FOI Chapters of the Annual Reports – 2022

List of contents:

1. Introduction

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

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

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

First, major changes were made to the rules of fees for meeting requests for data of public interest with a view to easing access to data of public interest; the amendments to the Privacy Act and the Cost Decree entered into force on 13 October 2022[1]. The possibility of requesting fees because of the disproportionate use of labour resources regulated in Section 29 of the Privacy Act was deleted and with regard to the remaining cost elements (the cost of the data storage medium/making copies and the costs of delivery), the implementing decree established limits. Hereinafter, the costs of labour resources shall be borne in full by the organs performing public duties processing the data (data owners). In the case of costs not exceeding the minimum amount (HUF 10,000) set forth in Section 6 of the Cost Decree, no fee can be applied to cover the costs, while in the case of costs above this, the maximum amount that may be charged is HUF 190,000. There is no change in that only actually incurred - i.e. verifiable - costs may be covered by the fee and it should be underlined that charging a fee will not be mandatory in the future, it may only be done if the organ performing public duties processing the data decides responsibly to apply the rules concerning the establishment of the fee to cover the costs. In such a case, the request for data shall be fulfilled within 15 days from the payment of the fee by the requesting party.

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

As a result of the amendment adopted on 22 November 2022, a Central Information Public Data Registry was set up, which enables access to the most important financial management data of budgetary organs in an integrated central database, in particular, the data of budgetary support amounting to at least five million forints granted by them from domestic or European Union funds, public procurements, contracts and payments which are updated every two months and will be accessible for 10 years. The Registry enables the classification and comparison of the data. Obligees are to disclose the data generated on or after 29 November 2022 for the first time by 28 February 2023 at the latest. The mode and accurate content of the disclosure are set forth in Section 37/C of the Privacy Act and Government Decree 499/2022 (XII. 8) on the detailed rules of the Central Information Public Data Registry. The reports are to be filed using a downloadable datasheet in accordance with the Guidance in the User Rules[2]. As the operator of the new registry, the Nemzeti Adatvagyon Ügynökség Kft. publishes the data on the workday following the receipt of the datasheet. If a budgetary organ fails to meet its obligation to disclose the data on this platform, or discloses inaccurate or deficient data based on request the Authority launches *an authority procedure for transparency or may launch an authority procedure for transparency ex officio*. The period open for conducting a new authority procedure is 45 days. In the event of an infringement, the Authority orders expedited meeting of the disclosure obligation, which shall not be later than within 15 days. If the budgetary organ still fails to comply within 15 days, the Authority may impose a fine whose amount may extend from a hundred thousand forints to fifty million forints. Requests for launching a transparency procedure may be submitted to the Authority from 28 February 2023.

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

---

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

[2] https://kif.gov.hu/#/regulation

3. Important decisions of the Constitutional Court in 2022

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

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

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

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

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

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

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

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

The petitioner NGO made a request for data of public interest to a ministry in which it requested copies of reports on the Öveges-program project and the Bridge to the World of Work project investigated by the European Anti-fraud Office (OLAF) submitted to the Government and all other information or data concerning OLAF's and the Government's common position on these projects. The controller refused to issue the data stating that according to the Court of Justice of the European Union OLAF's investigative documents are entitled to a general protection, on the basis of which it was exempted from public access to the documents and only substantial public interests may allow for an exception. The court of first instance rejected the petition and established that an omission on the part of the respondent ministry with regard to the consultation to be conducted with the director general of OLAF may not automatically result in an obligation to issue the data. The reason for this is that in the absence of consultation, the director general of OLAF is entitled to make a decision on the issue of the data. The court of second instance taking action as a result of the petitioner's appeal upheld the judgment of the court of first instance. In its judgment, it established that in relation to the investigative reports, the ministry only carries out coordinating activities, which is not the same as any of OLAF's activities, thus the requested data were generated not by the ministry and not in relation to the performance of its public duties, hence the ministry is not under an obligation to make them accessible. In its judgment, the Curia upheld the force of the final judgment and established that *"the respondent [...] had a legal position concerning the rejection of the issue of the data worthy of examination"*, which the Curia also regarded as being well-founded, when by reference to the indicated European Union regulations through their interpretation, it arrived at the conclusion that *"the director general of OLAF is entitled to make the decision on the issue of the data"* (Curia judgment Pfv.IV.20.948/2020/6, Justification [20]–[21]). According to the opinion of the Constitutional Court, the question whether the court correctly interpreted the EU legal requirements applied and whether, on that basis, it justifiably identified OLAF in the present case as the organ entitled to make the decision is an issue of the interpretation of specialised EU law, whose review would be outside the Constitutional Court's duty to protect fundamental rights, even if it would otherwise disagree with the legal interpretation of the court.

4. Important court judgments in 2022

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

concerning the fact that national security interest obtained. In view of this, it was mandatory by force of the law for the respondent to refuse to issue the data without any additional consideration, hence the Curia found the petition for the review the final judgment submitted by the petitioner ungrounded.

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

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

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

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

Pf.20.117/2022/6.: The petitioner requested the issue of the vaccination plan against COVID-19 from the National Public Health Centre. The vaccination plan requested by the petitioner is included in the document entitled "*Schedule of tasks related to vaccination against COVID-19*" published by the Ministry of the Interior on its website. Following the launching of the litigation, the respondent referred to this and provided the electronic link to the document. The court pointed out that by reference to a public source, an organ performing public duties may fulfil a request for data, even if it was not that organ that had earlier made the information accessible to the public. It is not contrary to the purpose of the Privacy Act, if the controller voluntarily meets its obligation to provide data in the course of litigation; voluntary performance is in place also in the case of litigation, but when fulfilling a request for the issue of data in the course of litigation, the enforcement of the request cannot be regarded as unnecessary, hence the respondent was ordered to reimburse the petitioner's litigation costs.

Pf.20.213/2022/8.: In his request for data of public interest, the petitioner requested data of public interest from the respondent related to the tender grants provided by the respondent to two limited companies. Within 15 days, the respondent informed the petitioner that based on Section 1(3) of Government Decree 521/2020. (XI. 25.), it will

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

Pf.20.066/2022/5.: The petitioner requested data concerning an EU tender for agriculture, forestry and food processing. According to the respondent, some of the requested data are not public because according to Section 24(1) of Act XVII of 2007 on Certain Issues of the Procedure Related to Agri and Rural Development and Fishing Grants and Certain Measures (Agri Aid Act), the data generated or recorded in the procedure of the controller are not accessible as a main rule except for the data according to paragraph (2), for which the Agri Aid Act requires a quarterly disclosure obligation in any case (www.palyazat.gov.hu and www.magyarallamkincstar.gov.hu). The court of first instance ordered the respondent to issue all the requested data because the provisions under Section 24(1) and (2) of the Agri Aid Act are not consistent with any of the reasons for refusal under Section 27(2) of the Privacy Act, hence the provisions of the sectoral legal regulation are irrelevant from the viewpoint of the fulfilment of the data request. The respondent appealed and presented that the two directly applicable EU regulations provide as follows: according to Article 111 of Regulation (EU)1306/2013 only the data specified therein need to be disclosed on the beneficiaries of a grant, while according to Recital (32) of Regulation (EU)908/2014 publication should not go beyond what is necessary in order to reach the transparency objectives pursued. According to the respondent's appeal, the part of the data request on "*who evaluated*" the tenders and "*who carries out control*" cannot be the subject matter of request for data of public interest as these are the personal data of civil servants. The Court of Appeal referred to the fact that in its Decision Pfv. IV.21.093/2020/5 the Curia clarified: Section 24(1) and (2) of the Agri Aid Act may not restrict the range of accessible data of public interest and data accessible on of public interest grounds. Hence, the Court of Appeal had to examine whether it would have been right to differ from the decision of the Curia in a legal issue based on the appeal. In relation to the EU regulations referred to, the Court of Appeal pointed out that they regulate the obligation to publish and do not contain any prohibition as to providing access to additional information related to tenders upon special request in addition to the data which are mandatorily published. The names, responsibilities and duties of the persons evaluating and controlling tenders are data accessible on of public interest grounds of civil servants according to Section 26(2) of the Privacy Act. In view of all this, the Court of Appeal upheld the decision of the court of first instance.

Pf.20.023/2022/10.: The court of first instance ordered the respondent to issue the calculations made in accordance with the requirements of Section 133(2) of Act CXLIII of 2015 on Public Procurement in a context of the announcement of the concession tender for motorway operating services and the related data substantiating compliance with the relevant legal requirements (all other data substantiating the 35-year period of the contract according to the invitation to tender) to the petitioner. The court pointed out that it does not follow from the fact that the Public Procurement Act does not require the accessibility of the data that they could not be accessible as data of public interest. Concerning the nature of the data supporting decision-making both paragraphs (5) and (6) of Section 27 of the Privacy Act are applicable in the legal dispute, because the announcement was published based on the calculation preceding the announcement, i.e. a decision has already been made, but the calculation and the related data substantiating compliance with the relevant legal requirements also support future decisions as the concession tendering procedure continues even after sending the invitation to tender, and the preliminary calculation is finalised when the contract is concluded. When applying Section 27(5) of the Privacy Act, the controller should have carried out the public interest balancing test according to Section 30(5) of the Privacy Act. In this context, for the court's discretion it is necessary for the controller to enclose the data concerned by the data request as a sealed document in the lawsuit, with regard to which it is warranted to restrict access according to its own consideration; if respondent fails to do so, it is also unable to comply with its interest in providing evidence. Because of this, the court upheld the decision of first instance.

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

Pfv.20.040/2022/5.: The petitioner's data request was primarily aimed at having access to the loan contract between the Government of Hungary and the Export-Import Bank of China and secondarily, in the event of a dismissal of the data request, to the specific information the minister has considered and the foreign policy and

foreign economic interests that would be jeopardised by the disclosure of the loan contract. The court pointed out that under Section 27(2)(f) of the Privacy Act, an act may restrict access to data of public interest in view of external relations. Section 2(3) of Act XXIX of 2020 promulgating the Convention on the investment for the reconstruction of the Budapest-Belgrade railway (hereinafter: BB Railway Act) specifies that the issue of data shall be refused for 10 years from the generation of the data, if access to the data would jeopardise Hungary's foreign policy and foreign economic interests free from undue external influence, and according to Section 2(4), the minister in charge of foreign economic affairs shall decide on whether or not a request to access the data can be fulfilled and on the disclosure of the data, having weighed Hungary's foreign policy and foreign economic interests and also obtaining the position of the Government of the People's Republic of China. In view of Article 3(8) of Act XXIV of 2016 promulgating the Convention, the minister is bound by the statement of the Chinese party: "[...] *Information provided by the parties to one another of this Convention or generated as a result of the Convention implementation shall not be disclosed and shall not be transferred to any third party without the prior written consent of the two parties."* According to the court's decision, the minister has no obligation to justify his considerations as the BB Railway Act does not specify the criteria of consideration as it is within the discretionary powers of the minister; the court may not review the minister's consideration as that has no legal basis. The court annulled the final judgment ordering the respondent to fulfil the request for data of public interest and upheld the judgment of first instance rejecting the petitioner's petition.

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

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

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

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

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

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

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

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

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

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

7. Personal data accessible on public interest grounds

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

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

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

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

Otherwise, the refusal to disclose the data has to be justified, i.e. the petitioner has to be informed why the data is not accessible on public interest grounds, or why it is not related to the discharge of public duties by a person performing public duties, or why the data clearly belong to the protected private sphere of the data subject. In addition, the established case law of the courts and NAIH has also to be taken into account. The provisions concerning access to data of public interest have to be applied to accessing data accessible on public interest grounds; in the absence of a provision for publication, these data can be accessed through data requests.
In addition, it is an important requirement to which the attention of controllers must be called in every case that personal data accessible on public interest grounds may be promulgated respecting the principle of purpose limitation. The provisions of Annex 1 of the Privacy Act and separate acts concerning the legal status of persons discharging public duties govern the publication of personal data accessible on public interest grounds on websites. According to the justification of the amendment of 2013: "*Although the rules on accessing data of public interest are to be applied to access such data, the nature of these data as personal data remains in spite of their accessibility, as the most important safeguard of data protection, the data requirement of the principle of purpose limitation must still be upheld and enforced in full in the course of the subsequent use of the personal data already published. At the same time, purpose limitation cannot be an impediment to the freedom of the press. The act intended to constrain the use of publication obviously contrary to the original intent of the legislator, such as the publication of databases containing personal data within the framework of the law."*

To the extent that the processing and accessibility of data accessible on public interest grounds is needed for the transparency of public affairs and for the democratic discussion of public matters, processing (necessary and sufficient) in line with this also qualify as lawful under the GDPR [Recital (153), Article 17(3)(a), Article 85 and Article 86] provided that it is done with the appropriate legal basis and purpose. Establishing to what extent the data processed relate to the performance of public duties or to what extent they are part of privacy to be protected requires separate consideration in each case. In the justification of its Decision 443/D/2006. AB, the Constitutional Court expounded that "*it is not in itself sufficient for a restriction of a fundamental right to be the constitutional (...)that it is done to protect another fundamental right or freedom, or with a view to some other constitutional purpose, it is also necessary that it complies with the requirements of proportionality: the importance of the purpose to be achieved and the seriousness of the infringement of the fundamental right caused for that purpose must be in proportion to one another.*"

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

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

The Hungarian Medical Chamber (MOK) requested the Authority's position on MOK's recommendation for the transparency of medical ethics procedures, the constraints of implementation in the current legal environment and the law amendments needed for implementation[3]. GDPR Article 86 provides that: *"Personal data in official documents held by a public authority or a public body or a private body for the performance of a task carried out in the public interest may be disclosed by the authority or body in accordance with Union or Member State law to which the public authority or body is subject in order to reconcile public access to official documents with the right to the protection of personal data pursuant to this Regulation."*
In its earlier statement,[4] the Authority expounded that it follows from the joint interpretation of Section 26(2) of the Privacy Act and Section 112 of Act CLIV of 1997 on Healthcare (Healthcare Act) that if an ethics procedure initiated in the context of a physician performing his public duties (for instance, fraud in the context of medical activity) was closed, then the right to informational self-determination of the person performing public duties may be restricted. With a view to the fulfilment of a request for data of public interest, it is necessary to distinguish whether the ethics procedure conducted by MOK concerns and if so, to what extent, the performance of public duties by the physician. When a decision bought as a result of the ethics procedure is made accessible to fulfil a data request, the disclosure has to be restricted to the content relevant to the performance of public duties by the physician. According to the regulations in force, the fact of a final penalty imposed under an ethics procedure, the date when the decision

[3] https://naih.hu/dontesek-infoszab-allasfoglalasok?download=504:allasfoglalas-az-orvosetikai-eljarasok-transzparenciajara-vonatkozo-javaslatrol
[4] Statements NAIH/2017/1936/5/V and NAIH/2017/1936/10/V

imposing the penalty becomes final and an indication of the date of its statutory limitation as other personal data related to the performance of the public duties of physicians qualify as data accessible on public interest grounds. The legal situation would be clearer, if the Act (such as an amendment to Section 112 of the Healthcare Act) were to determine which data of the ethics procedure can be accessible through data request. For the time being, the publication of these data on websites is not required by any legal regulation, i.e. they do not qualify as personal data accessible on public interest grounds. *(NAIH-1715/2022)*

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

A legal adviser asked for information on the interpretation of the aggregated data on personal allowances paid to persons employed by public bodies (Privacy Act, Part III (Management Data), Annex 1, disclosure unit in point 2). According to judicial practice, if by virtue of the nature of the work, the activity can be carried out not only on the basis of an employment relationship but also under some other legal relationship aimed at the performance of work, in view of the principle of the freedom to contract, the parties can freely decide on the type of contract (civil law contract or employment contract) for the work to be carried out. Because of this, the range of persons employed and the full publication of the data related to the use of public funds in relation to them should be interpreted broadly with a view to proactive freedom of information. In view of the above, all the circumstances of the case should be considered to establish whether the public funds paid in lieu of the legal relationship and the performance of tasks by a given person were used for the purposes of his/her employment. Under the law, in the case of employees, the number of persons (headcount) receiving payment from the given organ has to be disclosed quarterly (every three months) together with the total amount in forint terms. In the case of managers, it is also quarterly (every three months) that the number of persons in managerial positions or senior officials is to be stated at the given organ, and what is the amount paid to them in total (as wages or dues). Furthermore, if they received regular benefits, then what the total amount paid by the organ for these benefits was, and over and above these, what cost reimbursement they received and what the total amount paid for this during the given period was. Point 3 of the publication unit covers every employee not in a managerial position. It is also quarterly that their benefits received from the given organ (personal and other benefits) and their total amount during that period is to be stated. The text of the statement is available in full in the website[5] *(NAIH-933/2022)*

The request for data concerning the disclosure of wage data of employees making use of the work time allowance due on trade union work at a public transportation company was lawfully rejected. Employees carrying out trade union work at the company are not in the category of persons performing public duties, in view of the fact that these activities are not included in the functions and powers of the company providing public services. In addition to this, there is no legal provision currently in force that would ensure the accessibility (accessibility or publication) of the personal data of persons carrying out trade union activities. Although Section 2(1) of Act CXXII of 2009 on the Economical Operation of Business Organisations in Public Ownership (Public Company Operations Act) classifies the data listed therein as accessible on public interest grounds and also provides for their publication, this, however, does not automatically render other personal data processed by organisations or companies discharging public duties accessible on public interest grounds. The requested data may be made accessible in a cumulative form or in a manner unsuitable for the identification of persons. *(NAIH-3353/2022)*

8. "Post-Covid"

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

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

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

Section 15 of Act XLVII of 1997 on the Processing and Protection of Healthcare Data and Related Personal Data and the provisions of Decree 1/2014 (I. 16) EMMI on the order of reporting infectious diseases provide a clear legal framework for the collection of epidemiological data on infectious patients. However, any conclusion to be drawn from the raw set of data or answering any professional questions arising and/or data requests is only possible after the appropriate validation and analysis of the data, which includes the correction of accidental errors and the comparison of individual data fields with the help of computer programs in order to identify conflicting information.

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

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

Data concerning vaccinations are recorded in a separate interface in the Electronic Healthcare Service Area (hereinafter: EESZT). This means that data on infected persons and data on vaccination are located in two different databases. (In the meantime, a so-called Master Table was generated from the two databases.) The system includes only the location of the vaccination, not the place of residence. There was no time to enter additional data, the primary objective was a rapid recording of the data. One of the fundamental problems and source of errors of data entry was that the system did not provide an opportunity for the automatic entry of the patient's personal data - i.e. entering these data from the accurate and creditworthy healthcare database already available through an interface. Thus, the physicians and healthcare providers admitting the patients had to key in the data manually, increasing the errors arising from erroneous data entry. The ratio of erroneous data concerning the cause of death exceeded 30 percent, and only the data on the dead are validated, hospital care data are not. Another important aspect is that it is not possible to isolate, if a hospital patient is also Covid-19 infected, but the reason for his/her hospital care is not this, as the Covid-19 infection would not otherwise require hospital treatment. In individual cases, the physician providing care could sort these out, but at other times this is not professionally possible, and this may change also from hour to hour for any patient.

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

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

8.2. NAIH's inquiries

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

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

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

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

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

In addition, the Authority examined what data NNK was required to transfer every week to the pandemic- evaluation register based on Section 2(3)(a) of Government Decree 333/2021. (VI.10.) in force at the time of making the request. The obligation to forward data applied only to the data of the PCR findings and not to the place of treatment or those requiring hospitalization. With respect to hospitalized Covid patients and those requiring treatment by ventilator, the Authority accepted NNK’s justification and established that in view of the fact that NNK did not have the requested data, there was no infringement when it rejected the request for these data. The Authority also requested information from EMMI about the statistical analyses it received from the National Health Insurance Fund Manager (NEAK) pursuant to Section 2(2) of the decree. According to the provision referred to, NEAK in collaboration with NNK, OMSZ and OKFŐ produces statistical analyses supporting vaccination strategy, which it sends inter alia to the minister for human resources on a weekly basis. The Authority has found that the questions in the data request cannot be answered from these analyses, because they concerned the vaccination data of those infected by Covid in general, and did not contain data concerning the hospitalization, mechanical breathing support and death of the infected patients. Because of this, the Authority accepted EMMI’s justification and established that in view of the fact that EMMI did not have the requested data, there was no infringement. The Authority found the same with regard to the Prime Minister’s Office for the same reason. Although the data request did not concern NEAK, the Authority also requested information from NEAK, which explained that it only had data on deaths in publicly funded hospitals in Hungary , but it failed to confirm, despite repeated requests, whether the requested data are available to NEAK concerning those treated and deceased in publicly funded hospitals in Hungary. *(NAIH-2597/2022)*

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

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

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

9. The transparency of municipalities

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

9.1. The accessibility of criminal data

The accessibility of criminal personal data is a recurrent problem [see Constitutional Court Decision 3177/2022. (IV. 22.) AB presented], and this was also discussed in last year's report: the fact in itself that a criminal procedure is in progress in relation to a case does not exclude the accessibility of all of the documents. Based on judicial practice, the body of representatives of a municipality may put cases on its agenda, in relation to which a criminal procedure is in progress; however, in view of the provisions of Section 27(2)(c) and (g) of the Privacy Act, the preliminary opinion of the investigative authority, the prosecution or the court taking action in a criminal case (depending on the phase in which the criminal case is) has to be obtained before the session with regard to the pending criminal procedure, which data of the case are subject to the conditions excluding accessibility ; also appropriate organisational and technical (data security) measures have to be taken during the preparation and holding of the meeting to ensure that the data indicated by the organs taking actions in the criminal case are not made accessible to the public. Following anonymisation depending on the answer of the organs contacted, the data may be promulgated while respecting the requirement of purpose limitation in processing. *(NAIH-4668/2022)*

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

According to another complaint, a business organisation fully held by the municipality of a city with county rights, which manages public funds and performs public duties, failed to fulfil the request for data of public interest concerning the organisation's transparency report because a criminal procedure was in progress in relation to that

report. When contacted by the Authority, the police station taking action in the criminal case stated that the criminal procedure was no longer in progress when the data request was submitted, thus access to the document could no longer violate the public interest in conducting the criminal procedure. *(NAIH-1099/2021)*

9.2. Self-governments of ethnic minorities

Also as part of the KÖFOP research project, the Authority studied and analysed the enforcement of freedom of information in relation to the self-governments of ethnic minorities; the positions of the professional managing organs as well as of the government offices were solicited and the Deputy Commissioner for Ethnic Minorities was also involved in the comprehensive inquiry. Summarising the investigations of specific individual cases, the signatories of the joint report[6] consider it appropriate that the municipal executive and the staff of the mayor's office should actively cooperate in the mandatory electronic publication - i.e. the publication of the relevant documents in the appropriate publication units - and in the fulfilment of requests for data of public interest. The performance of these tasks presupposes mutual, efficient and ongoing cooperation regulated by an agreement based on consensus as well as by internal rules. It is also necessary that the legislator expressly provide, among the mandatory content elements of the administrative contract, for the tasks promoting the transparency of self-governments of ethnic minorities and their distribution in Section 80(3) of Act CLXXIX of 2011 on the Rights of Ethnic Minorities (hereinafter: Ethnic Minorities Act). In the future, informative and case management processes supporting the fundamental work of the self-governments of ethnic minorities, including the development of information and training materials and, in this context, the organisation of personal and online training courses which similarly to the representatives of municipalities provide adequate knowledge and information to the representatives of the self-governments of ethnic minorities with a view to the transparent operation of the self-governments, will have major importance. *(NAIH-8317/2022)*

The municipal executive of a municipality, which also has an ethnic minority self-government, invited the position of the Authority concerning the person of the controller in relation to a request for data of public interest (aimed at accessing data on the emoluments of representatives, employment on public works, contracts of assignment and other wage-type payments). Taking the definitions of the Privacy Act as the point of departure, in this case the ethnic minority self-government is the organ which, in the course of its operation, generates data of public interest and data accessible on public interest grounds and it follows that the ethnic minority self-government is responsible for the data. The Authority established that the data to be accessed through the request for data of public interest were processed by the various organisational units (organisation and administration, compliance, finance, audit and internal supply) of the mayor's office, even though they relate to the operation of the ethnic minority self-government. As the performance of public tasks by an ethnic minority self-government is affected under the professional supervision of the municipal executive through the various organisational units of the mayor's office, according to the position of the Authority, the fulfilment of the requests for data of public interest is also the task of the mayor's office managed by the municipal executive. *(NAIH-166/2022)*

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

9.3. The transparency of statements of assets

Interest for the statements of assets of mayors and representatives of municipalities, as well as self-governing bodies of ethnic minorities continue to be keen[7]. The statements of assets of mayors and municipal representatives are data accessible on public interest grounds, which must be made accessible to anyone by way of data request. *(NAIH-6476-2/2022)*

Because of the high number of data accesses based on individual requests, several municipalities wished to make decisions on the publication of these data in organ-specific publication schemes and therefore, in compliance with

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

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

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

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

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

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

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

9.5. Financial management data

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

The complainant wished to access data related to the use of a property held by the municipality subject to local protection. Following the calls of the Authority, the controller municipality made the contracts available to the complainant, but the information related to the financial conditions and the names of persons administering the transaction - representatives of business organisations, law offices - were blocked. The Authority called the

attention of the municipality to the fact that the data of business organisations and undertakings entering into business relationship with the municipality and the data of the law office, as well as of the person representing it. are data of public interest or data accessible on public interest grounds. As the municipality failed to respond to the calls of the Authority, a public report was issued on the case. *(NAIH-221/2022)*

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

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

9.6. Data accessible on public interest grounds, personal data

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

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

Municipal representatives obtain their mandates enjoying the confidence of the majority of voters, this underlies their responsibility for the entire municipality, including the representatives' rights and obligations. The quality and effectiveness of the work of the municipality depends fundamentally on the work of the municipal representatives, so exercising the rights of representatives is also an obligation: to appear, to prepare, to ask questions, to make comments, to vote responsibly, to comply with the confidentiality obligation, to maintain contact with voters and to behave in a manner worthy of public activities. Thus, the representatives' votes cast on the individual items of the agenda at a public session of the body of representatives are data generated in relation to their discharge of public duties and are data accessible on public interest grounds, the votes cast by roll call can be displayed on the display showing the results of the vote. *(NAIH-6902/2022)* The accessibility of the votes of representatives cast in private sessions is restricted by secret ballot according to Section 18(4) of the Municipalities Act. *(NAIH-5501/2022)*

A representative made a video and sound recording using his mobile phone prior to the opening of the session of the body of representatives and shared the recording in a public Facebook group. The complainant explained that persons not qualifying as public actors (municipal executive, deputy municipal executive, heads of the departments of the mayor's office) also participated in the session of the body of representatives, and the purpose of the controller was to discredit the session of the body of representatives and of the municipal representatives and make

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

In a case related to the amendment of the local building code of a municipality, the Authority found unauthorized processing because of the publication of the decision of the body of representatives on residents' request submitted for the review of the settlement development concept and the settlement planning instruments, and called upon the municipality to remedy the infringement found. With respect to proposals made within the framework of partnership reconciliation with names and other personal data, it is not the citizen who submitted the proposal that is relevant, but the content of the proposal is important for the municipality's decision-making. Because of this, the publication of the identity and personal data (name, address, other identification data) of the person making the proposal cannot be regarded as necessary either when considering the proposals, or when developing the final decision or when publishing the decision. *(NAIH-5736/2022)*

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

10. Freedom of expression - on-line transparency

A complainant objected to being included in a publication of an NGO dealing with events suspicious of corruption. In his view, the publication was on the one hand based on untrue articles and on the other hand it placed the collected information into a new context and drew untrue conclusions from them. The controller informed all the data subjects of the processing prior to its commencement. The information provided said that the primary legal basis of processing was Article 6(1)(e) of the General Data Protection Regulation because the petitionee functions as a foundation for public benefit, its goal is inter alia to map out problems of corruption, informing the public, checking whether expectations concerning transparency were met and facilitating transparency, particularly in view of the use of public funds. Publishing the publication serves this purpose and therefore constitutes an activity of public interest. Secondarily, in view of the practice of the Authority, the petitionee also indicated Article 6(1)(f) of the General Data Protection Regulation and also carried out a balancing test in this context. First and foremost, the Authority stated that data protection supervisory authorities will not and may not take action in cases subject to the competence of civil courts and the right to the protection of personal data cannot become an instrument of restricting opinions hurtful to the data subjects and (perceived to be) unlawful from the viewpoint of civil law. Accordingly, the Authority did not and could not examine the petitioner's allegations concerning untruthfulness and defamation. At the same time, by indicating two legal bases for the same processing operation, the controller violated the principle of transparency. The Authority accepted the legitimate interest of the controller as the legal basis of processing with the provision that although the petitionee acted superficially in assessing the circumstances of the petitioner and in the balancing of interests and did not do everything in order to examine the consequences of processing, particularly those concomitant with accessibility, with regard to the individual life situation of the petitioner, the deficiencies exposed in relation to the balancing test did not reach the level enabling the establishment of an infringement in view of all the circumstance of the case and the purpose of processing. In this regard, the Authority took into account in particular that the petitionee carries out activities of public benefit as an NGO. Furthermore, the Authority established an infringement of Article 21(4) of the General Data Protection Regulation, because, in its information, the petitionee listed the right to object in the same sentence as the other rights of data subjects, mentioning only that a data subject has a right to object, although pursuant to the General Data Protection Regulation, the controller has to display the information related to the right to object clearly and separately from all other information. *(NAIH-1047/2022)*

In another case, the complainant objected to the fact that the information displayed on the datasheet of the one-man law office bearing his name included data referring to negative credit events on a company information website. In the course of the procedure, the Authority had to decide whether the data of the one-man law office qualify as the personal data of the lawyer. The Authority based its decision on the fact that in the event of a legal

person, such as the law office, the legal person and the natural persons behind it can be clearly delineated and although a natural person takes action by necessity on behalf of and in the interest of the legal person, this does not warrant classifying legal facts related to the legal person as part of the private sphere. Doubtless, the relationship between the natural and the legal person in the case of a one-man law office is much closer, yet even in this case the subjects of the law are clearly separate, the rights and obligations of the law office can be clearly separated from those of the member of the law office as a natural person. The Authority also referred to Recital (14) of the General Data Protection Regulation, which clearly states that the Regulation does not cover the processing of personal data, which concerns legal persons. In view of this, the Authority rejected the petitioner's petition. *(NAIH-740/2022.)*

11. The transparency of environmental data

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

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

Also in the area of access to environmental information, one of the most frequent reasons of rejection is reference to supporting decisions pursuant to Section 27(5)-(6) of the Privacy Act. It is a general problem that the holders of the data maintain automatically the restriction of access to data supporting decision-making even after the decision has been made, although by then the main rule is the accessibility of the data. In the public procurement procedures concerning the development of Lake Fertő Aquatic Centre I (Procedure 1) and the development of the Lake Fertő Aquatic Centre II (Procedure 2), the draft contracts demanded the use of an Llc specified by name to perform the monitoring tasks. The notifier requested the tourism development non-profit company (hereinafter: Zrt.) to provide the details of the procedure concerning the selection and use of the Llc. According to the Zrt., the data of the procedures in progress are data supporting decision-making and thus they are not accessible until the selection of the winning bidder. At the time of the data request, Procedure 1 was already closed, hence the Zrt. incorrectly referred to Section 27(5) of the Privacy Act. Procedure 2 was still in progress at the time of the data request. Despite this, the Authority did not accept the Zrt.'s reference to Section 27(5) of the Privacy Act, because the specification of the content of the public procurement documentation also qualifies as "decision", including that the draft contract constituting a part of the documentation named the Llc. as performing monitoring. The data supporting the decision to select it and the public procurement document - as the decision on launching the public procurement decision was already made and the announcement of the procedure was already published - are accessible to the public as a main rule. The Zrt. failed to accurately specify the legal regulation that prohibits the issue of public procurement documentation in the event of a request for data of public interest and in what way the accessibility of data concerning the selection of the company for monitoring and of the public procurement documentation would jeopardize the closure of the procedure - i.e. its justification did not exceed the level of generalities. When carrying out the balancing test based on Section 30(5) of the Privacy Act, according to the Authority's position, the fact that the data concerning the selection of the company for monitoring qualifies as environmental information based on Section 2(c) of Government Decree 311/2005. (XII.25) is of particular importance. The requirement of monitoring serves the protection of an area, which is part of world heritage, it is a protected nature conservation area, it is part of the Natura 2000 network, it is a special bird protection area and a natural conservation area of outstanding importance, there is therefore an overriding public interest in the accessibility of the data concerning the selection of a company doing it. *(NAIH-4719/2022)*

An NGO submitted a data request to the National General Directorate of Water Management (hereinafter: OVF) in relation to the Lake Fertő Aquatic Centre. The subject matter of the data request was a letter by the regional water management directorate containing a statement that the final state planned by the contractor would enable the performance of their specialised tasks in the beach zone. In OVF's view, if it had to presume in all its internal correspondence that it was likely to come to the attention of a third party, the communication would cease to be able to transmit certain data, facts and statement, which would significantly hamper the activities of the organs of public administration or even render it impossible. The Authority does not doubt the public interest in restricting the accessibility of internal communications among organs of public administration. However, the fact whether the organ's decision was already made or not, is of fundamental importance in restricting public access. Based on

Section 27(6) of the Privacy Act, they have to assume that even internal correspondence could be accessible to the public if they cannot substantiate why they believe that access to their internal correspondence would jeopardise the lawful functioning of the organ or the performance of duties without undue external influence. Future decisions will also have to be accurately specified and they have to be made within the foreseeable future, so the Authority did not accept OVF's statement that the requested letter "*would qualify as a document serving as the basis for responding to any other requests from citizens*". *(NAIH-3894/2022)*

Another notification objected to the fact that the protocols and testing data from the testing of sub-surface waters by a company and the testing of the monitoring wells located on one of the premises of the company submitted to the Budapest Disaster Management Directorate (hereinafter: Directorate) and the documents of the authority investigations of the company's premises by the Directorate were not issued. According to the information provided by the Directorate, the requested data were uploaded to the OKIR system. Similarly to the notifier, the Authority also experienced that there was no possibility to query the data because the database "*was under development*". The Directorate also explained that with regard to the data uploaded to the OKIR system, the controller according to Section 3(9) of the Privacy Act was not the Directorate, hence it was unable to forward data from the database. Pursuant to Section 2(a) of the Regulation, the results of sub-surface monitoring qualify as environmental information. The Privacy Act does not specify as a condition of fulfilling data requests that the organ performing public tasks determine the purpose of processing the requested data. Furthermore, neither does the convention on access to information, public participation in decision-making and access to justice in environmental matters adopted in Aarhus on 25 June 1998 (promulgated by Act LXXXI of 2001) subject the issue of environmental information to a condition of the same content specified in Section 3(9) of the Privacy Act. The Directorate sent numerous monitoring documents to the Authority, hence these data were processed by the Directorate and were obviously generated in relation to its activities, so they have to be issued to the person requesting them, while blocking the data to be protected in view of the fact that they were not accessible from the public source indicated. Information about the data does not replace the issue of the data. In relation to public access to the requested statements of the specialised authorities, the Authority explained that environmental information in general consists of objective data and facts, in the case of which – particularly once the decision was made – it is highly questionable whether their accessibility would frustrate the efficient implementation of the decisions or jeopardise independent and effective work by civil servants, free from undue external influence. The Directorate should have carried out the balancing test required under Section 30(5) of the Privacy Act and should have presented its criteria and results to the Authority. The Authority called upon the Directorate to send the monitoring results, the requested protocols and statements by specialised authorities to the notifier. However, the Authority terminated the investigation because in the meantime, the notifier also launched a court procedure. *(NAIH-252/2022)*

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

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

12. Public education, higher education

Inquiry into a number of data requests addressed to School District Centres were put on the agenda, which were related to education-related social problems and debates. The most significant of this was the complaint of the Teachers' Trade Union (hereinafter: PSZ) because of rejecting requests for data of public interest – *how many colleagues working in public education and vocational education were on sickness benefit, for altogether how many days they were absent, how many employment relationships were terminated and of this, how many people retired or diseased between 1 January and 30 June 2021* – submitted to the Hungarian Treasury (MÁK), the 60 School District Centres and the 40 Vocational Training Centres. After 90 days, in their letters rejecting the data request, the contacted organs referred to not processing the data in the requested format, they could not be required to generate them, and they also made reference to Constitutional Court Decision 13/2019. (IV. 8.) AB, which stated that "*the controller is not under an obligation to collect data, or to generate new, qualitatively different data or data series by way of the comparison of the data it processes*. *Furthermore, the person requesting the data may not claim a right to have somebody else query the data, which are otherwise accessible."* In the course of its inquiry, the Authority found that a substantial part of the data requested by the notifier were processed by these organs and the Constitutional Court Decision referred to may not be applied as reason for rejection because the data need not be generated by physically searching one by one for sickness benefit documentation and death certificates and other documents as they have been available electronically and could be obtained from the databases and payroll programs processed by the employers with a simple IT operation. Moreover, in an earlier period, MÁK already provided the data indicated in the petition for inquiry to the notifier and the legal environment has not changed since then.
In this case, the Authority contacted and sent several calls and orders to the Klebelsberg Centre (KK), the National Office for Vocational Training and Adult Training, MÁK, the Ministry of Human Resources, the Ministry of the Interior, the Ministry of Culture and Innovation, the Office of Education and to all the School District Centres and Vocational Training Centres of Hungary. In its response, the Ministry of the Interior explained in detail that the school district as employer processes the data related to the personal remuneration of teachers; with regard to sickness benefits, the school district as employer records the absence data of public employees (e.g. the fact of incapacity for work and its duration) in the centralised payroll system (KIRA) and forwards the medical documents related to incapacity for work to MÁK.
However, in the absence of legal authorisation, the school district does not record the specific reason for incapacity for work. Thus, concerning the issue of how many employees were on sick leave or received sickness benefit as a result of viral infection, the employer does not have recorded data. The data processed by the school districts can be generated using mathematical and IT operations. The data sets indicated are processed by the organisational unit of the school district in charge of human resources, the average headcount of those working there is 5 to 6 people per centre. The generation of the data by the school district is possible by querying KIRA and the SAP HR module of the KRÉTA administration system and by sorting them in Excel tables. This means that the data that the trade union requesting the data wished to access were existing recorded data actually processed by the school districts, except for whether the reason for the sickness benefit was coronavirus infection, and they can be retrieved from the databases of the school districts by electronic query. In this case, based on the Fundamental Law, the Privacy Act as well as the relevant decision of the Constitutional Court, the school district is under an obligation to meet the request for querying the data according to specific criteria and organising them in a table. Ultimately, the school district centres and the vocational training centres complied with the Authority's call and issued the requested data of public interest to the notifier. *(NAIH-235/2022, NAIH-237/2022, NAIH-3649/2022)*

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

In another group of cases, also a Member of Parliament turned to the Authority because of the negative response of the Ministry of Human Resources (EMMI). The notifier would have liked to know the number of students commencing and successfully completing training, providing the qualifications and skills needed to fill the post of a teacher, and the number of those newly entering the teaching profession in academic years 2020/2021 and 2021/2022 in a breakdown by kindergarten/school. With regard to the first two questions EMMI stated that it did not have the data in the absence of competence and with regard to the third question, it referred to Constitutional Court Decision 13/2019. (IV. 8.) AB. The data requested by the notifier are data of public interest, which the notifier in July 2019 had already received retroactively for 9 years for the period 2010-2019. In the course of its investigation, the Authority found that the notifier was not informed of which organ performing public duties processes the requested data, or of the fact that with regard to the 3rd question the data are available from October. Furthermore, the notifier requested the data not for each kindergarten and each school, but for teachers in kindergarten and school – i.e. he requested two data each with regard to the two years mentioned, , so based on

the above, the Authority called upon EMMI to send the latter data to the person requesting them free of charge and without delay. The data in points 1 and 2 of the data request can be requested from the Ministry for Innovation and Technology (hereinafter: ITM), which the notifier did and turned to ITM and the Office for Education.
In its response, ITM explained that according to their position, EMMI informed the Authority not about who qualifies as controller with regard to the requested data, but indicated that the area of higher education and vocational training as a special area now belong to the scope of responsibilities and powers of ITM. So, they again informed the notifier that ITM does not qualify as controller according to Section 3(9) of the Privacy Act with regard to the data requested. After this, the Authority called upon ITM and EMMI to investigate the whereabouts of the data of public interest requested to be accessed by the notifier and asked for information whether the requested data are processed by the two ministries mentioned, to which organ the data requested by the notifier were forwarded from EMMI and where the notifier can turn to in order to request the issue of the data. Furthermore, the Authority informed the ministries that the capacity of controller according to Section 3(9) of the Privacy Act can only be interpreted in the context of processing personal data; however, this case did not concern the accessibility of personal data. In its response, EMMI informed the Authority that the Office for Education (hereinafter: OH) has the responsibilities and powers with regard to the requested data. At the same time, OH invoked Constitutional Court Decision 13/2019. (IV. 8.) AB and stated that it was unable to produce the data requested by the notifier even with substantial human resources, hence it was not going to alter its position concerning the issue of the data. ITM informed the Authority that the requested data can be obtained from the higher education information system (hereinafter: FIR); OH was responsible for FIR's operation and they ensure the accessibility of data of public interest and data accessible on public interest grounds processed in FIR. Based on the above, the Authority established that the data of public interest requested to be accessed were processed by OH, the data were available electronically and could be obtained with simple IT operation. Based on the above, the Authority called upon OH to send the data of public interest processed in FIR and to be accessed to the notifier without delay. Upon the Authority's call, OH's president issued the data available in OH on 11 March 2022 to the notifier as requested. *(NAIH-7637/2021, NAIH-552/2022)*

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

The students of the Szeged University of Sciences notified the Authority that the Students Self-Governing Body (EHÖK) failed to respond to their data requests submitted four times in which they objected to the inaccessibility of spending by EHÖK and the student self-governing bodies of the faculties on EHÖK's website. The Authority established an infringement and called upon EHÖK to send the data of public interest requested to be accessed to the notifiers in the format required by them; the data request can also be fulfilled by publishing the data in EHÖK's website and sending the specific URL addresses to the notifiers. Finally, EHÖK's new president informed the Authority that they fulfilled the notifier's data request. Nevertheless, the Authority called the attention of EHÖK to the fact that as an organ performing public duties, EHÖK has to meet its electronic publication obligations as required by Chapter IV of the Privacy Act and to publish its data of public interest on its website according to the general publication scheme of Annex 1 to the Privacy Act. *(NAIH-3263/2022.)*

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

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

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

The Authority established that the purpose of conducting the authority procedure for the supervision of data classification initiated by the Budapest Municipal Court was in actual fact impossible as the conditions of conducting an authority procedure for the supervision of data classification did not exist with regard to the data according to

the subject matter of the litigation. Upon the call of the Authority, the controller was unable to show which of the information requested in the complaint was classified data. In this context, it only informed the Authority that the documents with which it could produce the requested data – the filing records kept according to Section 43(3) of Government Decree 90/2010. (III.26.) on the order of processing classified data (hereinafter: Government Decree) - carried repeated classifications. According to the position of the controller, the filing records can only be used to assist with the handling of documents, the data requested by the petitioner cannot be produced from them.

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

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

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

Pursuant to Section 62(4) of the Privacy Act, the classifier of the data shall be a party to authority procedures for the supervision of data classification. Therefore, as a preparatory question for the authority procedure for the supervision of data classification, the Authority also wished to clarify who classified the data according to the subject matter of the litigation before the Budapest Municipal Court and what was their classification marking. It was found that the classifiers, shown in the repeated classification marking of the filing records according to Section 7 of the Act on the Protection of Classified Data, classified data other than those constituting the subject matter of litigation, hence they could not become parties to the authority procedure for the supervision of data classification as persons classifying the data that constituted the subject matter of the litigation in progress before the Budapest Municipal Court. At the same time, the legal regulations in force do not enable the Authority to examine the lawfulness of the repeated classification at the controller applying the repeated classification marking under an authority procedure for the supervision of data classification, involving the controller or its representative in the procedure as a party because only the classifier may be a party to an authority procedure for the supervision of data classification.

The Authority continues to emphasize the following in relation to classification and fulfilling requests for data of public interest.

The Fundamental Law protects personal data, but in the case of data of public interest, it endeavours to guarantee access and dissemination, which is a precondition to participation in public affairs and public life. This was confirmed by the Constitutional Court when it declared that free access to information of public interest allows for the control of lawfulness and efficiency of the elected representative bodies, the executive power and public administration and encourages their democratic operation. Because of the complicated nature of public affairs, citizens' control and influence over decision-making by the public power and the administration of affairs can only be efficient, if the competent organs disclose the necessary information. [Constitutional Court Decision 32/1992. (V. 29.) AB]

The classification of data is the most severe restriction of the freedom of information. When in relation to some information reference is made to the fact that it is classified data, the following should be taken into account:

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

"With regard to the extent of the restriction, furthermore, attention must be paid to the fact that withholding information may not apply in general to the documents, hence constitutionally a regulation which withholds

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

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

14. Other cases commanding substantial public interest

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

15. International affairs

Council of Europe Convention on access to official documents (CETS No. 205., promulgated in Hungary by Act CXXXI of 2009) entered into force on 1 December 2020. However, the 10-member independent expert group mandated to monitor the implementation of the Convention (one of whose expert members is NAIH's President)

met for the first time in Strasbourg only on 18 November 2022, where they discussed primarily the rules concerning in the procedures of the expert group.

The 13th International Conference of Information Commissioners (ICIC) was held in Puebla (Mexico) in 2023 with the title "*Access to information, participation and inclusion in the digital age*". The most important message of the mutually accepted statement was the joint protection of the autonomy, independence and inviolability of the supervisory authorities.[8]

UNESCO also issued an important statement at the conference organised on the occasion of the International Day of Freedom of Information entitled "*Tashkent Declaration*", in which it calls upon all governmental and non-governmental actors to create and operate a legal, political and institutional environment that ensures the exercise of the right to the freedom of information in accordance with international standards.[9]

16. NAIH's freedom of information project

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

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

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

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

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

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

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

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

rejected every single question. The Guidelines for Municipalities issued is recommended expressly to this target group.

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

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

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