in the report

- Data Governance Act: Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and the amendment of Regulation (EU) 2018/1724
- Regulation (EU) 2023/2854 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and the amendment of Directives (EU) 2017/2394 and (EU) 2020/1828
- Convention 108: Convention for the protection of individuals with regard to automatic processing of personal data done in Strasbourg on 28 January 1981.
- Act CXCV of 2011 on Public Finances
- AJBH: Office of the Commissioner for Fundamental Rights
- Act CXI of 2011 on the Commissioner for Fundamental Rights (hereinafter: Ombudsman Act)
- General Administrative Procedure Act, Act CL of 2016 on General Administrative Procedure
- Fundamental Law, Hungary's Fundamental Law (25 April 2011)
- General Data Protection Regulation: see: GDPR
- BRFK: Budapest Police Headquarters
- Criminal Procedures Act, Act XC of 2017 on Criminal Procedure
- BTLE, Borders, Travel and Law Enforcement Expert Group Additional activity of the Borders, Travel and Law Enforcement expert group
- Decree 14/2002. (VIII.1.) IM on the rules of court administration
- BVOP: Büntetés-végrehajtás Országos Parancsnoksága, National Headquarters of Penitentiaries
- Act CVII of 1995 on the Penitentiary Organisation
- Act CCXL of 2013 on the Execution of Penalties, Measures, Certain Coercive Measures and Detention for Misdemeanours

- CEF: Coordinated Enforcement Framework
- Charter: European Union Charter of Fundamental Rights
- CIS: Customs Information System
- CSC: Coordinated Supervision Committee (carrying out the joint supervision of the large information systems of the European Union)
- Digital Act: Act CIII of 2023 on the digital state and certain regulations on the provision of digital services
- DGA: Data Governance Act: Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and the amendment of Regulation (EU) 2018/1724
- DPF: EU-US Data Privacy Framework
- DSA: Digital Services Act, Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a single market for digital services and amending Directive 2000/31/EC
- ECRIS: European Criminal Records Information System
- ECRIS-TCN: centralised system for the identification of Member States having information concerning judgments against third country nationals and stateless persons), as well as those needed for the implementation of national part of the requirements in the European Union legal acts concerning the framework of interoperability between the information systems of the European Union.
- EDPB: European Data Protection Board
- EDPS: European Data Protection Supervisor
- EES: European Entry/Exit System
- EESZT: Healthcare Service Space
- EMÖI: Europol Magyar Összekötő Iroda: Europol Hungarian Liaison Office
- EPPO: European Prosecutor's Office
- E-privacy directive: Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)
- ETIAS: European Travel Information and Authorization System
- CJEU: Court of Justice of the European Union
- Eurodac system: European Dactylographic Comparison system
- Europol regulation, Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA

- Health Data Act, Act XLVII of 1997 on the Processing and Protection of Health and Related Personal Data
- Act CLIV of 1997 on Healthcare
- GDPR, General Data Protection Regulation: Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC.
- GVH: Economic Competition Office
- Act XCVII of 2013 on data processing by the defence forces and military administrative tasks in connection with meeting certain defence obligations
- Act CLXXXV of 2012 on Waste
- Act L of 2013 on the security of electronic information of central and local government bodies
- IMEI: Igazságügyi Megfigyelő és Elmegyógyító Intézet, Judicial Institute for Observation and Mental Treatment
- IMI system: Internal Market Information System
- Privacy Act, Act CXII of 2011 on the Right of Informational Self-Determination and the Freedom of Information
- KBSZ: Közlekedésbiztonsági Szervezet, Road Safety Organisation
- KEKVA: The goals and principles of Act on Public Interest Asset Management Foundations Discharging Public Duties (hereinafter: Public Interest Asset Management Foundation Act)
- Act CXL of 2004 on the General Rules of Public Administrative Procedures and Services
- Act LXIII of 1999 on the Supervision of Public Areas
- Act on Government Administration, Act CXXV of 2018 on Government Administration
- Act CXCIX of 2011 on Civil Servants
- Classified Data Act, Act CLV of 2009 on the Protection of Classified Data
- MBVK: Magyar Bírósági Végrehajtói Kar, Hungarian Association of Judicial Officers
- Municipalities Act, Act CLXXXIX of 2011 on Hungary's Municipalities
- NAVÜ: Nemzeti Adatvagyon Ügynökség, National Data Asset Agency
- NEBEK: Nemzetközi Bűnügyi Együttműködési Központ, International Criminal Cooperation Centre
- NSZI: Nemzeti Szociálpolitikai Intézet, National Social Policy Institute
- NSZKK: Nemzeti Szakértői és Kutató Központ, National Expert and Research Centre

- Act LXVI of 1992 on the Registration of the Personal Data and Addresses of Citizens
- OBH: Országos Bírósági Hivatal, National Office for the Judiciary
- OIF: Országos Idegenrendészeti Főigazgatóság, National Directorate-General for Aliens Policing
- Act XXV of 2023 on complaints, notifications of public interest and rules relating to the notification of abuse
- Act CXXX of 2016 on Civil Procedure
- Act V of 2013 on the Civil Code
- Scheval regulation: Council Regulation (EU) 2022/922 of 9 June 2022 on the establishment and operation of an evaluation and monitoring mechanism to verify the application of the Schengen Acquis and repealing Regulation 1053/2013
- Act XXIX of 2016 on forensic experts
- Act CXII of 1995 on personal income tax
- Act III of 1993 on Social Administration and Welfare Benefits
- Tromsø Convention, Council of Europe Convention on access to official documents (CETS No. 205., promulgated in Hungary by Act CXXXI of 2009)
- Act LIII of 1994 on Judicial Enforcement
- VIS: Visa Information System
- VIS decision: Council decision 2008/633/JHA of 23 June 2008. concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences
- VIS Regulation, Regulation (EC) No. 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas
-
- Other legal regulations:
- Directive 2009/103/EC of the European Parliament and of the Council of 16 September 2009 relating to insurance against civil liability in respect of the use of motor vehicles, and the enforcement of the obligation to insure against such liability
- Government decree 149/1997. (IX. 10.) on guardianship authorities and child protection and guardianship proceedings
- Act XXXI of 1997 on the protection of children and guardianship administration

- Act XXI of 2022 on data processing for national defence
- Act LXXI of 2009 on mandatory insurance against civil liability in respect of the use of motor vehicles
- Government Decree 499/2022 (XII. 8.) on the detailed rules of the Central Information Public Data Register
- Act CLXXXI of 2007 on the transparency on public grants from public funds
- Government Decree 499/2022 (XII. 8.) on the detailed rules of the Central Information Public Data Register
- Act CXXII of 2009 on the More Economical Operation of Business Organisations in Public Ownership
- Decree 18/2005 (XII. 27.) IHM on the publication models for the publication of data in the publication schedules
- Act XCVII of 1995 on air transport
- Act CLXXXV of 2010 on media service and mass media
- Classified Data Act, Act CLV of 2009 on the Protection of Classified Data
- Act CI of 2023 on the system of utilisation of national data assets and certain services
- Decree 16/2014 IM on the detailed rules for the enforcement of imprisonment, detention, pre-trial detention and detention in lieu of a fine
- Act LXXIV of 2016 on the protection of the townscape
- Act CLXXXIV of 2005 on the technical investigation of traffic accidents on the railways and waterways and other traffic incidents
- Act CLXXXIII of 2005 on rail transport
- Decree 24/2012. (V.8.) NFM on the detailed rules for the technical investigation of serious railway accidents, railway accidents and unexpected railway incidents and for investigations by the operator of the vehicle
- Act LXXXI of 2001 on the Promulgation of the Aarhus Convention
- Act CLIV of 1997 on Healthcare
- Act XLIII of 2023 on the promulgation of the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, signed at Strasbourg on 28 January 1981, as amended by the Protocol of 10 October 2018 signed at Strasbourg
- Act CXV of 2023 on certain authority issues
- Act CCXXII of 2015 on the General Rules for Electronic Administration and Trust Services
- Government Decision 1538/2018 (X. 30.) on the establishment of a working group coordinating the government measures necessary for the development of the European Entry/Exist System (EES) and the European Travel Information and Authorization System (ETIAS)

- Regulation (EC) 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93
- Act CXXXI of 2009 promulgating the Council of Europe Convention on access to official documents
- Decree 31/2008. (XII. 31.) IRM on the activities of forensic experts
- Decree 78/2012. (XII.28.) BM on the adoption of a single filing plan for municipal offices
- Act LXXVIII of 1993 on Certain Rules for the Renting and Disposal of Dwellings and Premises, regulating the use of and the rules governing the use of immovable property owned by the municipality
- Act CXXII of 2021 on the amendment of certain laws on justice and related matters

Table of Contents

Nemzeti Adatvédelmi és
Információszabadság Hatóság

1055 Budapest, Falk Miksa utca 9-11.
Postal address: 1363 Budapest, Pf. 9.

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

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

Published by: Nemzeti Adatvédelmi és Információszabadság Hatóság -
Hungarian National Authority for Data Protection and Freedom of Information
Responsible publisher: Dr. habil 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. habil Attila Péterfalvi president
ISSN 2063-403X (Printed)
ISSN 2063-4900 (Online)