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

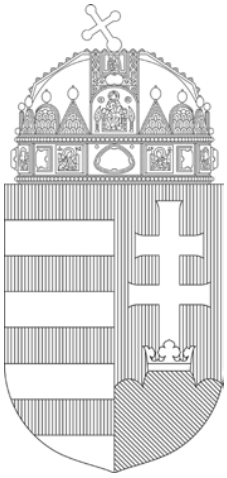
for Data Protection and Freedom of Information)

on its activities in 2023

B/7156

EXTRACT – FOI Chapters

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

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 per- son, the prevention of making notes or copies, the problems related to the ma- chine 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 rejec- tion 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 con- cerning 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 pub- lic 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 inter- est 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 transparen- cy 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.

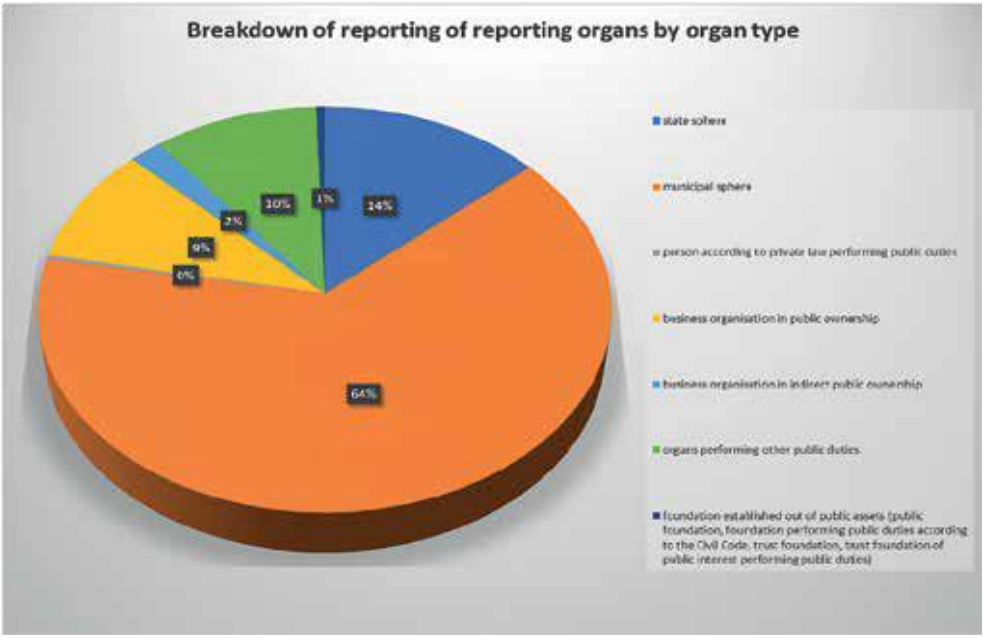
In the rather short period available for preparation between the promulgation of the regulation (22 December 2023) and its entry into force (1 January 2024), the Authority took every measure to apply the regulation efficiently and smoothly.

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.

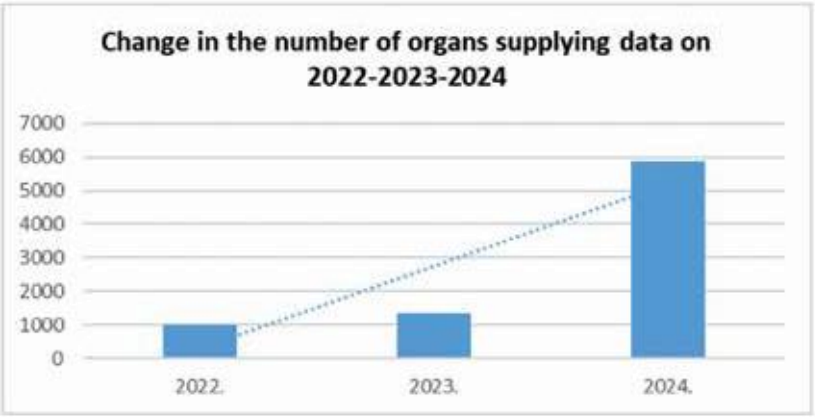
Following the preparations, the Authority received reports from **altogether 5,895** organs. The reporting obligation applies to the following organ types:

- 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.



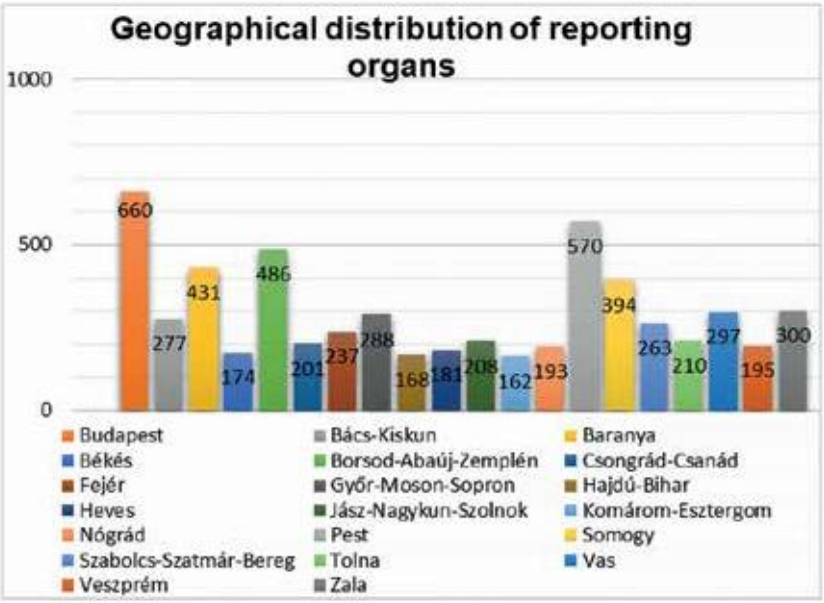
Looking back to preceding years, there was a major increase in terms of the reporting obligation to be complied with in 2023 relative to 2021 and 2022 because of the change in the legal regulation described above as reports were received from 997 organs in 2022 and 1,350 in 2023.



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

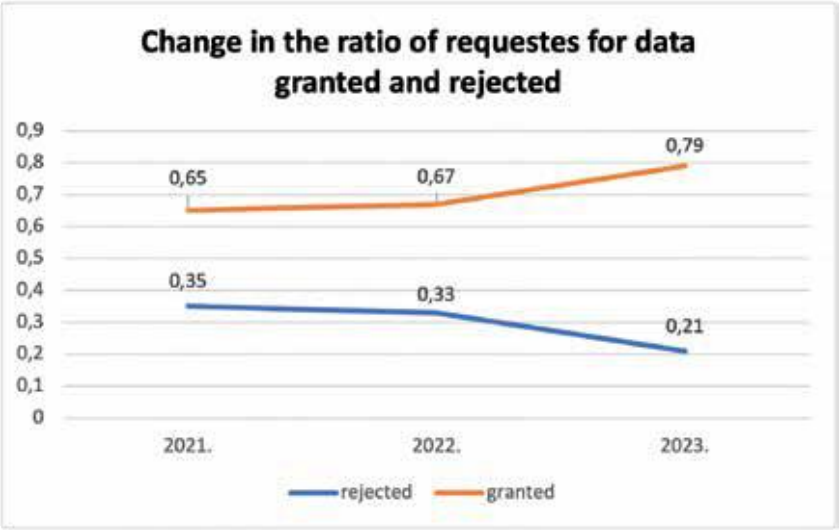
Besides the 432 local governments and their organs, 15 minority governments submitted reports on 2021; 584 local governments and their organs and 25 minority governments submitted reports on 2022. Reports on 2023 were submit- ted by 2,612 local governments and their organs, 870 budgetary organs founded 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).

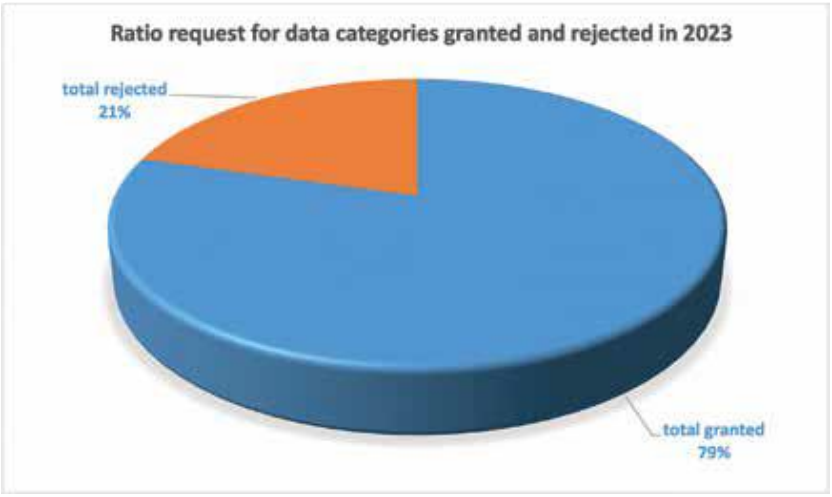


Similarly to the increase in the number of reporting organs, the ratio of requests for data of public interest granted and rejected showed a positive change relative to the data of the preceding years.

- 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.



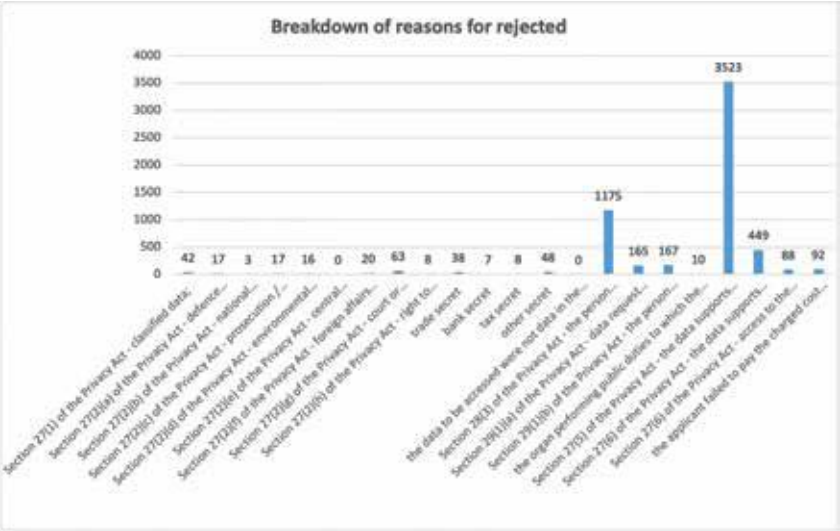
The expansion of the content of the reporting, which entered into force on 1 January 2024 showing the number of data requests submitted in the given year and the average number of days spent on meeting the data request, shows a more detailed picture of the practice of organs performing public duties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



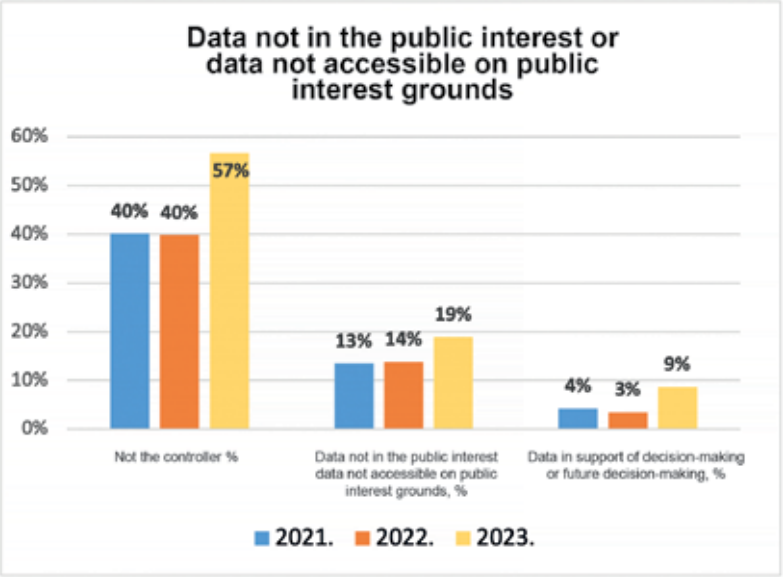
The reasons given by the organs performing public duties for excluding access to data were the following:

- 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).

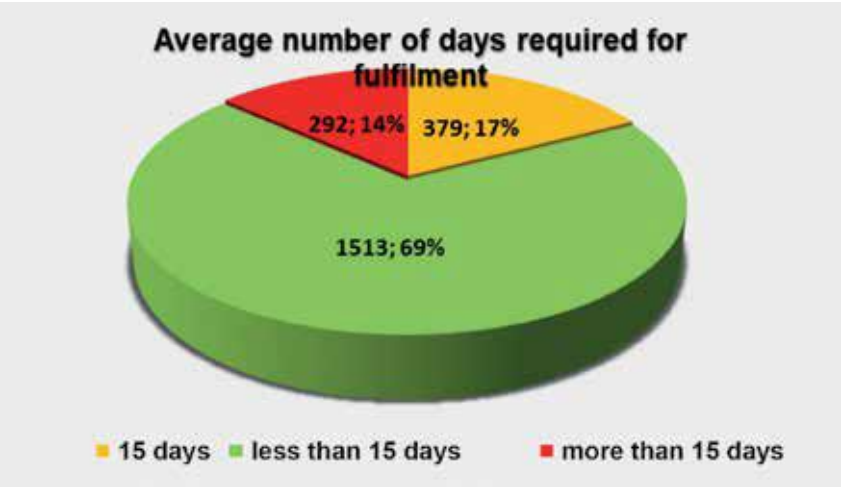


The reasons for rejection most frequently quoted in the previous years (2021, 2022) were also quoted in the first place in the 2023 reports. In terms of the use of reasons for rejection, one item differed substantially (17%) from the practice in preceding years: data not processed by the organ to which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

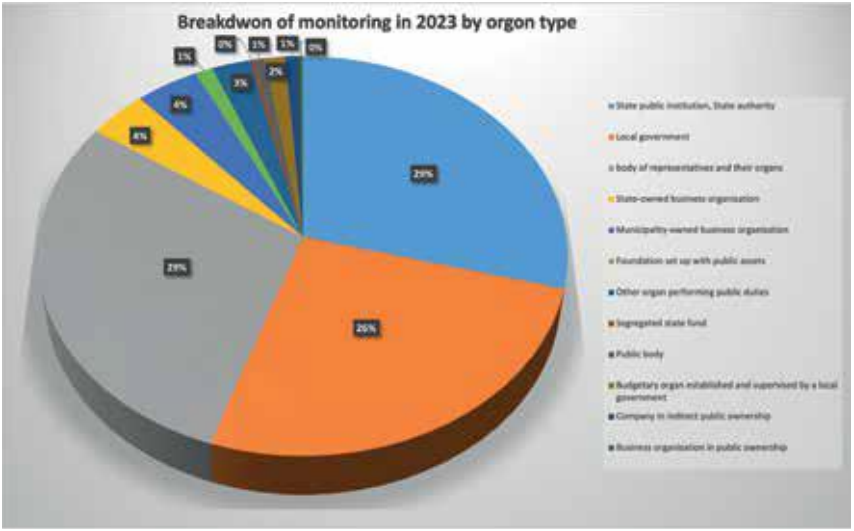
Of the organs (2,184) which received requests for accessing data of public interest, 69% (1,513) answered the request in less than 15 days; for 17% (379) this period was 15 days, and for 13 % (292) this period exceeded 15 days.



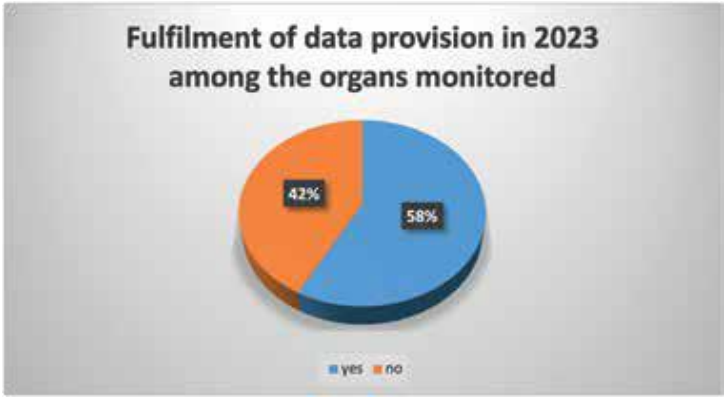
III.1.2. *Statistical data of the Authority's freedom of information monitoring activities in 2023*

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%).

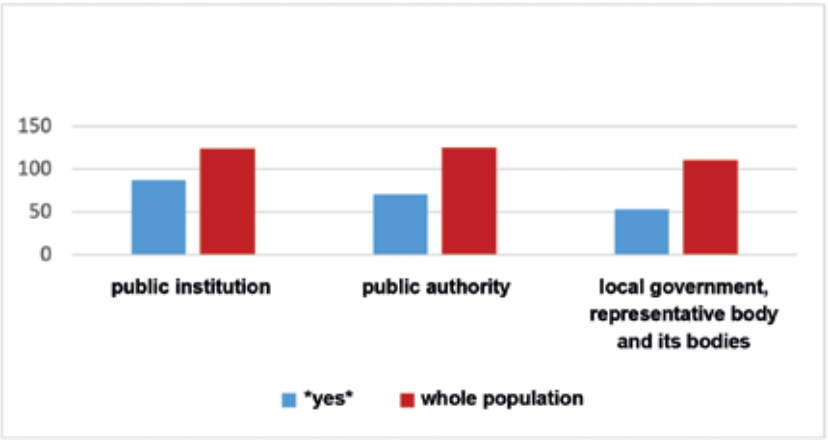


Of the monitored organs, 58% complied with and 42% failed to comply with their reporting obligation according Section 71/D(4) of the Privacy Act.



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 pro- cedures 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 termi- nated 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.

2 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 or- gans 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 en- tered 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 be- cause 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 pro- vide data as set forth in Section 37/C of the Privacy Act, because it was a frame- work 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 con- tract. However, the Privacy Act does not contain a provision that the full consid- eration 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) actu- ally 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 finan- cial 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 col- lected 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 imple- mented 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 obliga- tion 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 pos- sible to conduct searches in the database, for instance, we can learn which min- istries 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 unconstitution- ality 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 accessi- bility of dual nature data, held by Eximbank, i.e. data of public interest(or acces- sible 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 in- terest grounds held by Eximbank that performs public duties and manages public funds, so the Constitutional Court called upon the Parliament to meet its legisla- tive 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 deci- sion, the Constitutional Court established that OBH as an organisation manag- ing 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 ben- efits 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 can- not 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 gen- eral 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.3.3. *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 documenta- tion 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 petition- er 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, ir- respective 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 peti- tioner qualify as data of public interest, the capacity of the respondent as control- ler 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 per- sonal 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 inter- est. 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 perform- ing 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 per- sonal 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 grant- ing 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 infor- mation 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 ac- cessible 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 re- spondent. As a justification for denial, the respondent stated that it had to pro- duce 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 pro- cedure 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 consti- tutional interest in accordance with the justification of the Constitutional Court Decision (paragraph [56]). Pursuant to the Constitutional Court Decision (para- graph [58]), the fact that the requested information of public interest is not avail- able 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 re- ferred 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 sort- ing according to specific criteria and arranging them in tables cannot fundamen- tally 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 informa- tion "is ready and available". The respondent failed to present any other spe- cific 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 statis- tics 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 ac- cess 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 justifica- tion 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.3.3.1. 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 sup- porting decision-making; instead of the document principle, the data principle has to be applied; the controller may not invoke so-called "criteria of conveni- ence"; the decision rejecting the data request must be justified in terms of con- tent 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 docu- ment 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 with- out undue external influence, such in particular the free expression of its views generating the data during the preparatory stage of decision-mak- ing.[...]

As the Curia also accessed the content of the report, it upheld the position tak- en 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 com- mon 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 pub- lic 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 obtain- ing 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 rejec- tion 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, cer- tain 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 accessi- ble 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 gradu- ation from a doctoral school and his professional skills. Based on the legal reg- ulations 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 qual- ification 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 con- sent. 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 an- swer, the mayor had disclosed his school qualifications in the course of the elec- tion 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 cover- ing 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

3 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.

4 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 compli- ance 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 mem- ber, 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 guar- anteed 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 municipali- ties 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 munici- pality), i.e. the Government Office within the scope of its performance of pub- lic 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 inter- est 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, accessi- ble 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 municipal- ity was subject to investigation. The body of representatives of a city munici- pality 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 ex- ists. 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 accessi- ble 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 po- sition 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 ac- cess 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 organisa- tion 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 accessi- ble 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 authoriza- tion based on the rules of the Privacy Act.

Based on the practice of the court, it is also incorrect to interpret the legisla- tion, "when the organ performing public duties interprets the regulation under the Privacy Act and the General Administrative Procedures Act in a *lex gener- alis – 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 accord- ing 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 accord- ance 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 adminis- trative authority procedure in the case subject to the notification and that the re- quested 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 ob- tain 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 informa- tion 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 pub- lic 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 competi- tion 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 quali- fies 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 disap- peared. 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"*[5]. 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

5 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 condi- tions. 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 evalu- ated 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 ques- tion 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 du- ties has doubts concerning the issue of raw data, they should notify the request- ing 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 vacan- cies 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 teach- ing positions filled in, the number of persons pursuing educational and teach- ing 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 acces- sible 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 qualifica- tions 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 anoth- er 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 le- gal 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 request- ing 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 en- trusted 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 no- tions of personal request for data or data request for private interest. If the sub- ject 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 objec- tives 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 be- fore 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 man- age 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 accord- ing 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 circum- stance 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]

6 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 substan- tially in 2022 – it is no longer an autonomous decision of the institutions of ter- tiary 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 transac- tion 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 is- sue (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 associ- ated 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 compli- ance 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 pub- lic 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 mil- lion 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 so- ciety, 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 posi- tion 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 reg- ister 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 can- not be applied to provide data from the authority records; data from these re- cords 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 compli- ance 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 re- cords 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 accessi- ble 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 af- fairs that are important for public opinion, whose accessibility is not part of pro- viding 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 bail- iffs) 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 al- ready 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 per- sonal 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 interpret- ed. 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 pub- lic 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 re- ceives 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 fi- nancial background for the company's operation stems not only from its com- mercial 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 com- ply 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 re- quires 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 investigat- ing 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 web- site, 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 re- sults 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 en- forced, which means that the parts of the sound recording with regard to which there are justified reasons for excluding access as substantiated by the control- ler had to be edited or distorted by the controller prior to disclosure. The control- ler 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 integ- rity 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 no- tified 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 control- ler 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 con- troller 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 re- questing 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 wish- es 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 appear- ance 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 representa- tives 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 commit- tee 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 allow- ance to the Office's cashier, indicating the legal title for the repayment. The mu- nicipal 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 inter- est 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 un- der 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 break- down 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-ar- ranged 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 du- ties 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 requir- ing 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 superviso- ry 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 deter- mine 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, af- ter 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 pro- ceedings 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 per- son 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 neces- sity 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 re- gard 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 trans- parency 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 disclo- sure 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 disclo- sure 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 classifica- tion 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 ef- fect. 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 pub- lic 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

7 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 informa- tion, 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 clas- sified 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]

Table of Contents