National Authority
for Data Protection
and Freedom of Information

ANNUAL REPORT OF THE HUNGARIAN NATIONAL AUTHORITY FOR DATA PROTECTION AND FREEDOM OF INFORMATION (NAIH) 2021

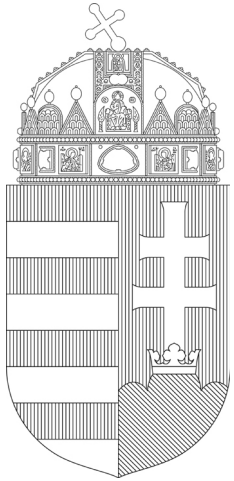
10 YEARS OF THE AUTHORITY

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

on its activities in 2021

B/18074

Nemzeti Adatvédelmi és Információszabadság Hatóság
(Hungarian National Authority for Data Protection and Freedom of Information)
Budapest, 2022.



Introduction

Greetings, Dear Reader

This year, we celebrate the 10th anniversary of the establishment of the National Authority for Data Protection and Freedom of Information, adding and underlining, that "NAIH identified itself as the heir to the Office of the Data Protection Commissioner and as the institution to continue its work, which functioned between 1995 and 2011".

We analyse the development and changes in its responsibilities and powers in detail in the coming chapter entitled "Review of the experiences of the first ten years of the Authority"; however, it can be clearly stated that the position of the Authority in the system of legal protection in the Hungarian constitutional state is stable and well accepted, and is adequately supported by its ever-strengthening organisation.

The Authority has a pioneering and inescapable role in the case of both informational rights in the field of the application and interpretation of the law, while its powers to supervise data classification are uniquely strong even in an international comparison. With regard to the latter, the investigation of the so-called Pegasus spyware case launched in 2021 should be mentioned, a detailed summary of which is accessible on the NAIH website.[1]

Naturally, there are areas where further development and progress would be needed. These include providing opinion on draft legislation and proposed legal regulations where we have been reporting difficulties for years; in cases of freedom of information, where it happens unfortunately that calls for compliant behaviour remain unsuccessful because of controllers showing inadequate willingness to cooperate. We are trying to find a solution also to this last problem within the framework of a comprehensive research project with outstanding EU support entitled "Mapping out the domestic practice of the freedom of information and enhancing its effectiveness in Hungary".

Budapest, 1 March 2022

Dr. Attila Péterfalvi

Honorary university professor
President of the
Nemzeti Adatvédelmi és Információszabadság Hatóság

1 https://www.naih.hu/adatvedelmi-jelentesek/file/486-jelentes-a-nemzeti-adatvedelmi-es-informacioszabadsag-hatosag-hivatalbol-inditott-vizsgalatanak-megallapitasai-a-pegasus-kemszoftver-magyarorszagon-torteno-alkalmazasaval-osszefuggesben

Overview of the Authority's first ten years of experience

1. Antecedents of NAIH's establishment, legal framework

The norms on which NAIH was founded – the Fundamental Law and the Information Act – date back to 2011, and the organisation started its operations on 1 January 2012. There was no legal succession in a legal sense, however, because of the responsibilities and the organisational and personal continuity NAIH identified itself as the heir to the Office of the Data Protection Commissioner and as the institution to continue its work, which functioned between 1995 and 2011. Thus, there was no real break, no new beginning in the history of the supervisory organisation of information rights, so the unbroken arc of organisational development can be well traced and analysed.

In 1995, a classical ombudsman's body began its operation, although the parliamentary commissioner supervising the protection of personal data and access to data of public interest had additional powers relative to other ombudsmen. In regulating the powers of the data protection commissioner, the legislator supported the procedures of the separate commissioner with expressly strong authority in a welcome but not self-evident manner, whose duties and powers extended to all the maladministration related to fundamental information rights (the only exception being the court procedures in progress) and it was authorised to examine all data processing in Hungary irrespective of whether it concerned the private or the public sector.

The amendment of the Data Protection Act in force since 1 January 2004 was an important step in determining the legal standing of the data protection commissioner: the commissioner was given official powers as an authority so he was able to order the blockage, erasure or destruction of unlawfully processed data, he was able to prohibit unlawful data processing and could suspend the transfer of personal data abroad. The controller could turn to the court against measures taken by the data protection commissioner. (This was very rarely the case.) Granting the powers of an authority clearly moved the position of the data protection commissioner away from the classical role of ombudsman. The Introduction to the data protection commissioner's 2010 report underlines that this year was one of "determined enforcement of rights: the first decision approved by the court, the first warning and the first reports" – at the same time, this could still be described as a kind of transitory period until 2011.

The reform of the ombudsman system (“there is one commissioner”) was concomitant with placing the legal standing of the data protection supervisory body onto a new basis as it would have clashed with the “independence criterion” of the Data Protection Directive of the EU in force at the time, if these powers were assigned to a “subordinate” ombudsman. In the light of Regulation, it proved to be a good decision to opt for the authority form in spite of the fact that there was serious political debate around the establishment of NAIH as a new authority both at Hungarian and European fora. The subject matter of one of the EU infringement procedures launched in January 2012 against Hungary was that by establishing NAIH, Hungary “had ended prematurely the six-year term of the former Hungarian Data Protection Commissioner, who was appointed in September 2008 and whose term of office would have ended in September 2014 only. The personal independence of a national data protection supervisor, which includes protection against removal from office during the term of office, is a key requirement of EU law. The re-organisation of a national data protection authority is not a reason for departing from this requirement,” argued the Luxembourg Court in its judgment in April.

This meant that the Authority had to demonstrate its independence and professionalism from a defensive position both in Hungary and abroad from the first minute of its existence. At the same time “ The confidence of citizens keeps being sound; this is clearly displayed by the amount of incoming complaints and other petitions received by NAIH (altogether 2929 in 2012) or the increased interest from DPOs. In 2012 numerous European and EU committees of inquiry (Schengen expert group, LIBE, Venice Commission) scrutinized our operation and law and the final conclusions were always positive (what’s more, the financial independence as well as the mighty authority powers of NAIH have been appreciated)”. – stated the Introduction to the first annual report of the Authority.

One of the positive outcomes of the transformation and the operation of the authority and its active international engagement was that it was not necessary to suddenly create a new administrative body at the time of the adoption of the new EU data protection regulation and in 2018 NAIH was able to begin discharging its GDPR duties already in possession of substantial experience as an authority. The new legal bases introduced by the Privacy Act, the data protection audit, the actively used fining powers and the cases of the data protection authority (where the joint interpretation of the Act on the General Rules of Administrative Procedures and Services and the Privacy Act by itself constituted a major challenge) enriched the Hungarian Data Protection Authority with experience several years prior to the entry into force of GDPR, which clearly eased the transition in

2018 (let us add: this was not in the least general or self-evident in certain other EU Member States).

2. Data protection – changes in organisation and regulation

In 2012, when the Authority came into being, complaints and cases relating to data protection law were dealt with by the Administrative Department and the Inquiry Department, and within this, the Division for Data Protection dealt with.

Pursuant to Section 60(1) of the Privacy Act in force at that time, the so-called authority procedure for data protection – whose background rules included the special provisions of the Privacy Act and the rules of the Act on Administrative Procedures and Services – could only be launched ex officio, i.e. based on the initiative of the Authority. Initially, a substantial part of the complaints related to data protection law was dealt with by the Data Protection Division in an inquiry procedure similar to that of an ombudsman, meaning that the result cannot be legally enforced; in addition, the Authority’s staff devoted significant resources to responding to so-called submissions for consultation, which in actual fact became instruments for the development of data protection law in essence.

In the initial period of the history of the Authority, dealing with administrative data protection cases was among the responsibilities of the Administrative Division belonging to the organisation of the Administrative Department originally set up with five data protection experts and a head of division. Over the years, as the number and proportion of submissions related to data protection law kept growing in relation to the total number of submissions received by the Authority, a separate Data Protection Department came into being to deal with both data protection investigations and administrative data protection cases; which is currently staffed by twenty data protection experts and four managers.

The burden of cases for the Data Protection Department increased substantially, particularly since the beginning of the application of GDPR, so in order to ease the workload, further differentiation of the organisation of the Authority became warranted and currently there are three departments that may conduct the Authority’s procedures in data protection cases according to an appropriate division of labour.

Over the years since the establishment of the Authority, the growing number of submissions related to data protection did not constitute the only challenge for the Data Protection Division and later for the Data Protection Department.

In the period preceding the application of GDPR and the setting up of the European Data Protection Board, the instrument of harmonising the legal environment for data protection in the Union was Directive 95/46/EC of the European Parliament and of the Council and common interpretation is worked out by the so-called data protection working party set up according to Article 29 of the Directive (hereinafter: Article 29 Working Party) consisting of the representatives of the supervisory authorities of the EU Member States.

The guidelines, recommendations and other documents issued by the Article 29 Working Party commanded increasing interest in the interpretation of the regulation by the Authority's organisational unit dealing with data protection cases, well before the adoption of GDPR.

Following the adoption of GDPR and particularly its entry into force and the beginning of its application, the interpretative role of the Article 29 Working Party and then the European Data Protection Board replacing it became increasingly decisive because the goal to be achieved through GDPR, namely a uniform level of legal protection in data protection cases guaranteed for individuals, could only be achieved in this way.

Looking back on the past ten years, it can be said that in the Authority's everyday work of interpreting and applying the law, it has to pay attention not only to the legal norms on data protection in force in the territory of Hungary – whether general or sectoral, the practice of the Hungarian courts and outstanding judgements of the EU court in a given case, but the decisions of the supervisory authorities and courts of other EU Member States, and of course the principled declarations of the European Data Protection Board may also be relevant. An international, but at least European outlook has essentially become indispensable also in the course of the everyday work of applying the law.

From the viewpoint of procedural law, there was a substantial change in dealing with data protection cases, namely with a view to compliance with Article 77 of GDPR based on the text of Section 60(1) of the Privacy Act in force since 26 July 2018, in that the authority procedure for data protection may also be launched on the basis of the data subject's request. In addition, naturally, the ex officio authority procedure for data protection also remains in place and as before, anyone, i.e. not only the data subject, but any other person, may initiate a data protection inquiry according to Subtitle 30 of the Privacy Act, which may also be launched ex officio.

In the context of the changes in substantive law and procedural law referred to above, it can be stated that the Authority's work in applying the law improved continuously, the conduct of the Authority's procedures became increasingly precise thanks to the experiences accumulated case after case and knowledge of procedural law and litigation experience became increasingly rich.

While GDPR Article 70(1) also specifies a number of special issues (such as administrative fines, decision-making based on profiling, etc.), GDPR Article 70(1)(e) grants general authority to the European Data Protection Board to issue guidelines, recommendations and best practices upon its own initiative or at the request of any one of its members or even the Commission of the European Union with a view to the uniform application of GDPR.

In its communiqué of 3 November 2018, the Authority itself made it clear that as far as the future is concerned, the guidelines of the European Data Protection Board will be regarded as the engine of development of EU data protection law; in the period preceding the application of GDPR, i.e. prior to 25 May 2018, the Hungarian Authority has issued a number of recommendations and opinions to help ensure compliance with the provisions of data protection law, in the development of which the staff of the Data Protection Department and its legal predecessor organisational units had a highly important role to play. Of these, the following recommendations are to be underlined:

- on the fundamental requirements of electronic surveillance system at the workplace (23 January 2013),
- on the data protection requirements of claim management techniques applied in the course of claim management, debt collection and factoring activities (3 July 2014),
- on the data protection requirements of preliminary information (29 September 2015), on the fate of on-line data after death (11 November 2015),
- on bearing the costs arising in issuing health documentation (30 December 2015),
- on making sound recordings, their accessibility and the right for issuing copies (4 August 2016),
- on the fundamental requirements of data processing at the workplace (28 October 2016).

Of course, in line with the guidelines issued by the European Data Protection Board, the Authority published recommendations also after GDPR became applicable and it is ready to issue recommendations in the future concerning issues, which are warranted because of the experiences of applying the regulation, the significance of a case or other signals received; thus, for instance, a recommendation was drafted recently concerning data processing related to the corona-virus epidemic, as well as certain data protection requirements related to data processing by political parties and organisations.

3. Data protection audit

The introduction of the institution of data protection audits was one of the most exciting data protection innovations of the past 10 years. It is of outstanding importance in achieving genuine data protection awareness that the legislator and the supervisory authority improved the level of awareness not only of data subjects, but also of controllers. This is achievable via campaigns, guidelines and recommendations but the data protection authority may have an even more proactive role and it can assist controllers directly.

Naturally, this cannot clash with its executive role, hence in order that the supervisory authority be able to take on such a strongly proactive role an institutional framework enacted by the legislator is needed. This was earlier provided by the Hungarian legislator by introducing the institution of data protection audit.

Pursuant to the provisions of the Privacy Act applicable between 2013 and 2018, the National Authority for Data Protection and Freedom of Information (NAIH) could conduct a data protection audit upon request of the controller with a view to ensuring high-level data protection and data security through the assessment of the data protection operations carried out or planned according to professional criteria specified and published by the Authority.

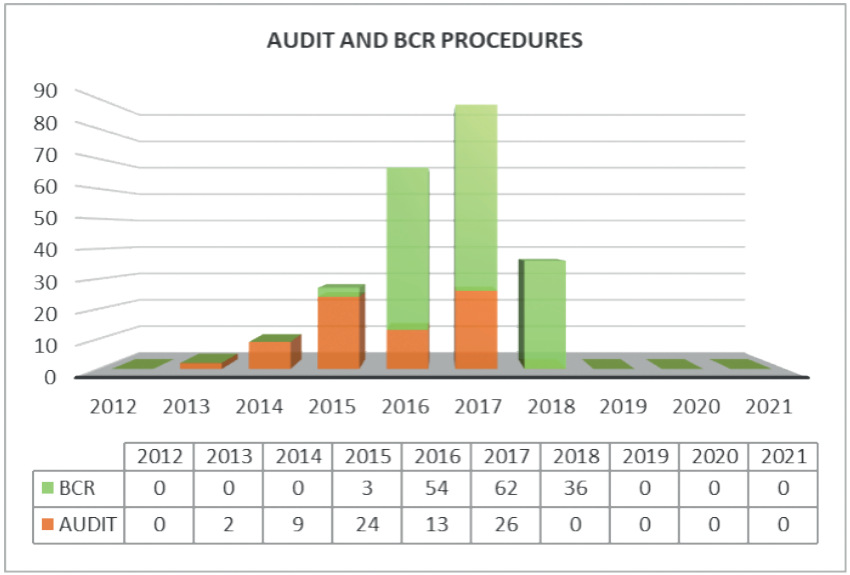
Essentially, the audit is a study of a system, an activity, a procedure or process and its goal was to examine to what extent the given system or procedure complies with the audit criteria specified prior to the audit. An audit is a general instrument of supervision, on the basis of which independent third actors assess the procedures of the audited organisation.

In the course of a data protection audit, the Authority assessed the extent to which the data protection knowledge of the controller was up-to-date and the extent to which legal provisions were reflected in its internal rules. It examined whether there were any regulatory deficiencies in the controller's data processing, whether there were any data protection risks and what steps should be taken to implement data processing in compliance with the legal regulations and made recommendations as to the way in which internal rules should be adjusted to the activities carried out by the organisation.

Data protection audits had benefits for all the stakeholders in data processing. Data subjects could meet data processing fully in compliance with data protection requirements. Controllers could learn a general methodology, which could assist them in evaluating their processing operations. And the Authority could learn the problem issues, with which all controllers struggle.

The general conclusion of data protection audits was that controllers failed to draft their Privacy Statements, their interest assessment tests and their contracts aimed at data processing in sufficient detail. Accordingly, the Authority endeavoured to issue more detailed guidelines in these areas. GDPR also confirmed the experiences of the data protection audits because the legislator adopted more detailed rules precisely in these areas.

After 2018, data protection audit procedures can no longer be conducted because after GDPR becoming applicable, the regulatory possibility for providing the data protection audit service ceased for the Authority. It should be indicated at the same time that a highly successful instrument was deleted from the Hungarian data protection regulation, which was a forerunner, inter alia, of the principle of accountability and the higher level data protection awareness appearing in GDPR.



	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
BCR	0	0	0	3	54	62	36	0	0	0
AUDIT	0	2	9	24	13	26	0	0	0	0

The Authority continuously monitored the evolving new EU regulations in the course of European cooperation, and it was one of its priority objectives to make all legal institutions known to the controllers upon the adoption of the common EU rules. As a result of this attitude, the Authority always urged the legislator to transpose the legal institutions of data protection (such as data breaches, binding corporate rules) still missing from Hungarian data protection law, but well established in European practice into the Hungarian regulation when amending the Privacy Act.

Even after the entry into force of GDPR, the Authority worked on easing the transition to the new data protection regime for controllers. Accordingly, the Authority, in cooperation with the other EU supervisory authorities, developed a form for reporting data breaches, which included all the mandatory data required by legal regulation and arranged these data into a fully transparent system. The Authority welcomed the development of the common form and actively participated in this work in order to allow controllers to know as soon as possible which data should be collected in the event of an eventual data breach in order to assist them in the proper development of their internal procedures and risk assessment mechanisms.

4. Supervision of data classification, procedures related to classified data

The strongest powers of the Authority as an authority (outstanding also in an international comparison) is related to classified data whose regulation was unaffected by GDPR. In retrospect, the amendment of the Privacy Act adopted and entered into force in 2015 can be regarded as a substantial milestone, which altered the regulatory environment of the Authority's procedures related to classified data, the authority procedure for the supervision of data classification, as well as the Authority's powers to have access to classified data.

The antecedent of this amendment was Constitutional Court Decision 4/2015. (II.13.) AB, which declared that based on the right to have access to data of public interest and data accessible on the grounds of public interest, substantive control must be ensured over classification which could be initiated directly, and is capable of examining the grounds for classification in terms of content, as well as the necessity and proportionality of the restriction of access. This means that under the Privacy Act, if the controller refuses to comply with a request to access data of public interest because of the data being classified and the person requesting the data may turn to the court to review the refusal, the court is under an obligation to initiate the authority procedure for the supervision of data classification and to suspend the litigation until the Authority brings its decision. As the authority procedure for the supervision of data classification may only be initiated ex officio, it is important that the Authority has the opportunity to launch an inquiry both on request and ex officio, which provides an effective legal tool to clarify the facts in sufficient detail and often leads to the launching ex officio of an authority procedure for the supervision of data classification.

5. Freedom of information over the first ten years of the Authority's operation

The changes in the legal environment fundamentally determined the situation of freedom of information over the past ten years as no relevant changes took place in the practice of the Authority with regard to the subject matter of the cases or the proportion of the Authority's cases (data protection vs. freedom of information, which has been stable at around 10% since 1995) over the past decade. Case numbers are, however, increasing continuously at a steady space: in 2012, we dealt with over 3,000 cases, which rose to over 1,200 in 2021, i.e. the number of cases quadrupled.

Those requesting data in 2012 were just as much interested in the operation and financial management of companies held by the state, issues of travel by state delegations and the content of the statement of assets of leaders of state and local government as in 2021. Naturally, transparency related to the corona-virus pandemic is a new subject, in relation to which the Authority made statements on several occasions, calling the attention of both the public and the decision-makers to the necessity of quick access to accurate and topical information in the public interest.

In addition, it is a growing tendency that public communications are conducted more and more through online community platforms, which the majority of society uses increasingly actively both for obtaining and for disseminating information. Apart from this, however, the subject matter of the complaints and requests for consultation did not change fundamentally over the past ten years.

6. Relevant changes in the legal environment:

Hungary's Fundamental Law entered into force on 1 January 2012, which included several provisions in addition to stipulating a basic constitutional right to access and disseminate data of public interest and designated NAIH as the supervisory body for the freedom of information linked to this right, but which had not been settled at the level of the Constitution earlier, including the following:

- pursuant to Article 38(1), the property of the state and of local governments shall be national assets; he property of the State and of local governments shall be national assets;

- according to Article 39, support or contractual payments from the central budget may only be granted to organisations of which the ownership structure, the organisation and the activity aimed at the use of the support is transparent.

Every organisation managing public funds shall be obliged to publicly account for its management of public funds. Public funds and national assets shall be managed according to the principles of transparency and the purity of public life. Data relating to public funds and national assets shall be data of public interest.;

- based on Article U(4), the holders of power under the communist dictatorship shall be obliged to allow statements of fact about their roles and acts related to the operation of the dictatorship, with the exception of deliberate statements that are untrue in essence; their personal data related to such roles and acts may be disclosed to the public.

The legislator integrated the rules of former sectoral laws related to the freedom of information into the Privacy Act and annulled the so-called "Glass pocket law", as well as the Act on Electronic Freedom of Information. The provisions concerning the rules of trade secrets related to data of public interest were no longer included in the new Civil Code, it only defined the notion of trade secret. The relevant amendment to the Privacy Act entered into force on 15 March 2014, simultaneously with the entry into force of the new Civil Code, and Act LIV of 2018 on Trade Secrets enacted to implement Directive 2016/943/EU of the European Parliament and of the Council did not amend this regulation.

In 2016, based on the legislative authorisation set forth in the Privacy Act, the Government enacted a decree on the extent of cost reimbursement that may be stipulated for meeting a demand for data of public interest, which entered into force on 15 October 2016. The Cost Decree, adjusted to the rules of the law, specify which costs incurred while requesting data of public interest can be charged to the person making the request and to what extent. Prior to this regulation, the cost elements that could be taken into account were developed by NAIH's practice, and the Government essentially codified this in its decree.[1]

In the context of the state of emergency caused by the COVID pandemic, the rules pertaining to the satisfaction of requests for data of public interest were modified temporarily. At the time of closing this report, the rules of Government Decree 521/2020. (XI. 25.) based on Act LVIII of 2020 may apply to individual requests for data of public interest (the Constitutional Court rejected the motion aimed at the establishment of the anti-constitutionality of this legal regulation and declaring it null and void, but at the same time, set forth a constitutional requirement in relation to its application[2]). Based on this regulation, if it is probable that meeting the request within 15 days would jeopardise the discharge of the public duties related to the state of emergency by an organ discharging public duties – a condition which the controller is under an obligation to prove – the due date for meeting the data request may be increased to 45 days subject to detailed justification (this due date may be extended once by a further 45 days based on the decree), of which the person requesting the data must be notified within 15 days from the receipt of the request.

1 See in detail: NAIH Report 2017, Chapter VII.2.

2 See Constitutional Court Decision 15/2021. (V. 13.) AB

On 1 December 2020, the Tromsø Convention (Council of Europe Convention on access to official documents) entered into force, promulgated in Hungary by Act CXXXI of 2009.

The ninth amendment to the Fundamental Law, which came into force on 23 December 2020, also included amendments relating to freedom of information. A paragraph (3) has been added to Article 39 of the Fundamental Law, which stipulates that public funds shall be the revenues, expenditures and claims of the State. Article 38 was supplement with paragraph (6) stipulating that the establishment, operation and termination of, and the performance of public duty by, a public interest asset management foundation performing public duty shall be regulated in a cardinal Act (the Authority issued a Communication[3] on the obligations of the model changing universities related to the freedom of information).

Some important changes were also introduced to the text of the Privacy Act over the first ten years of the Authority's operation.

Based on the amendment to the Privacy Act, adopted by Act XCI of 2013, personal data accessible on public interest grounds may be disseminated in compliance with the principle of purpose limitation, and the publication of such data on a website is governed by Annex 1 to the Privacy Act and the provisions of a separate Act on the legal status of persons performing public functions [Section 26 (2) of the Privacy Act].

The same act integrated the rules earlier found in the Civil Code into the Privacy Act with the following content: *„A natural person, legal person or organisation having no legal personality that establishes a financial or business relationship with a person belonging to one of the sub-systems of the public finances shall, upon request, provide information to anyone with respect to data that is public on public interest grounds based on paragraph (3) and that is in connection with such a relationship. The obligation to provide information can be fulfilled by disclosing the data accessible on public interest grounds, or by indicating the public source that contains the data disclosed earlier in an electronic form. If the party obliged to provide information on the basis of paragraph (3a) refuses to provide the information, the party requesting information may initiate the procedure of the organ authorised to exercise legal supervision over the party obliged to provide information."* [Privacy Act Section 27 paragraphs (3a) and (3b)]

3 https://www.naih.hu/dontesek-informacioszabadsag-tajekoztatok-kozlemenyek/file/481-tajekoztato-a-modellvalto-egyetemek-kozerdeku-adatokkal-kapcsolatos-kotelezettsegei-targyaban

Act CXXIX of 2015, on the one hand, made certain legal institutions of the GDPR (mandatory organisational regulation, data breach), which were still in the process of being negotiated, part of Hungarian law, and on the other hand, substantially amended the provisions concerning freedom of information.

Through these amendments, the Privacy Act made it clear that with regard to access to data of public interest specific rules are applicable to the organs or persons who provide services that are to be made use of on a mandatory basis, which cannot be provided in any other way, based on legal regulation or a contract concluded with a state or local government organ [Section 26(4)].

In addition, it also amended the provisions concerning data laying down the foundation for a decision, introducing the criterion of "additional future decisions" as a criterion laying down the foundation for rejecting the data request. Earlier, a data request could be dismissed only if access to the data would jeopardise the lawful functioning of the organ performing public duties or would jeopardise the performance of its duties without undue external influence [Privacy Act Section 27(6)]. In addition to all this, the amendment package adopted with Act CXXIX of 2015 brought about additional changes with respect to the order of requesting data of public interest, which based on the justification by the legislator *"in addition to reinforcing the guarantees of the protection of fundamental rights appropriately takes into account the interests of controllers."*

The Curia's group analysing case law examined the relevant court practice in cases concerning the release of data of public interest for the period up to December 2018 and published its findings in the form of a summary opinion. The objective was a general review of the judicial practice of litigations launched to release data of public interest, the exploration of differences in interpretation and case law and the related legal uncertainties, taking a stand with regard to the appropriate practice and interpretation and the need for the Curia to create a case law unifying instrument.

Finally, the Authority's comprehensive freedom of information project was launched in 2019 which, following the mapping out of the past and current position, targeted the solution of eventual deficiencies or problems through recommendations, information materials and other deliverables (such as recommendation to amend the law, thematic website, developed self-audit mechanism,

etc.) involving all the stakeholders (NGOs, members of the press, citizens, actors of local governments and central government, judges, etc.). The addressees of the recommendations included both decision makers and those applying the law, which meant that even if the current legal environment is unchanged, there is a well-grounded hope that the efficiency of the freedom of information in Hungary can be improved through the introduction of good practices, attitude building, making people aware of their rights and appropriate communication.

7. International aspects

At the international scene, the Authority has become an increasingly well-known actor: we continuously and actively participated in the work of Data Protection Working Party 29 of the European Union and its subgroups; first in 2012 and then in 2018, we organised a data protection and (for the first time in the world) freedom of information Case Handling Workshop, and in 2015 an international conference on drones (whose recommendations constitute one of the points of departure of the EU drone regulation that has matured by now); in 2016, we again organised the European data protection conference, while in 2018 we arranged for the session of the Berlin Working Group (an entity of long history based on the principle of voluntary organisation) in Budapest.

Since its creation, the Authority has consciously built and strengthened its international relations and has played its part in organising international events.

Over the past years, we participated in successful international and EU projects as collaborators or project managers in the support of co-authorities (Macedonia), protection of children's rights (Arcades), support for GDPR training (STAR) and making the SME sector aware of GDPR (STARII). The title of our children's rights project "*Kulcs a net világához!*" (Key to the World of the Net) was popular and produced its own results; there is a great deal of interest for its publications translated also into English to this very day.

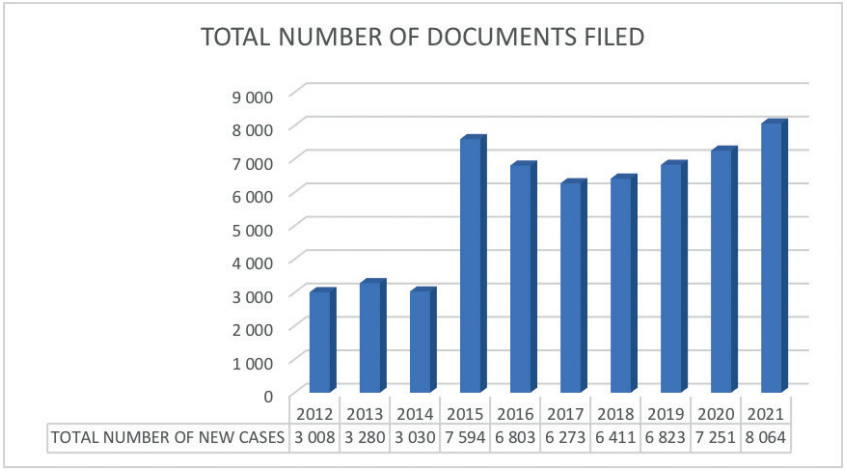
When the Authority was established in 2012, the type of cooperation implemented today within the framework of GDPR had still been unimaginable. GDPR has given national authorities tasks and powers, some of which are exercised. Today, the one-stop shop administration of cases, mutual assistance and other cooperative procedures occur regularly and in large numbers in the activities of the Authority providing a substantial part of the case statistics. Within the Authority, the Cabinet of the Vice President acts as liaison towards the other supervisory authorities. It seemed expedient to designate a separate organisational unit for this task.

The Authority has been actively involved in the activities of the European Data Protection Board from the very beginning. EU level cooperation is expected to bring about enhanced harmonisation and growing efficiency. In the coming years, the enforcement of GDPR will be the most important measure of the extent to which the intention of the legislator is manifested in everyday practice. GDPR influences international practice not only in the European Economic Area, but also beyond; let it suffice to refer to the compliance resolutions with respect to the United Kingdom, Japan and South Korea adopted in recent years. We trust that by the end of the next decade, we will be able to look back at the period that is still ahead of us, seeing that voluntary compliance has improved, enforcement has become stronger and GDPR has contributed to an improvement in the protection of privacy both in the European and the global scene.

8. The Authority's first ten years in numbers and a summary of he changes related to the operation of the Authority

For a longer-term review of the operation of an administrative agency and making it measurable, it is indispensable to examine the number of cases handled, the outputs created and their assessment both at home and internationally.

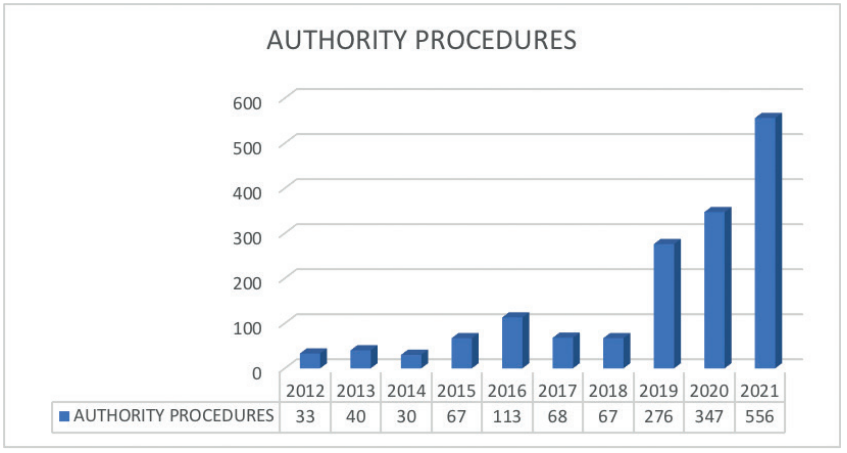
The number of the case files generated can provide a good point of departure for additional analysis and for a review of the tendencies of the past ten years.



	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
TOTAL NUMBER OF NEW CASES	3 008	3 280	3 030	7 594	6 803	6 273	6 411	6 823	7 251	8 064

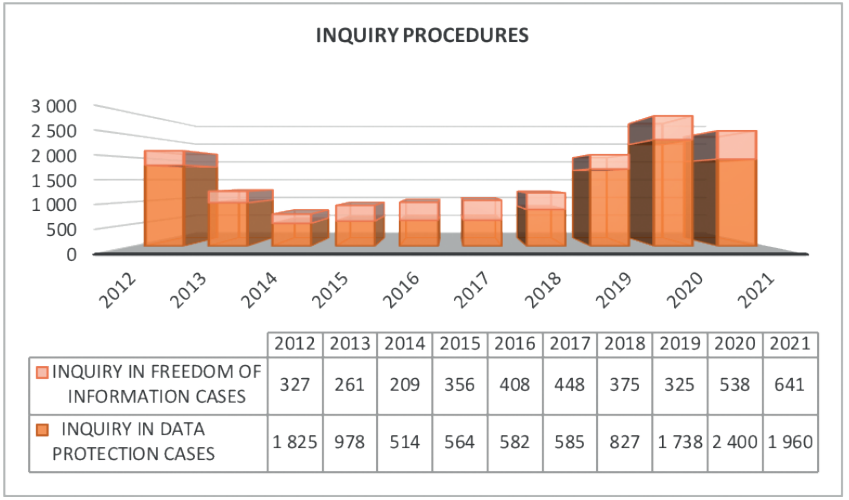
Reviewing the past ten years in the operation of the Authority by the measure of “case files”, it can be established that the overall number of substantive case files within its jurisdiction has been increasing steadily.

The most striking increase is noted in the number of cases conducted according to the authority-type procedural rules (Administrative Authority Procedures Act and General Administrative Procedures Act).

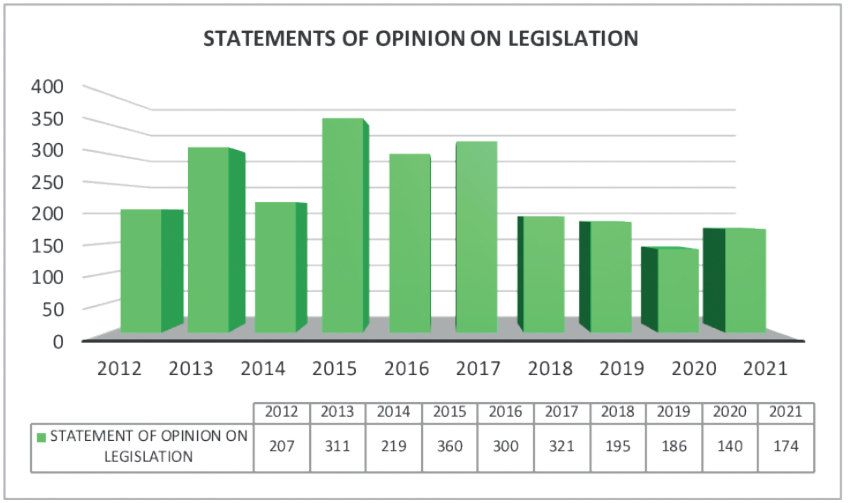


	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
AUTHORITY PROCEDURES	33	40	30	67	113	68	67	276	347	556

Through the increase in the number of authority procedures, the reduction in the number of inquiry procedures can be well traced in 2021:



	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
INQUIRY IN FREEDOM OF INFORMATION CASES	327	261	209	356	408	448	375	325	538	641
INQUIRY IN DATA PROTECTION CASES	1 825	978	514	564	582	585	827	1 738	2 400	1 960

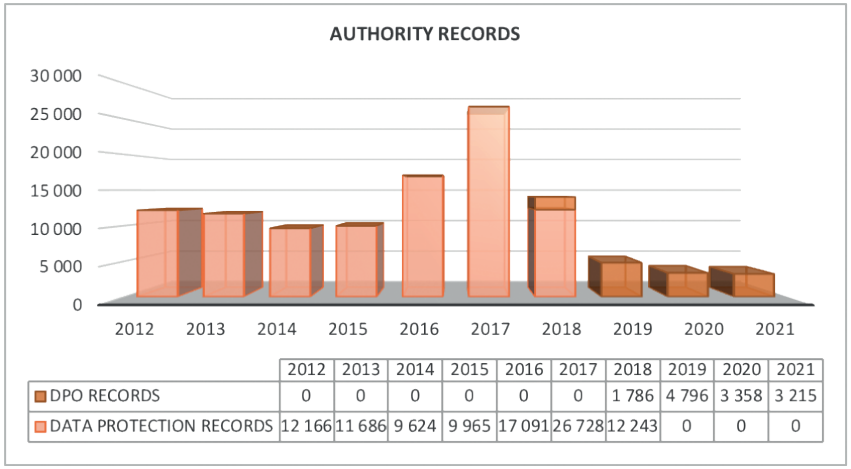


	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
STATEMENT OF OPINION ON LEGISLATION	207	311	219	360	300	321	195	186	140	174

The records of the Authority

The Privacy Act placed the data protection records on new foundations. The application of the provisions of both the Privacy Act and the Code of Administrative Procedures stipulated requirements essentially different from the earlier ones for the Authority. The renewed requirements for data protection records from 2012 entered into force on the day of the establishment of the Authority, so there was no transitory period which would have provided an opportunity to prepare for the application of the new rules. Relying on its own internal development capacity, the Authority began the implementation of the IT system for the data protection records as a priority task. In the course of the development, particular attention was paid to enabling electronic completion and log-in and to reducing the administrative burden on both controllers and the Authority. The number of cases generated in the records amounted to many thousands over the past years, hence the Authority kept them separate from the inquiry and Authority procedure type cases. The incoming log-ins and modification requests have been processed in separate filing books in the electronic processing systems. These were also presented separately in statistics.

As a result of the mandatory application of GDPR, the data protection records ceased to exist; at the same time, the Authority set up the records of the data protection officers, relying on its own development resources. The following figure shows the data processed in the two registries over the past ten years:



	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
DPO RECORDS	0	0	0	0	0	0	1 786	4 796	3 358	3 215
DATA PROTECTION RECORDS	12 166	11 686	9 624	9 965	17 091	26 728	12 243	0	0	0

The Authority had to combat a number of difficulties upon its establishment in 2012. The number of cases in progress taken over from the Office of the Data Protection Commissioner was substantial and the IT infrastructure taken over was unable to ensure efficient work for the Authority. The Authority did not have the financial resources or budgetary funding for the full-scale roll-out of the IT system and the implementation of the complex infrastructure and information systems and a web portal, indispensable for sustainable, modern operation. The funding for the development and maintenance of the new infrastructure was omitted from the planning of the 2012 budget, which had to be modified in order to ensure the functionality of the Authority.

The refurbishment of the central office in Szilágyi Erzsébet fasor designated in 2012 ended in 2016. With the increase in tasks, the number of staff also increased from the initial 59 to above 100 persons, thus the constricted space in the central office became a substantial impediment to everyday work. The possibility of changing the central office was outlined in 2019 and it was implemented at the end of 2020. The move to Falk Miksa utca provided the right working environment for the Authority to operate for the long term.

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

I.1. Statistical characteristics of our cases

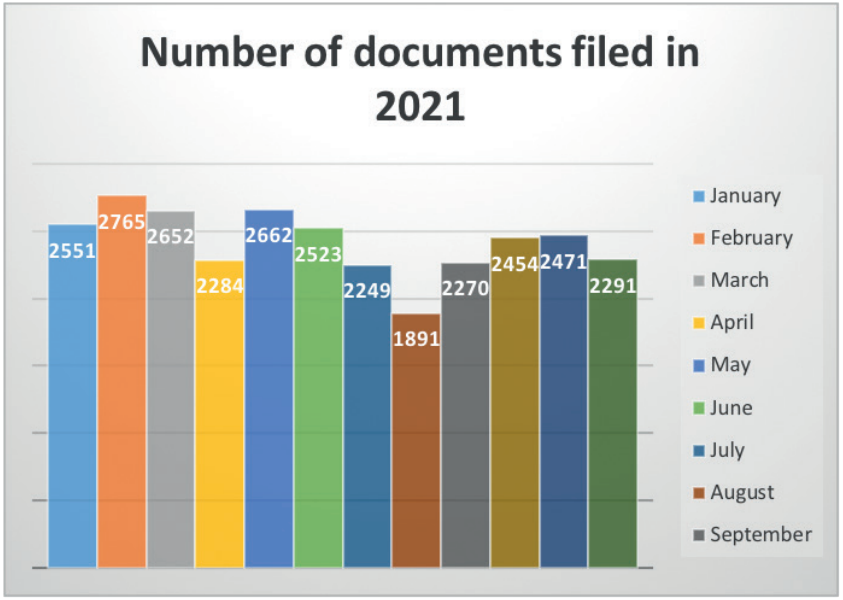
In accordance with the objectives of the National Digitalisation Strategy (2021-2030), the Authority supported the implementation of organised, consistent and transparent institutional operation expected (also) from the autonomous organs of public administration with the least possible extra administrative surplus at the level of an administrative authority. The Authority successfully implemented machine access to its office storage space and the e-mail module integrated into its administrative system. The next step was the migration of the assignment of cases by the heads of the separate organisational units to an electronic interface and the testing of the administration module of the Integrated Legislative System (IJR) was also implemented.

The reduction of the administrative burden is a complex task, which means, on the one hand, the possibility to start and process cases online in a client-friendly and fast manner at the front-office level and, on the other hand, electronic communication through the use of regulated electronic administrative services. At the back-office level, it requires the streamlining and digitalisation of file management and administrative processes, as well as a reduction in the lead times of processes.

The priority strategic objective of the Authority remains the implementation of e-administration in as wide a circle as possible through the implementation of e-administrative services and the development of the related internal case management system (IRMA).

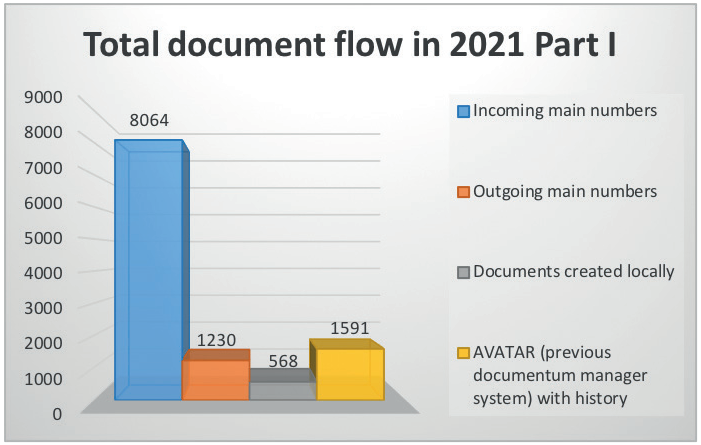
NAIH's case management area is able to support the efficient operation of the Authority through the use of an organisation development tool aimed at the improvement of activities, such as the process management activity. The goal is that organisational units carry out as few redundant operations as possible.

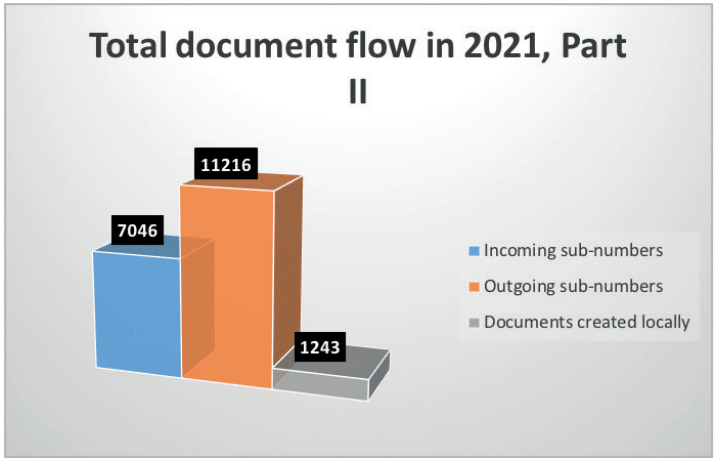
Over and above, the Authority forecasts further increases in case management tasks as a result of the expansion of the tasks of the various professional areas and the rise in case numbers showing a growing tendency year after year.

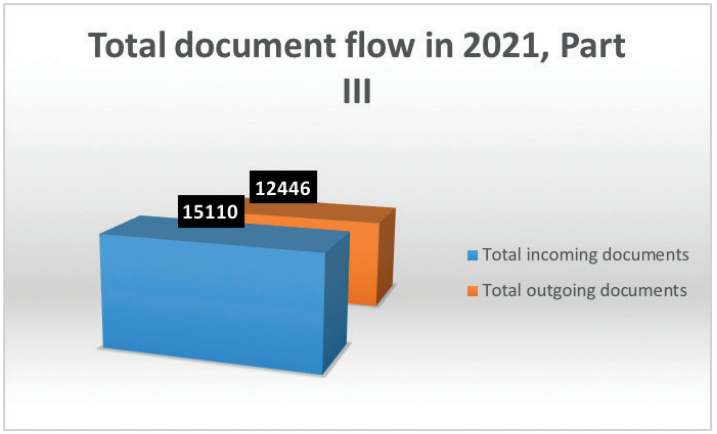


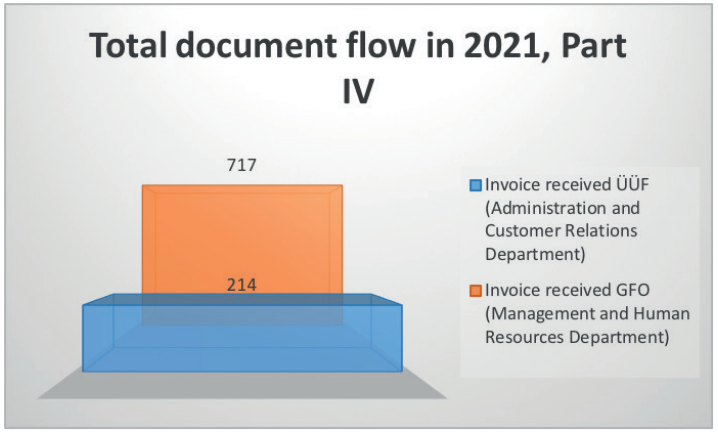
The reorganisation of the technical tasks in client relations was associated with the execution of multi-faceted tasks, thereby making it possible to provide broad-spectrum information on questions not related to, or not requiring, individual case-specific investigations, procedural acts of the Authority and other specific tasks carried out by the Authority.

A Hatóság 2021. évi iratforgalmi statisztikája









In 2021, 8,271 new cases were filed and 7,440 cases were preallocated in the Authority's electronic file management system. Together with cases carried forward from earlier years (1,591), altogether 9,872 cases were in progress before the Authority.

The tendency observed in the preceding year, according to which the number of submissions for consultation continued to decline (from 1,710 to 1,464), while the volume of inquiry procedures showed a substantial increase exceeding the preceding year's numbers by more than 500 cases (3,456) in the period under study.

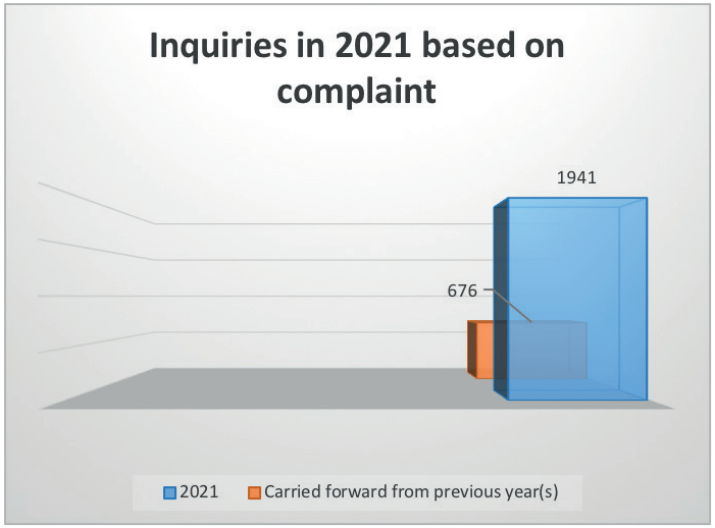
Major case types of the Authority in 2021

Authority cases	556
Inquiry cases	3456
Consultation cases	1464
Authority audits	630
Statements of opinion on legislation	174
GDPR cooperation (IMI)	1062

Inquiry procedures in 2021 – Data protection

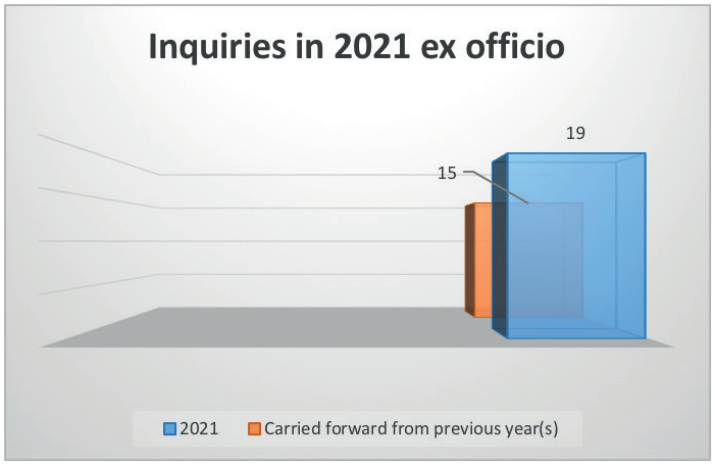
Inquiry cases based on complaints in 2021

2021	1941
Carried forward from previous year(s)	676



Inquiry cases ex officio in 2021

2021	19
Carried forward from previous year(s)	15



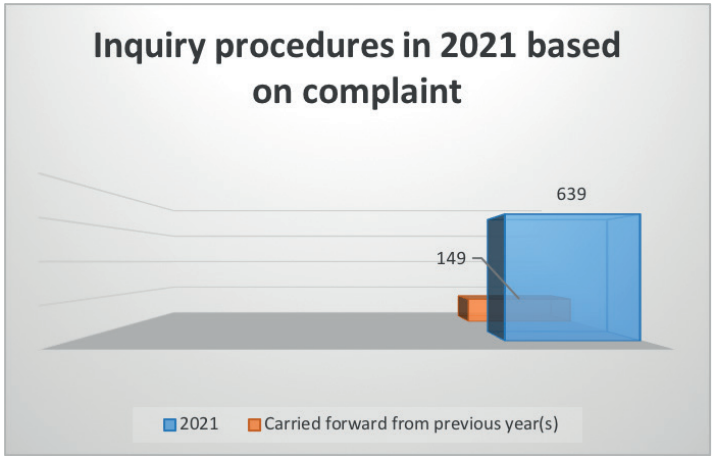
Data protection inquiry procedures in 2021 per case type

Case type	Total	Carried forward from previous years	New cases
Inquiry procedure ex officio	**34**	**15**	**19**
Inquiry procedure ex officio in data protection cases – Law Enforcement Directive	8	3	5
Inquiry procedure ex officio in data protection cases – GDPR and other	24	11	13
Inquiry procedure ex officio in data protection cases – GDPR és other – data breach	2	1	1
Inquiry procedure based on complaint	**2617**	**676**	**1941**
Inquiry procedure based on complaint in data protection cases – data breach	207	50	157
Inquiry procedure based on complaint in data protection cases – Law enforcement data breach	6	1	5
Inquiry procedure based on complaint in data protection cases – Law Enforcement Directive	76	27	49
Inquiry procedure based on complaint in data protection cases - GDPR and other	2328	598	1730

Inquiry procedures in 2021 – Freedom of information

Inquiry cases based on complaint in 2021

2021	639
Carried forward from previous year(s)	149



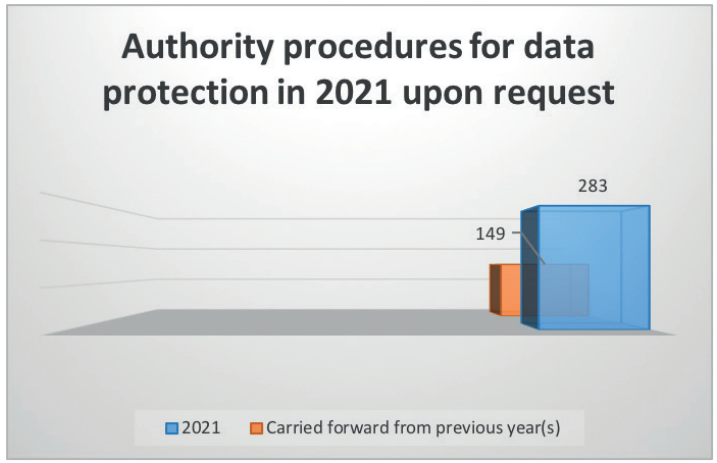
Inquiry cases ex officio in 2021

2021	2
Carried forward from previous year(s)	15

Number of Authority procedures in data protection cases in 2021

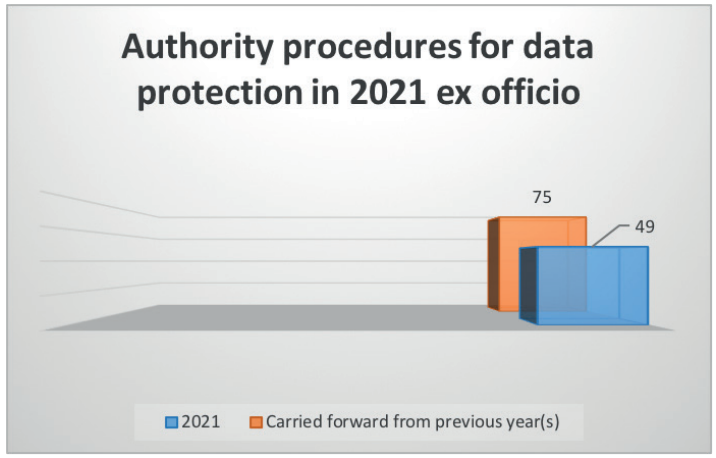
Authority data protection procedures in 2021 upon request

2021	283
Carried forward from previous year(s)	149



Authority data protection procedures in 2021 ex officio

2021	49
Carried forward from previous year(s)	75



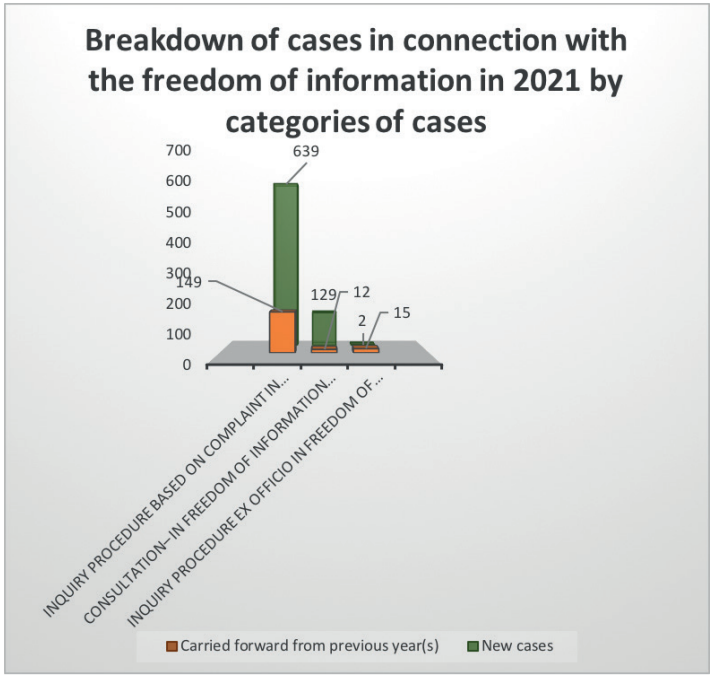
Authority procedures in 2021 by case type

Case type	Total	Carried forward from previous years	New cases
Authority data protection procedure ex officio	**111**	**62**	**49**
Authority data protection procedure ex officio – Law Enforcement Directive	6	1	5
Authority data protection procedure ex officio - Law Enforcement Directive – data breach	2	0	2
Authority data protection procedure ex officio – GDPR and other	79	47	32
Adatvédelmi hatósági eljárás hivatalból - GDPR és egyéb - adatvédelmi incidens	23	14	9
Authority data protection procedure ex officio – GDPR and other – freedom of the press and the expression of opinion	1	0	1
Authority data protection procedure upon request	**432**	**149**	**283**
Authority data protection procedure upon request – Law Enforcement Directive	11	2	9
Authority data protection procedure upon request – Law Enforcement Directive – data breach	2	2	0
Authority data protection procedure upon request – GDPR and other	396	140	256
Authority data protection procedure upon request – GDPR and other – data breach	22	5	17
Authority data protection procedure upon request – GDPR and other – freedom of the press and the expression of opinion	1	0	1

The Authority brought 92 decisive decisions in its procedures referred to. It levied data protection fines in 36 cases to a total amount of HUF 68,100,000 and procedural fines totalling HUF 4,490,000 in 27 cases. In addition, the Authority requested the review procedure of the Curia as extraordinary remedy in 4 cases, it initiated a complaint procedure for the uniform application of the law against the judgement of the Curia and lodged a constitutional complaint with the Constitutional Court on one occasion.

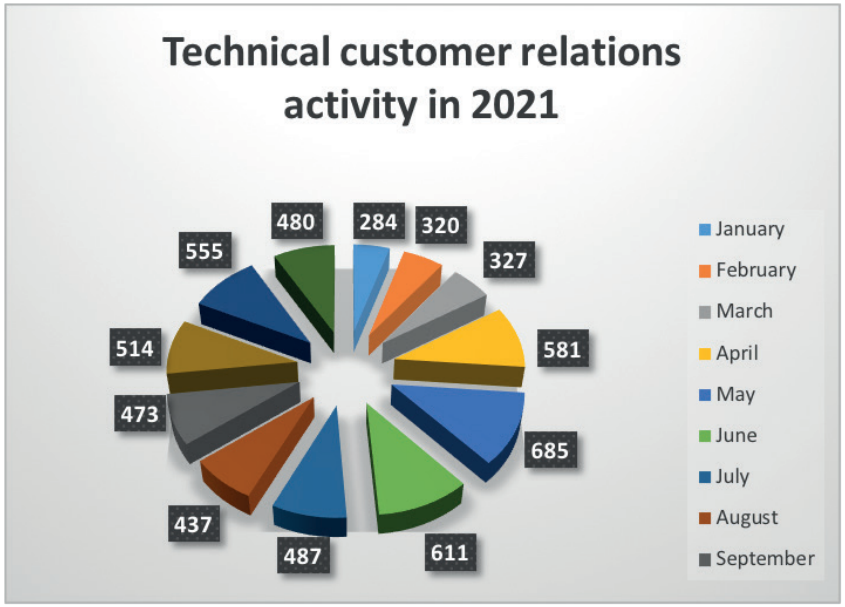
Breakdown of freedom of information cases in 2021 by case type

Case type	Total	Carried forward from previous years	New cases
Inquiry procedure based on complaint concerning freedom of information	788	149	639
Consultation – concerning freedom of information	141	12	129
Inquiry procedure ex officio concerning freedom of information	17	15	2

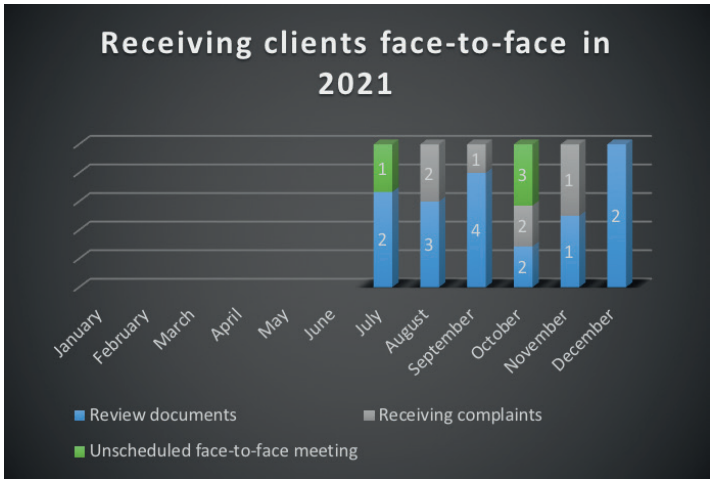


In 2021, the Authority's Customer Service received 5,704 calls, which relative to the preceding year represents a highly substantial rise of over 90 percent (!), primarily due to the fact that as of April 2021 the Authority's Customer Service was available to clients on every workday of the week as a result of the rapid reorganisation demanded by the emergency caused by the corona-virus pandemic.

Beyond the questions regarded as traditional, those requesting support from the Customer Service asked for assistance primarily in relation to the documents intended to be submitted on e-paper, or the selection of a channel of communications related to their cases in progress and most appropriate for their needs. In addition, our colleagues provided information on the exercise of data subjects' rights and called the attention of data subjects to the forms accessible in the Authority's website to facilitate the enforcement of rights, answered questions arising in relation to the Authority's procedures and called their attention to the possibility of making use of the direct assistance provided by data protection officers mandatorily or optionally appointed by controllers with a view to exercise their rights more efficiently.



The Authority's face-to-face Customer Service activities were suspended during the period of the epidemiological emergency of the past year, bearing in mind its substantial risks, from 1 January 2021 to 1 July 2021. Subsequently, complaints were lodged in person and the right to review documents and/or make statements related to the procedures by the Authority subject to the Administrative Procedures Act was exercised on 23 occasions.



Administrative audits in 2021

Administrative audits in 2021	562
Carried forward from previous year(s)	68

Case type	Total	Carried forward from previous year	New cases
Data protection administrative audit – Law Enforcement Directive	1	1	0
Data protection administrative audit – Law Enforcement Directive – data breach	24	7	17
Data protection administrative audit - GDPR and other	23	9	14
Data protection administrative audit - GDPR and other – data breach	582	51	531

Statements of opinion on legislation in 2021

2021	169
Carried forward from previous year	5

Case type	Total	Carried forward from previous year	New cases
Statement of opinion on draft legislation upon request (opinion on bill, consultation)	163	1	162
Proposal of legislation (statement of opinion of own bill, legislation initiated)	11	4	7

Major areas in international cooperation in 2021 (GDPR, IMI)

2021	895
Carried forward from previous year	167

Case type	Total	Carried forward from previous year	New cases
Cooperation as concerned authority in EEA partner authority procedures – data breach	44	6	38
Cooperation as concerned authority in EEA partner authority procedures under GDPR 56,60,61,62,64,65	1018	161	857

I.2. Annual conference of data protection officers

In view of Article 25/N(2) of the Privacy Act, the President of the Authority convened the annual conference of data protection officers in November 2021. The event served as a forum of regular professional contact between the Authority and the DPOs notified to it by some 9,200 organisations at the time of the conference.

In the spirit of professional cooperation, the Authority provided an opportunity for the data protection officers to shape the content of the presentations at the conference. The President of the Authority assessed the needs of the data protection officers, their professional expertise and their questions and problems related to data protection and the freedom of information affecting a wider range through an online questionnaire accessible from the invitation to the conference.

I.2.1. The results of the preliminary questionnaire survey

The officers notified to the Authority reached the questionnaire exclusively through the link accessible from the e-mail inviting them to the conference, so it was indeed the DPOs – or the users of the e-mail addresses notified as contact details for the DPOs – who were reached by the list of questions. The Authority received 290 responses to the survey, which unfortunately constituted a substantial 100-person decline relative to the interest shown in 2020. Another surprising data was that 49.3% of the respondents filled in the series of questions related to the conference for the first time and the participants participating in the surveys in both 2019 and 2020 made up no more than 26% of the respondents.

Of the voluntary respondents, 14% have been discharging the duties of data protection officer only for a few months; however, 36% have been involved in data protection for over three years, showing a slight increase relative to the results last year. Of the respondents, 52% discharge the duties of data protection officer not just for a single organisation; moreover, 21% were appointed by four or more controllers or data processors.

As seen in earlier years, half of the respondents has tasks related to freedom of information at their organisation, thus presumably a substantial part of them is linked to the public sector.

The results related to the up-to-dateness of the knowledge of the officers revealed that similarly to the substantial decline in 2020 (from 70% to 45% in 2019),

the number of participants in one-day or multi-day training courses requiring personal participation declined also last year (to 26%). At the same time, half the officers (up from 33.4%) expanded their knowledge of data protection through online training courses also due to the pandemic. Thirty per cent of them, i.e. 88 officers carried out their duties without participating in any data protection training at all.

Despite this, only 65.5% of the respondents regarded themselves as well-prepared and up-to-date in data protection law and practice subject to the GDPR; 35.5% of the respondents stated this in the area of audit knowledge and no more than 56.6% concerning the data protection issues of using cameras, even though the conference of 2020 discussed precisely this issue.

Almost two-thirds of the respondents were supported by their respective organisations in expanding their data protection knowledge, typically by participating in organised training. However, there was a 12% increase in the number of officers who did not receive any support for their activities.

Have you received support from your organisation for expanding your data protection and data security knowledge?	2020	2021
Through paid time off work	16,4 %	12,8 %
Through internal training	14,6 %	13,4 %
Through organised training	30,5 %	27,2 %
Through subscription to professional content	19,5 %	20,0 %
None of the above	32,1 %	34,8 %
Other...	6,9 %	6,6 %

More than 81% of the respondents had already been informed about the Authority's information on data processing in relation to the corona-virus before completing the questionnaire. With regard to knowledge that can also be obtained independently, it should be underlined that 81% of the respondents had already read the guidance of the Article 29 Data Protection Working Party on data protection officers; however, hardly more than half of them had read the guidance of the European Data Protection Board on the processing of personal data using video devices. 55% of the respondents read the Authority's 2020 report.

A number of officers visiting the Authority's website renewed in January 2021 weekly or more frequently was roughly of the same proportion (46%) as last year.

How often do you visit the website www.naih.hu?	2020	2021
Weekly or more frequently	45,9 %	46,6 %
Monthly	33,1 %	36,2 %
Less frequently	17,9 %	15,2 %
Never	3,1 %	2 %

Visits to the website of the European Data Protection Board did not change in merit among the officers, even though the Authority has regularly called attention to it in order to access new guidelines.

How frequently do you visit the website of the European Data Protection Body?	2020	2021
Weekly or more frequently	19,8 %	15,2 %
Monthly	31,9 %	37,9 %
Less frequently	35,7 %	36,2 %
Never	12,6 %	10,7 %

In terms of the officers' activities, the percentage results corresponded to last year's figures showing that a significant majority comply with their advisory tasks to be provided to controllers or processors and staff conducting processing work and the management of their entities typically request their professional opinion of the tasks specified under GDPR Article 39. However, similarly to the results experienced in recent years, the majority have not carried out any internal data protection compliance investigation or audit since their appointment, or if they have, they have not documented it and they have not prepared any plan for their activities, which could improve the prevalence of the principle of accountability, the level of awareness and transparency within the organisation.

Since your appointment as data protection officer, have you...	2020 Yes	2021 Yes
provided an opinion on internal rules or a draft concerning the processing of data?	89,2 %	90,7 %
eceived an invitation from the head/management of the organisation to state your position concerning an issue related to data processing?	92,6 %	90,7 %
produced an internal audit plan?	42,8 %	47,2 %
conducted a documented internal audit?	40,5 %	44,8 %

The answers have shown that requests for data protection impact studies have not yet arisen in many places.

Since your appointment as data protection officer, have you...	2020 Yes	2021 Yes
held data protection awareness training?	74,4 %	76,6 %
held data security awareness training?	58,5 %	56,9 %
contributed to drafting an answer related to the exercise of data subject's rights?	61,3 %	68,6 %
contributed to the management of a data breach?	46,9 %	54,1 %
conducted a data protection impact study?	47,2 %	55,9 %

This appeared in the series of questions for the first time, thus no change can be measures, but close to 90% of the respondents saw some improvement in data protection awareness at their organisation.

The organisation appointing the data protection officer published the contact data of the officer in the case of 94.5% of the respondents and only 47% of them recorded personal data breaches since GDPR has become applicable.

In addition to the above, the data protection officers were encouraged to provide feedback on the presentations of the 2020 conference, which showed that they were adjusted to the general preparedness of the participants. The Authority took the questions and feedback received into account when compiling new training materials.

With respect to NAIH's 2019 online conference for data protection officers...						
	1	2	3	4	5	
I have not seen its materials	49	30	72	69	69	I have seen all the videos and documents
they gave me nothing new because of my work / it was not useful	11	26	152	81	19	most of the materials were new to me / were useful
it was about too fundamental issues	12	33	224	16	4	it was too complicated, difficult to follow

I.2.2. Electronic training materials of the conference for data protection officers

The conference presenting the most important results and experiences of data protection and the freedom of information in 2021 was held on 7 December 2021 for data protection officers notified to the Authority who registered for the event. The event was organised as a hybrid with 50 persons participating in person and several hundred people online, in view of the pandemic situation and the large number of those entitled to participate

In his opening address, Dr. Attila Péterfalvi reviewed and assessed the Authority's annual activities and results. He called attention to the renewed website of the Authority, which became accessible in 2021 on the Data Protection Day; he underlined the novelties in the field of electronic administration, the possibility of launching cases at the Authority using the e-Paper service through an identified and secured channel of communication. Addressing the data protection and freedom of information cases related to the pandemic, he also presented statistical data: the number of investigations, authority procedures and submissions for consultation related to the corona-virus exceeded 210. Dr. Péterfalvi called attention to the 2021 amendments of the Privacy Act and to the consultations in relation to providing opinion on legal regulations arising from the Authority's task and to the most important international cases.

Following the President's Introductory Address, dr. Attila Kiss, head of the Department for Certification and Social Relations and one of the organisers of the conference, took the floor. He discussed the information and statements related to the corona-virus published by the Authority in 2021, underlining the pos-

sible legal basis of processing the fact of immunisation against the corona-virus as information concerning health-related data, its conditions according to GDPR Article 9(2) and the related Hungarian regulations. He also called the attention of controllers to the fact that it is an expectation that the Privacy Statement is made available to the data subject when collecting information concerning the fact of immunisation from the data subject even in the case of processing based on legal regulation, which is indispensable for the enforcement of the principle of transparency, as well as the principle of data minimisation and the expectations concerning data security when collecting special category data.

Dr. Endre Győző Szabó, Deputy President, presented the novelties in Guidelines 07/2020 on the concepts of controller and processor in the GDPR, adopted by the European Data Protection Board in 2021. In his presentation, he discussed the responsibility of the controller, which is unlimited in relation to processing, as well as in the relationship between the controller and the processor, as responsibility is borne more significantly by the controller in this hierarchic legal relationship. Then, he analysed the issues of compliance related to the transfer of data to third countries after the Schrems II judgement and data transfer to the United Kingdom following Brexit.

Dr. Viktor Árvay, head of the Department for Authorisation and Personal Data Breach Notification, presented Guidelines 1/2021 on examples regarding personal data breach notification by the European Data Protection Board; it is noteworthy that the Authority initiated its adoption. At the beginning of his presentation, he called attention to the importance of risk assessment in relation to the onset of a personal data breach, and with a view to reducing such breaches, he presented certain criteria of building up indispensable and adequate data security. He highlighted that – when assessing risks – the controller needs to weigh what impact a personal data breach may have on the rights and freedoms of the data subject, as a personal data breach may in the absence of adequate measures taken in time give rise to physical, pecuniary and non-material damage to natural person data subjects. He indicated that with regard to identified risks, 3+1 obligations may appear for the controller under GDPR Articles 33-34. Guidelines 1/2021 presents the good practices, which may facilitate an improvement in the level of data security and the reduction of risks posed by a personal data breach through legal cases and practical examples.

Dr. Dániel Eszteri, head of the Division for Data Breach Notification, presented three legal cases of outstanding importance handled by the Authority in connection with personal data breach management. In many cases, the Authority learns

of the onset of personal data breaches through notifications in the public interest. Generally, these are more serious cases than the ones notified by the controllers as the controllers have not necessarily learned of them or have not been able to identify them as personal data breaches. In relation to personal data breaches related to development errors and other vulnerabilities of the websites of a travel agency and a financial service provider and the erroneous address by Government Office (NAIH/2020/66; NAIH/2020/2094; NAIH-2894/2021), he stated that in many cases the controllers' practice reflects that they failed to carry out risk assessment appropriately not only in determining the expected level of data security, but also with respect to personal data breaches. Thus, it happens that they qualify a higher risk data breach as risk free and because of this, it happened several times that the controller failed to notify the data subject of the data breach, and so failed to meet its obligations set forth in GDPR in relation to high risk data breaches.

The head of the Data Protection Department, dr. Melinda Kovács, highlighted the questions related to the notion, delineation and relationship of controllers and processors from among the questions sent in by the officers. In many cases, without detailed knowledge of the processing operation, it is not possible to unambiguously state whether the person processing personal data is a controller or a processor. The speaker underlined the difference between an insurer and an insurance broker manifested in the fact that the insurance broker qualifies as a processor so long as it does not act for its own purposes, at which point it becomes a controller. In the case of an occupational health physician both capacities obtain, i.e. he may appear as an independent controller beside the employer with regard to processing operations affecting employees, but at the same time, he may also appear as a processor within a narrow range. In addition to these issues, the data protection officers completing the preliminary questionnaire were most interested in the processing of health-related data with the appropriate legal basis, to which the head of department responded by underlining a couple of questions.

Dr. Eszter Horváth, head of the Department of Regulatory Issues and Supervision of Data Classification, spoke of the experiences of personal data breaches taking place in relation to processing operations subject to the Privacy Act from the viewpoint of the Authority. To avoid any misunderstanding, she reminded the audience of the personal and objective conditions, which must be met for processing to be subject to the Privacy Act and not the GDPR. The Police pursues processing operations also for the purpose of law enforcement, but it applies not only the provisions of the Privacy Act because with respect, for instance, to

data processing for HR purposes, the rules of GDPR govern also when managing personal data breaches. As to the expectations governing the management of personal data breaches, the Privacy Act – with the exception of processing for national security purposes – contains similar obligations for controllers. Controllers conducting processing operations subject to the Privacy Act may find it particularly difficult to manage personal data breaches, attributable primarily to the fact that these organisations tend to have a large headcount, they process numerous special category data and a large number of data, they have access to registries and other electronic information systems and are not necessarily able to adequately develop data protection awareness because of the staff being overstretched. In addition, the speaker presented risk assessment criteria and frequent controller errors through several legal cases.

Dr. Júlia Sziklay, head of the Department for Freedom of Information, delivered a presentation on a current project of the Authority, in which staff members of the Authority in cooperation with other experts have been conducting research into the Hungarian and international situation of freedom of information and the possibilities of its development for close to two years. Under the project, beyond the analysis of controller responses given in relation to the obligation of electronic publication and responses given to individual data requests, focus group interviews and data collection by questionnaires were also organised; the results will be accessible from the page of the Authority's website dedicated for this purpose. One of the Authority's objectives includes the development of an online interface aimed at facilitating Government transparency.

The head of the Authorisation Unit, dr. Péter Horváth, addressed the questions received from the officers in relation to the notifications of personal data breaches; in this regard, he spoke about the obligations of controllers. The time and date of learning of a data breach is frequently misunderstood by controllers; he also called attention to the fact that in appropriate cases notification by stages may also be necessary and acceptable provided that all the essential information is not yet available on the data breach. With respect to delayed notifications, it is always necessary to verify the circumstance giving rise to the delay, thus notification by stages may be a better solution in many cases. Questions were submitted, inter alia, about the Code of Ethics and the impact assessment.

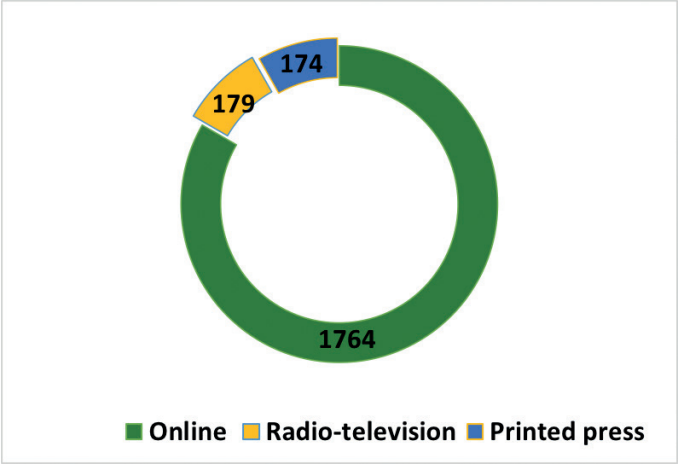
By way of closure, dr. Attila Kiss answered questions received from the participants during the conference. Most questions related to the verification of the fact of immunisation to the employer and there was substantial interest for the problems related to electronic copies and the discharge of their duties and responsibility of the data protection officer.

The recordings of the presentations at the conference can be accessed through the website of the Authority using the MTVA Médiaklikk streaming service from February 2022; thanks to the support of MTVA, the presentations recorded over the past two years also remained accessible to those interested in data protection and freedom of information (https://naih.hu/adatvedelmi-tisztviselok-konferenciaja/).

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

Below we summarise the Authority's media appearances in 2021. Between 1 January and 31 December 2021, members of the media published altogether 2,117 news items about the Hungarian National Authority for Data Protection and Freedom of Information. As to the types of media, most of the time news on the activities of the Authority were broadcast by the online media altogether on 1,764 occasions (83.33%). NAIH was presented in the printed press in 174 cases (8.22%) and 179 times (8.45%) in the electronic media.

Share of NAIH's appearances in the various media in 2021



Source: Observer Budapest Médiafigyelő Kft.

II. Data protection cases

II.1. Application of the General Data Protection Regulation

II.1.1. Major decisions adopted in cases subject to the General Data Protection Regulation

1. Use of artificial intelligence for the analysis of voice recordings by the Customer Service (NAIH-7350/2021., NAIH-85/2022.)

A financial institution (hereinafter: bank) automatically analyses the recorded sound material of calls to and from its Customer Service. Using the results of the analysis, the Bank determines which dissatisfied customer needs to be called back and in relation to this, it analyses the emotional status of the speaker, as well as the other characteristics and it also uses this for the qualification of the work of its Customer Service staff. With the help of speech signal processing based on artificial intelligence, the keywords according to a predetermined list are automatically analysed together with the emotional/mood condition of the speaker. The results of the recognised keywords and emotions are stored per call linked to the given call, and the calls can be listened to within the voice analysis software for 45 days. Based on the above, the voice analysis software ranks the calls, which is in fact a suggestion as to which data subject needs to be called back first and foremost. This data is also stored linked to the call in the voice analysis software. Reviewing these data, the bank's senior employees decide which clients should be called back by the Customer Service.

The purpose of processing is the quality control of calls based on variable parameters, the prevention of complaints and client churn and an improvement in the efficiency of staff members dealing with the calls. The Privacy Statement concerning the phone-based Customer Service provided to the data subjects gives generalities concerning processing and does not include any information of merit on voice analysis. Furthermore, the Privacy Statement only includes quality control and complaint prevention as purposes. The bank based the above processing on its legitimate interests in retaining its customers and improving the efficiency of its internal operations. The processing operations related to these interests, which are strongly different, are not presented separately in the Privacy Statement or dealt with in the course of the interest assessment, they are blurred.

rtificial intelligence means the development of computers and robots in a way that enables their operation so as to imitate or even surpass human capacities. The bank's own data protection impact assessment established that this processing was of high risk for several reasons, it was suitable for profiling or scoring and the processing operation could have a legal impact on data subjects. The impact assessment and the legitimate interest assessment, however, failed to provide solutions of merit for the management of these risks. It follows from the principle of operation of artificial intelligence that in general it is hard to see through it or follow it, so outstanding data protection risks arise even among the new technologies. Inter alia, for this reason, the use of artificial intelligence in the course of data processing requires particular attention not just on paper, but also in practice. The Authority called attention to the risks concerning similar issues as early as in its report of 2012.

The bank's statements also confirm that it was aware of the fact that it had provided neither appropriate information on processing related to the voice analysis under study, nor the right to object for years as it decided that it could not resolve the issue of providing them. The bank's privacy statement and legitimate interest assessment are contrary to this as according to them, the bank fully ensures data subject's rights. According to the General Data Protection Regulation, the basis of processing could only be consent given freely and actively in possession of appropriate and thorough knowledge, the possibility of which did not even arise in the present case. All the bank established was that this processing was necessary for the enforcement of its interest it desired to achieve and it failed to actually examine proportionality and the side of the data subjects, understating the substantial risks to fundamental rights. The bank expressly failed to have regard to the safeguard effect of the right to adequate information and the right to object.

Because of the invalidity of interest assessment, the Authority established that a legal basis according Article 6(1)(f) or any other legal basis listed in Article 6(1) of the General Data Protection Regulation obtained in relation to the automatic analysis of voice recordings by the bank's Customer Service. The generation of a document in itself does not constitute meeting the controller's obligations. In the cases of using a new type of high-risk technology, the existence of actual safeguards and the regular review of merit should be regarded as minimum expectations. In relation to the legal basis of legitimate interest, it is important to underline that a controller may not process personal data at any time for any reason just because there are no other possibilities and other legal basis cannot be applied. The safeguards must ensure in practice the possibility of data subjects

becoming aware of the processing and being able to object to it because after processing – particularly in the case of processing for a short period of time or on a one-off basis – the right to object is deprived of substance.

Based on the above, the Authority established ex officio that the processing practice of the bank related to the voice recording analysis under study infringed Article 5(1)(b), Article 6(1), Article 6(4), Article 12(1), Article 13, Article 21(1) and (2), Article 24(1) and Article 25(1) and (2) of the General Data Protection Regulation. Based on Article 58(2)(d) of the General Data Protection Regulation, the Authority ex officio orders the bank to modify its data processing practice so as to comply with the General Data Protection Regulation, i.e. it should not analyse emotions in the course of voice analysis and to appropriately guarantee the data subject's rights in relation to processing, particularly, but not exclusively, the rights to obtaining appropriate information and to object. In connection with the bank's employees, processing must be restricted to the necessary and appropriate information that must be provided to them, also indicating the related accurate consequences. In addition, the Authority imposed a data protection fine of HUF 250 million on the bank.

2. Lawfulness of processing carried out in relation to the fund-raising activities of an NGO: possible legal bases, obligation to inform (NAIH-3211/2021.).

Because of a change in the regulatory environment, processing for the purpose of direct acquisition is no longer based on authorisation by legal regulation, which means that the controller is responsible for the selection of an appropriate legal basis adjusted to the characteristics of processing as regulated under Article 6(1) of the General Data Protection Regulation. If the controller deems that the legal basis according to Article 6(1)(f) is applicable to substantiate the primacy of its legitimate interest, it has to conduct a legitimate interest assessment test.

According to the position of the Authority, the data processing activities of NGOs carried out upon first contact with a view to fundraising may be based on the legitimate interest of the controller substantiated by appropriate interest assessment in the absence of other legal bases, such as mandatory processing based on legal regulation or the consent of the data subject. Consequently, based on Article 19(1)(a) of Act LXVI of 1992 on the Registration of the Personal Data and Addresses of Citizens (hereinafter: Registration Act), they may request data subject to the conditions set forth in the Registration Act.

If interested, the addressee himself contacts the initiating agency, thus the legal basis of processing for the NGO will in such cases be the consent of the data subject.

The subject matter of the Authority's procedure is the data processing practice of a foundation (hereinafter: foundation) related to fundraising contacts by post; its processing practice related to calling upon those having paid donations to it for further donations and its procedure related to meeting the access request of the data subject lodging the complaint.

The foundation took up contact with persons, on the one hand, who could potentially make donations for the purpose of fund-raising. To do this, it requested personal data from the register of personal data and addresses. A foundation referred to Article 6(1)(e) of the General Data Protection Regulation and Government Decree 350/2011 (XII. 30) on the financial management of NGOs, certain issues of fundraising and being of public utility (hereinafter: NGO Government Decree) as the legal basis of the personal data processed in relation to this (name, postal address).

Called upon by the Authority, the foundation submitted a document called interest assessment test. The foundation cited the legal basis according to Article 6(1)(e) of the General Data Protection Regulation for processing for the purpose of recruiting supporters, i.e. if processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, and it also underlined that through this, the foundation has a legitimate interest in processing the data. In addition, the Privacy Statement accessible during the period of processing under study indicated the consent of the data subjects as the legal basis of processing. However, the foundation failed to cite a legal regulation that would have required it to discharge a public task, as the legal regulation it referred to (NGO Government Decree) does not prescribe such tasks, and furthermore, the foundation also failed to verify the consent of data subjects to the processing.

The Authority examined whether the legitimate interest under Article 6(1)(f) exists on the basis of the controller's statement and the enclosed interest assessment, and it found that the document lacked a consideration of the rights and freedoms of data subjects, an analysis of the impact of the processing on data subjects and a presentation and justification of why the interests of the foundation enjoy priority over these. In other words, the interest assessment only identified the foundation's own interest and it failed to carry out a comparison of the

interests, accordingly it failed to meet the requirements expected by the General Data Protection Regulation. In this way, the foundation was unable to substantiate based on Article 5(2) that its processing was lawful, transparent and having the appropriate legal basis, therefore the Authority established that the foundation infringed Article 5(2) of the General Data Protection Regulation and in view of these, also Article 6(1), because it processed personal data without the appropriate legal basis, unlawfully and non-transparently.

After 3 months following payment by cheque, the foundation sent another postal letter of information to the donors provided that they had not earlier requested the deletion of their personal data. The foundation provided information in the first letter of solicitation about the follow-up to the donation, i.e. about the fact that if the data subject pays money to the foundation using the cheque, the data subject automatically gives his consent to the foundation to process his personal data for the purpose of informing the donor of the work of the foundation and the use of the donation paid and to call upon him for additional donations.

According to the position of the Authority, however, the donation by data subjects through paying a cheque cannot be regarded as a valid consent to processing for the purpose of calling on them to make further donations, i.e. as a specific, unambiguous statement of the data subjects' will. The payment transaction initiated by data subjects by cheque as a mode of making a donation applies to the data subject making a payment and granting a donation to the foundation. In order for the foundation to use the personal data of the data subjects provided in the course of making the payment for a purpose other than processing related to the payment of the donation for contacting the data subjects again after making the donation, the relevant consent of the data subjects is required. The lawfulness of processing can be established, if the controller has a valid legal basis for the processing of the personal data for each purpose of processing and furthermore, if the data subject received appropriate information and possibility for decision-making concerning the purpose for which his personal data would be processed.

According the findings of the Authority, the foundation processed the personal data of data subjects who had earlier made donations to it without a valid legal basis for the purpose of contacting them following the donation, because the content elements required for the validity of consent were missing whereby the foundation infringed Article 6(1) of the General Data Protection Regulation, the principle of lawfulness according to Article 5(1(a), and Article 7(1).

The foundation's statement, the content of the Privacy Statement and the information in its records of processing present processing differently both in terms of purposes and legal basis, through which they did not present the picture of a thoroughly considered processing and did not provide genuine information on the processing, whereby the foundation infringed the obligation to provide information in a concise, transparent, intelligible and easily accessible form using clear and plain language as set forth in Article 12(1) of the General Data Protection Regulation and the principle of transparent processing according to Article 5(1)(a). Furthermore, the foundation failed to provide appropriate information on data processing for the purpose of contacting the data subjects following the donation in the course of contacting the data subjects by mail whereby it infringed the provisions of Articles 13 and 14 of the General Data Protection Regulation.

According to the Authority's position on meeting the data subject's right to access, even if the data subject requests information which is not or no longer available to the controller, this may not serve as the basis for totally omitting to provide information, i.e. the controller must, in this case, provide transparent information to the data subject based on Article 12(1) of the General Data Protection Regulation. If the data subject exercises his right to access, the controller is under an obligation to provide information, and the controller is obliged to respond appropriately to the data subject's request.

3. Customer satisfaction survey based on legitimate interest (NAIH-2857/2021)

Having had his car inspected/serviced by the obligee as a specialised service station, the complainant provided his e-mail address to the obligee upon its request. At this e-mail address, he received an e-mail from the obligee to measure his satisfaction, on the basis of which he expressed his opinion. After this, he received an unsolicited e-mail sent to this e-mail address with the request to fill in a satisfaction questionnaire related to the above, then another e-mail, in which he was again invited to complete the questionnaire because of not having answered the former e-mail. These e-mails included the vehicle identification number of the complainant's car, but the e-mails were not sent by the obligee but by a third person the complainant could not identify. The complainant's consent to having his data forwarded was not requested, and he did not receive any information about this. The unsolicited e-mails contained a generic designation in the name of [car brand name], not the specific legal entity on whose behalf they were sent.

According to the facts of the case identified, the e-mails in question were sent by the importer in a contractual relationship with the obligee as the exclusive Hungarian importer of the type of cars corresponding to the complainant's car through a data processor. With respect to the e-mails in question, the controller was not the obligee but the importer. Information on this is generally provided together with the service worksheet, which was omitted in the present case. According to the information, the data may be forwarded to the car manufacturer as well; this, however, is only done in the form of anonymous statistics according to the exposed facts of the case, so the Authority did not investigate this – incidentally cross-border – issue. Ex officio, the Authority extended its investigation to the general data processing practice of the importer related to the measurement of customer satisfaction.

In this individual case, the complainant received no information at all about data processing according to the statements by the importer and the obligee. In the absence of proper information and effective rights of the data subject, the importer could not have a legitimate interest in the individual case.

With regard to data processing practices, the importer's legitimate interest does not apply to obtaining knowledge about customer satisfaction for the purposes of monitoring its service and trading partners and quality assurance in the face of providing adequate information and processing too much personal data. The importer cannot substantiate in what way the following processed data are linked to the indicated purposes of measuring satisfaction and complaint management: customer's name, e-mail address, address, phone number, age, sex, undercarriage number of the vehicle, the car's registration number, technical data, the name of the brand partner used, the date of the service used and the content of the feedback. In the absence of feedback from the customer or non-negative feedback, any data other than the statistical data of the car and the work at the service station, while in the case of negative feedback and an individual complaint, any processing of data other than the personal data indispensable for complaint management is in breach of the law, and therefore it has to be modified. A data protection fine of HUF 5 million was imposed in the case.

4. Data management related to condominium CCTV systems (NAIH-5896/2021., antecedent case numbers: NAIH/2019/3200., NAIH/2020/1000.)

The Authority investigated a camera system in a condominium in a data protection authority procedure. In addition to reprimanding the condominium for unlawful data processing, the Authority made several significant findings in its decision.

In the course of clarifying the facts of the case, the person and liability of the controller were examined. Although the complaint indicated the company representing the condominium as the controller, the Authority qualified the condominium as such. For this, the Authority took the explanation to the Condominium Act into account, according to which the condominium has only relative legal capacity, thus it has no legal capacity with regard to personality rights, and it cannot be either on the side of the injured party or that of the infringing party in the infringement of personality rights. In relation to this, however, the Authority's position is that this has relevance from the point of view of civil law. What is relevant from a data protection perspective is that a condominium as an independent subject of the law qualifies as controller as "any body" according to the definitions of the General Data Protection Regulation, which is represented – organisationally – by a natural person, the joint representative (chairman of the management committee), or by another non-natural person, such as in this case, a company. For example, a condominium may process the personal data of its co-owners when it operates security cameras. This is in line with the statement of the condominium in the present case and the fact that in all the contracts concluded for the installation and operation of the camera system the condominium is the client and not the company acting as joint representative or the person representing its or its manager.

In general, however, it cannot be excluded that, in certain cases, the person or body acting as the joint representative of the condominium may also become an independent controller for the purposes of the processing set out in the Rules of Organisation and Operation of the condominium. The person or body acting as joint representative or the representative of the body also becomes a data controller if, in certain cases, it overrides the decision of the condominium. However, in the present case, no such circumstances existed.

Another important finding of the decision concerned the legal basis of processing. The condominium cited Section 25 of the Condominium Act – the number of votes required for the decision concerning the instalment of cameras – as the legal basis of processing. However, the Authority disagreed with this because according to its position, the legal basis of processing may be that of legitimate interest according to Article 6(1)(f) of the General Data Protection Regulation. The reason for this is that the interest of the condominium as controller and of the co-owners holding at least two-thirds of the total ownership shares, in the given case override the right of the co-owners to the protection of their personal data who did not vote for the camera system in view of the results of the vote.

In addition, according to Guidelines 3/2019 on processing of personal data through video devices by the European Data Protection Board, the legal basis applicable to CCTV surveillance may be primarily that of legitimate interest.

The cameras operated by the condominium included some that also monitored public areas. However, monitoring public areas is only possible in a limited range of cases, under explicit legal provisions, as this activity may encroach upon the privacy of the person being monitored by the camera when processing personal data even against his will.

The Authority has also taken into account the provisions of Guidelines 3/2019 in connection with public area surveillance cameras, which, in addition to stating that, in general, the use of a camera surveillance system for the purpose of monitoring a private property may extend to the boundary of the property, it has acknowledged that in exceptional cases a situation may arise when the extent of the video surveillance cannot be narrowed down to the area of the private property because in this way it would not provide sufficiently efficient protection. With the application of appropriate technical or organisational measures (e.g. covering up the area not relevant for the purpose of monitoring or filtering of the monitored part by means of IT tools), the controller is entitled to extend monitoring by camera to the immediate surroundings of the area in its ownership.

At the same time, if the controller does not apply solutions covering up public areas, or if the controller deliberately operates a camera system surveying a public area, it has to apply all the requirements of the General Data Protection Regulation specified for controllers, including, inter alia, it has to base its processing on the appropriate legal basis.

In view of the fact that in the present case, some of the cameras of the condominium also surveyed a public area and the condominium did not apply solutions for covering it up, the Authority established that the condominium operated cameras for public area surveillance without legal basis.

According to the request, persons without appropriate qualifications also had access to the live images streamed by the cameras and to their recordings. However, it follows from the principles of integrity and confidentiality that personal data have to be processed so as to ensure their adequate level of security and confidential processing, inter alia, in order to prevent unauthorized access to personal data and devices used for the processing of personal data, and their unauthorized use.

According to the act on condominiums, the operator of the camera system may only be a person defined in the act on the rules of the activities of bodyguards and security guards and private investigators. This act requires specific qualifications for those who are authorised to perform the activities of bodyguards and security guards. Accordingly, those persons may carry out the activities of bodyguards and security guards and operate the condominium's camera system who have the qualifications of a security guard, bodyguard, asset guard or security organiser. According to the position of the Authority, operation includes the monitoring of live streamed images and access to recordings, i.e. only those persons may have access to the recordings, who have one of these qualifications.

In view of the fact that in the course of the authority procedure for data protection, it was not verified that the managing director of the company acting as the joint representative of the condominium, or the chairman of the Audit Committee have such qualifications, the Authority established that these persons were unlawfully authorised to have access to the recordings made by the camera and therefore, the condominium violated the principle of integrity and confidentiality.

Because of all these infringements, the Authority reprimanded the condominium and ordered that if it intends to carry on the processing in relation to camera surveillance, it must be rendered lawful based on the appropriate legal basis and the interest assessment needed for that must be carried out in order to comply with the requirements of the legal basis according to Article 6(1)(f) of the General Data Protection Regulation. In addition, the condominium must not operate cameras surveying public areas, i.e. it is must terminate processing related to such cameras, or it should modify the angle of view of these cameras. Finally, it should process personal data based on the appropriate processing and access rules in relation to camera surveillance in order that only persons having the qualifications of a security guard, bodyguard, asset guard or security organiser should have access to images live streamed by the cameras and to the recordings made by them; it should provide the appropriate information to data subjects including that set forth in Article 13(1)-(2) of the General Data Protection Regulation.

5. Making a voice recording unlawfully accessible – unlawful processing of the personal and special category personal data of a minor data subject (NAIH-1743/2021)

Based on a petition, the Authority launched a data protection procedure; according to the petition, the petitionee secretly recorded a conversation in which per-

sonal data and special category of personal data of the minor petitioner were discussed and subsequently published in a Facebook group.

The information in question was disclosed at a meeting organised with a view to discuss a problem related to the petitioner as indicated by the head of the kindergarten, in which in addition to the petitioner's mother and the head of the kindergarten, the petitionee also participated who is the mother of one of the kindergarten group mates of the petitioner. According to the petition, the petitionee secretly made a voice recording with her mobile phone in her pocket from the first 46 minutes of the conversation and uploaded it to a Facebook page, which was the page of a group created for kindergarten parents. According to the statement of the petitioner, the petitionee did not ask for the consent of the legal representative of the petitioner for making the voice recording, and she informed her neither of the fact of making the recording, nor its use, meaning its disclosure.

When exploring the facts of the case, the Authority established that the recording was truly made of the conversation mentioned by the petitioner, which included numerous personal data of the petitioner, such as his name, address, the fact that he did not belong to the given kindergarten district, it included information presenting his behavioural problems, as well as statements affecting particularly sensitive areas of privacy, according to which there were three deaths in the family in the recent past. In addition, special category personal data were also stated, i.e. information on his health - taking medication, examinations, development, and the fact of illness as well. It was established that the recording was removed from the Messenger group, but it was sent by e-mail to three additional persons.

Based on the statements of the petitionee made in the course of the procedure, the reason for making the recording was that professional reasons were also voiced in the course of such a conversation, which can be difficult to recall later, and the purpose of disclosing it in the Messenger group used by the parents was to inform the other parents, because as far as she knew, apart from her, no parent was aware that "a small child struggling with severe problems of the nervous system attended the group" and she was worried about the children. She also invoked the interests of the children as the reason for sending the recording to three persons by e-mail.

However, the Authority established in its decision that as far as the sharing of the recording was concerned, the purpose cited by the petitionee could not be regarded as a lawful purpose according to GDPR, because the conversation took

place with the participation of two persons concerned in the main subject matter with the assistance of the head of the kindergarten, i.e. among three persons in private, and although conflicts related to other children and general problems were also discussed, the point of departure was the conflict between the child of the petitionee and the petitioner.

Furthermore, according to the position of the Authority, this kind of transfer of information, in addition to being an intervention of unnecessary extent into the privacy of the petitioner, is inappropriate because it carries the possibility and risk that in possession of the link – or in the event of sending the file by e-mail – the addressee may forward the recording also to other persons.

Over and above these, the Authority established that the data processing by sharing the recording was without a legal basis. Furthermore, the principle of fair processing was also violated in view of the fact that the petitionee made the recording in secret, without the representative and those present being aware or informed about it, knowing from the very beginning that the conversation was to focus on the problems related to the behaviour of the petitioner and their background. Having no inkling about this, the representative as the mother of the petitioner shared information sensitively affecting the petitioner's privacy, as well as information on his health condition. In the course of the conversation, the petitionee underlined several times and also attempted to reinforce with her questions and comments that the petitioner was sick and did all this being aware of the recording in progress.

Based on the above, the Authority sustained the petitioner's petition and reprimanded the petitionee based on GDPR Article 58(2)(b) because she infringed the provisions of GDPR Article 5(1)(a), (b) and (c) and Articles 6 and 9, and based on its powers as set forth in GDPR Article 58(2)(f), it prohibited the disclosure of the recording on an online platform or in any other way, and ordered the petitionee to refrain from such behaviour in the future. In addition, based on the provisions of GDPR Article 58(2)(g), the Authority ordered the petitionee to notify the addressee to whom the recording was forwarded by e-mail of the necessity to delete the recording.

6. Disclosure of personal and special category personal data of a minor in the media (NAIH-68/2021., antecedent: NAIH-6450/2020.

The petitioner, a minor acting through his legal representative, lodged a complaint with the Authority in relation to a report aired by a national commercial

television channel. According to the petition, news was broadcast reporting on the fact that two young boys were injured in an accident at a family home of a named settlement. The report showed the street, the house, its roof structure burnt down and details of the - life-threatening - health condition of the injured boy were disclosed, stating his given name.

According to the position of the Authority, if sufficient information is provided about a data subject, which can make his person unambiguous for a certain group, even if it is small, he must be regarded as identified. A private individual, who is not a public actor in a broader sense, such as a politician, media personality, publicly known figure of cultural, social or sports life, or another person widely known for a local community, etc. can generally be identified only by acquaintances, friends, relatives, colleagues, schoolmates, etc., i.e. personal acquaintances, provided that his given name and place of residence are known.

In its procedure, the Authority established that together with all the information provided, the report was all in all suitable for identifying the data subject for individual viewers. The presentation of the family house and its environs, the disclosure of the child's given name and the fact that he belongs to a young age group, followed by the information that "the family did not wish to make a statement" together made it clear that the subject of the report was the family living in the given house.

The totality of information linked to the house and the family presented and the youngster with the given name in the named settlement unambiguously identified the data subject to those knowing him.

The controller, however, had neither appropriate purpose, nor legal basis for the disclosure of the health-related data on the identifiable data subject.

In view of the fact that in this case, the report was not on a specific person – in which case, obviously, the presentation of the identified person is indispensable – but an event, a report on that event according to the position of the Authority could have been produced without disclosing information suitable for identifying the data subject. The disclosure of information enabling the identification of the data subject did not provide any kind of additional information with regard to the purpose of the report in the public interes.

The processing did not have a lawful legal basis either because, in general, a reference to journalism as an activity in the public interest as referred to by the

controller is not acceptable as the legal basis of processing and several court judgments confirmed that the legal basis of such processing is the legitimate interest of the controller. The petitioner, however, failed to substantiate that such a legitimate interest existed, nor was it able to verify compliance with the exception according to Article 9 concerning the disclosure of health-related data.

Moreover, the petitioner's family objected to having any kind of content broadcast about them in advance and the channel broadcast the report in spite of this objection. Although the objection was only received by the staff member making the report, the reason for this was that the staff member contacted the family in a Messenger message, first reaching the mother of the injured boy, then the boy's brother when no answer was forthcoming from her, , but the reporter failed to take into account the objection of the boy. The Authority's position is that an argument concerning the professional freedom of an editor does not exempt the petitionee from its responsibility as controller. According to the petitionee, it does not have internal procedures or regulations governing the collection of statements from individuals and the recording of consents, so in the absence of organisational measures under GDPR Article 25, the controller may not have been aware of the petitioner's prior objection, even though the relevant statement was in the possession of one of its staff members.

The Authority imposed a data protection fine of five million forints and ordered the erasure of the data; the petitionee satisfied the order. The judgment of the court upheld the Authority's decision.

7. The content of the data subject's right to access with respect to data generated in the course of examination by an expert witness (NIAH-7689/2020; antecedent: 2658/2021)

The complainant participated in an examination by a seconded forensic expert, after which he requested the expert to let him have copies of all the data he had provided during the examination, as well as copies of the professional data generated by the expert in relation to the evaluation of the tests (marking and encrypting his responses given while doing a Rorschach-test and a document containing the calculation of the aggregated indicators).

After analysing GDPR, the Act on Experts, the Fundamental Law and the professional rules applicable to experts, the Authority concluded that the right of access to these data cannot be exercised due to the independence of the expert, the interests of other actors in the procedure concerned by the secondment, as

well as the exclusion of other data subjects' rights in the data to be accessed (rectification, erasure).

The Authority is of the opinion that the data subject may not exercise additional rights with regard to the experts' professional markings and the professional methodological process, even if the data subject has the required expertise; he cannot request correction of the "erroneous data", he cannot ask for rectification meaning that he may not request the expert to arrive at some other conclusion, because a modification of merit cannot be regarded as the right to rectification as set forth in GDPR.

Access to the professional material of the expert by the data subject could influence the results of an eventual subsequent examination whether carried out in the given procedure or in an additional one, it would not show a real result, if the data subject could be in possession of the data, which resulted in the given conclusion.

The phrase "shall not adversely affects the rights and freedom of others" set forth in GDPR Article 15(4) can be interpreted according to the Authority so that the data subject should not have access to information, which could generate an expert opinion reflecting a status other than the real one about him with a view to the fairness of court procedures and expert opinions.

Summarising the above, the Authority arrived at the conclusion that it cannot be reconciled with the principles and ideology of GDPR and the Hungarian legal regulations in force, if the data subject has access to certain data for a purpose other than checking the lawfulness of processing, and it may serve for checking on the experts' work bypassing legal requirements or in order to enable their use for influencing the results of a subsequent expert opinioni.

Over and above the data provided by him and the content of the completed expert opinion, the data subject is not entitled to have access to indicators, markings, other professional materials generated by the expert during his professional work, not indicated in the expert opinion, because access to them would serve a purpose other than that stipulated in GDPR, namely the checking of processing, hence the Authority did not order the issue of copies of these data.

8. Access to health-related data concerning the psychiatric treatment of a minor; the limits of the right to access (NAIH-1612/2020; antecedent: NAIH-103/2021

The mother acting as the legal representative of her child wished to have access to the entire material of the psychiatric treatment of a minor (including all the notes, treatment logs, drawings, tests, their results, other memos generated in the course of the child's treatment, furthermore all the notes made by physicians or expert nurses in relation to the child, every perceived, examined, measured, projected or derived data. as well as all data, voice recordings, protocols, copies of electronic and paper-based correspondence, which could be related to and affect the foregoing).

The healthcare provider refused to issue the copies, citing Section 193 of Act CLIV of 1997 on Healthcare[4] (hereinafter: Healthcare Act).

Based on the available documents, the Authority established that the psychiatric treatment and the health status of the child – the child had been diagnosed with emotional disturbance, presumed or genuine intend to commit suicide, whose problems can be traced back to the conflicted relationship between the parents according to the documents – genuinely carries the possibility that access to the data by either parent of the child could have detrimental legal consequences for the child. The dispute between the parents had substantial impact on the child's health status, the child's statement concerning the parents, his thoughts and feelings about the parents disclosed in the course of the examinations were recorded in the documents.

Making use of the authorisation set forth in Section 193 of the Healthcare Act in refusing to allow the right to access is not without limitation and according to the Authority's position it does not provide an opportunity for ordering a restriction of the right without a detailed examination concerning the entire documentation. So, the controller is not entitled to restrict the right to access by the legal representative in general without examining its justification in detail, in this case bearing in mind the interest of the data subject who is a child. The controller may not arbitrarily adopt a decision, whose lawfulness cannot be verified and at least the onset of a disadvantage is not likely for every document and data affected by the refusal to disclose.

4 Article 193 of the Healthcare Act: in the case of a psychiatric patient, the patient's right to access medical records may be exceptionally restricted if there are reasonable grounds to believe that access to the medical records would seriously jeopardise the patient's recovery or violate the personal rights of another person. Only a doctor is entitled to order a restriction.

When making a decision based on Section 193 of the Healthcare Act, it is not sufficient according to the Authority's position to declare that access to the documentation could have detrimental consequences with regard to recovery as this is a precondition to applying this provision of the law, it has to be evaluated separately from it to see for what reason access to the specific content could be injurious and what sort of detrimental consequences it may have with regard to the cure of the patient. Section 194 of the Healthcare Act expressly requires justification. Naturally, the controller may not refer to the specific content of the document as a result of such an examination, but it has to examine to what extent and for what reason any given document may be subject to the restriction.

The Authority ordered the controller to examine item-by-item with respect to every document related to the child whether access by the mother to the entirety or a part of a given document or data included in it could have a detrimental consequence with regard to the cure of the child, or whether a conflict of interest exists between the mother and the child with regard to access to the data, also considering the time elapsed since the treatment; and if the controller did not find the onset of such a detriment with regard to any document or a part thereof, or any conflict of interest in relation to it, the controller should issue the copy of the document or a part thereof to the complainant.

9. The processing of data subject's phone numbers in the course of an information campaign related to the corona-virus pandemic (NAIH-1366-1/2022.; antecedent: NAIH/2020/3082.)

The Authority received over a hundred complaints objecting to the data processing practice of the phone-based information campaign of Jobbik Magyarországért Mozgalom (hereinafter: Jobbik) related to the corona-virus pandemic. According to the complainants, the phone calls were made to phone numbers, of which they had earlier declared that they did not wish to receive phone calls for advertising purposes and furthermore, they did not receive any information in the course of the call, for what person their personal data were processed and from what source they obtained them.

As the Authority received many similar complaints, it examined them in a combined form.

In the course of the inquiry procedure, the Authority tried to contact Jobbik on several occasions, as well as Irántyű Politikai és Gazdaságkutató Intézet Kft., asking for information about the methodology of the campaign, the mode of making the phone calls, the source of the database and the storage of the phone numbers.

Jobbik was not cooperative in the course of the inquiry procedure, giving evasive answers to the questions of the Authority and it failed to respond to the additional contact by the Authority in the course of the investigation.

In view of the fact that Jobbik was not cooperative in the inquiry procedure, the Authority conducted an Authority audit ex officio at Jobbik and its processor Irántyű Politikai és Gazdaságkutató Intézet. In the course of this, the Authority held an on-site inspection, in the course of which it reviewed Jobbik's data processing processes.

In the course of its inquiry procedure, the Authority established that:

(1) with respect to public phone numbers it regards the legal basis according to GDPR Article 6(1)(f) acceptable; in contrast, with regard to phone numbers where the data subjects did not give their consent to receiving phone calls for the purposes of direct marketing, providing information, public opinion polls or market research, or expressly objected to such practices by way of statements, Jobbik had no legal basis, and therefore infringed GDPR Article 6 with regard to this processing;

(2) through the fact that the practice by Jobbik and Irántyű Intézet was not uniform and the information provided to data subjects concerning objections was not unambiguous to the data subjects, Jobbik infringed its obligations according to GDPR Article 12(1) and (2);

3) furthermore, in view of the fact that during the period of the campaign, Jobbik did not have an appointed data protection officer, it infringed GDPR Article 37.

In view of all this, the Authority called upon Jobbik:

(1) not to collect phone numbers in the future with regard to which the subscriber stated that he does not wish to receive phone calls for the purposes of direct marketing, providing information, public opinion polls, market researcher, or commercial advertising;

(2) to review its processing practice and modify its information accordingly concerning its processing operations;

(3) to meet the data subject's request in accordance with GDPR Article 12(1) and pursuant to GDPR Article 12(2) it should clearly facilitate the data subjects' exercise of their rights;

(4) to review and transform its processing practice, taking into account the principle of accountability when verifying the legal basis for its processing and appropriately cooperate with the Authority in the future.

The Authority also ordered Iránytű Intézet to appropriately cooperate with the Authority, should it become affected by the Authority's procedural acts in the future.

In view of the fact that as a result of the audit by the Authority, finally both Jobbik and Iránytű Intézet provided appropriate information to the Authority and in view of the fact that the system of the online accessible interface containing the contact data of natural persons used by Jobbik as the primary source does not indicate any objection to calls aimed at providing information, public opinion polls or market research, in this case, the Authority waived launching its procedure, but at the same time, it decided to publish its call in its website based on Section 58(2) and Section 59(1) of the Privacy Act. The call is accessible on the Authority's website.[5]

II.1.2. Recommendations issued by the Authority

1. Recommendation to amend the Privacy Act with a view to establishing the possibility of efficiently combating websites implementing grossly unlawful processing operations by restricting access to the content on these websites or by removing such content

On 13 July 2021, based on Section 57 of the Privacy Act[6], the Authority made a recommendation to the Minister of Justice for the amendment of the Privacy Act with a view to establishing the possibility of efficiently combating websites implementing grossly unlawful processing operations through restricting access to the content in these sites or removing such content.

5 https://www.naih.hu/adatvedelmi-jelentesek

6 Privacy Act Section 57: *"If, based on the findings of the inquiry, the Authority considers that the infringement or its imminent threat is attributable to an unnecessary, unclear or inadequate provision of law or a public law regulatory instrument, or it can be traced back to the lack or deficiency of legal regulations concerning the issues of data processing, then, in order to prevent future infringements and their imminent threat, the Authority may present recommendations to the organ authorised to adopt such laws or issue such public law regulatory instruments, or to the organ drafting the law. In the recommendation, the Authority may propose to amend, repeal or adopt a law or public law regulatory instrument. The requested organ shall inform the Authority within sixty days of its position, or of the measures taken in conformity with the recommendation."*

In some of the data protection procedures in front of the Authority, notifiers object to infringements implemented in websites where, on the one hand, the person of the controller is not identifiable and the infringement constitutes a substantial breach of personality rights on the other hand, because, for instance, it involves the disclosure of information on the sexual life and orientation of data subjects, which are special category data under Article 9 of the General Data Protection Regulation, without the consent of the data subjects and in many cases alongside other identifying data. In the course of its practice, the Authority also met with infringements of Article 10 of the General Data Protection Regulation by the unlawful processing of personal data in decisions concerning the establishment of penal liability and criminal acts or the related security measures. Recital (38) of the General Data Protection Regulation declares as a general rule that children merit specific protection with regard to their personal data as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. The former legal environment did not enable an efficient stand to be taken by the Authority in the absence of knowledge of the person of the controller or its cooperation in such cases.

In many of the above cases, the infringing content is located under domains outside the European Union, or at hosting service providers operating outside the European Union, hence the identification of the controller or the processor and ordering them to erase the data is not always successful. Frequently, online service providers outside the European Union, particularly those providing unanimous domain services, failed to cooperate with the Authority and there are numerous impediments to the implementation of the Authority's decision against them.

For these reasons, the Authority initiated the amendment of the Privacy Act in its recommendation NAIH-6164-1/2021 with a view to letting the Authority have an efficient instrument for more vigorously combating the above infringements. Rendering data disclosed by electronic communications networks (hereinafter: electronic data) inaccessible is an existing instrument provided by criminal regulations for the courts, in addition sectoral legal regulations enable, for instance, the National Tax and Customs Administration and the Transportation Authority to use this with the technical cooperation of the Nemzeti Média- és Hírközlési Hatóság (National Media and Communications Authority, hereinafter: NMHH). Based on the above recommendation, the Privacy Act was amended as of 1

January 2022 and new Sections 61/A - 61/D regulate the Authority's new instruments, the temporarily removal of electronic data and making electronic data temporarily inaccessible.

The Authority may order the temporarily removal of electronic data in the course of its data protection procedure or its audit. The precondition to ordering this is that in the absence of this measure, the delay would pose an irreparable and serious damage to the right to the protection of personal data, and that the data concerned qualify as the personal data of a child or the special category data of any data subject or criminal personal data. In its order concerning the temporarily removal of electronic data, the Authority can obligate the hosting service provider or the intermediary service provider pursuing hosting services as specified in the Act on certain question of electronic commercial services and services related to the information society to temporarily remove electronic data, with which they have to comply, within one workday. If the obligated service provider fails to implement the Authority's order to temporarily remove electronic data, the procedural fine of a hundred thousand forints to twenty million forints can be imposed on the service provider, moreover, as a temporary measure, the Authority may order rendering the electronic data temporarily inaccessible.

The Authority discloses the order for making electronic data temporarily inaccessible by way of an announcement. The day of the communication of the order is the third day following the publication of the announcement. All providers of electronic communications services are subject to the order, without being specified in the order. The implementation of the temporary unavailability of electronic data is organised and supervised by the NMHH on the basis of the Act on Electronic Communications.. The Authority may impose a procedural fine of a hundred thousand forints to twenty million forints on the electronic communication service provider, which fails to comply with the order concerning the temporarily removal of electronic data.

The Authority may also order the temporary inaccessibility of electronic data or the temporary removal of electronic data in the framework of the enforcement procedure pursuant to Article 61(7) of the Privacy Act if the disclosure of any electronic data constituting personal data is unlawful on the basis of a final decision of the Authority in a data protection authority procedure and the Authority has ordered its deletion, but the controller has not carried out the erasure despite repeated requests by the Authority. In such a case, the above rules shall apply mutatis mutandis.

2. Recommendation for amending Section 7(7) of Act XLVII of 1997 on the processing and protection of personal data concerning health and related personal data (hereinafter: Health Data Act)

With reference to Section 38(4)(a)[7] of the Privacy Act, the Authority initiated the amendment of Section 7(7) of Act XLVII of 1997 on the processing and protection of health and related personal data (hereinafter: Health Data Act) with the Minister of Human Resources.

Notifications of similar content were received by the Authority from both private individuals and healthcare providers within a short period of time raising issues of interpretation related to the healthcare sectoral legal regulations and data protection rules.

Based on the notifications, the Authority noted that certain provisions of the Health Data Act and Act CLIV of 1997 on Healthcare (hereinafter: Healthcare Act) are not in line with the data protection regulation in force, hence the Authority submitted a recommendation of amendment to the Minister for Human Resources.

According to the wording of Section 7(7) of the Health Data Act in force at the time of the notification *"in the event of the death of the data subject, his/her legal representative, close relative and heir shall be entitled – based on a written request – to have access to the health data related to the cause of death and related to medical treatment prior to the death, to inspect the health documentation and to receive a copy of them at his/her own costs."* Pursuant to Section 3/A of the Health Data Act: *"The mandatory rules incorporated in EU legal acts or legal regulations on the processing of personal data incorporated in the health data and health documentation shall apply to the processing of the circumstances of the death of the deceased person and the cause of death, as well as the personal data included in the health documentation of the deceased person."*

According to the Authority's interpretation, even in the absence of an express reference to Section 3/A of the Health Data Act, the legislator's intention may be presumed with respect to the fact that Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement

7 Pursuant to Section 38(4)(a) of the Privacy Act: *"Acting within its functions referred to in paragraphs (2) and (2a), the Authority: a) may make recommendations with respect to new laws and to the amendment of laws pertaining to the processing of personal data, the access to data of public interest and to data accessible on public interest grounds, and shall give its opinion with respect to draft laws affecting its functions;"*

of such data and repealing Directive 95/46/EC (hereinafter: GDPR or General Data Protection Regulation) is implicitly applicable to Section 7(7) of the Health Data Act.

In this case, if GDPR is applicable to the above processing, the cost reimbursement rule according to the Health Data Act – whereby a person entitled to obtain copies of the documents may do so only at his/her own cost – is not reconcilable with the rule under GDPR requiring the provision of a copy free of charge on the first occasion [GDPR Article 15(3): *"The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs."*

According to the position of the Authority, the amendment of these provisions has become necessary because it is indispensable that the obligation to apply the GDPR in the underlying context, must be clearly derived from the provisions of the sectoral laws, including the GDPR requirement to provide the first copy free of charge

As a result of the Authority's request, the competent Minister amended Section 7(7) and Section 24(11) of the Health Data Act with effect from 29 June 2021, thereby bringing the contested provisions into line with the provisions of the General Data Protection Regulation by stating that first-time copying is free of charge.

3. Recommendation on certain data protection requirements related to data processing by political parties and organisations

On 19 February 2021, the Authority launched a recommendation on certain data protection requirements related to data processing by political parties and organisations. In view of the fact that the Authority has already presented this recommendation in greater detail in its 2020 annual report, this will not be repeated in the 2021 annual report, but the full text of the recommendation will continue to be available on the Authority's website[8].

8 https://www.naih.hu/ajanlasok

II.1.3. Annual conference of data protection officers: questions and answers

The annual conference of data protection officers was organised pursuant to Section 25/N(2) of the Privacy Act on 7 December 2021, where staff members of the Authority provided answers to the questions previously asked by the data protection officers, answering those considered to be more significant. This subsection summarises these questions and the detailed answers of the Authority.

1. Do 'external contracted' private (even self-employed) partners performing the same or different specific tasks as the controller's own employees qualify as processors or independent controllers?

Pursuant to GDPR Article 4(7) controller means the natural or legal person, which alone or jointly with others determines the purposes and means of the processing of personal data. It follows that the decisive element of the delineation of the capacity of controller/processor is whether the given person makes decisions of merit concerning processing or no. By way of examples, decisions of merit concern the following processing circumstances, which may be regarded as cornerstones:

- determination of the purpose of processing,
- determination of the range of the processed data,
- decision on the legal basis of processing,
- decision on the period of processing,
- decision on access to personal data,
- decision on forwarding the data,
- decision on the use of personal data for different processing purpose in the course of other activities,
- decision on making use of a processor,
- ensuring and implementing data subjects' rights,
- decision on bringing the fundamental data security measures.

As against this, the capacity of processor requires that the processor carries out the processing of personal data on behalf of the controller and carries out the relevant processing operations. Another condition is that the processor be an independent subject of the law, separate from the controller. Another important characteristic is that the processor carries out the instructions of the controller, it may process personal data exclusively under the written instructions of the con-

troller (the only exception to this rule is if the processing of personal data is required by legal regulation for the processor).

So, the answer to the question is that persons, organisations ("external partners"), which do not constitute part of the controller's organisation, process personal data on behalf of (entrusted by) the controller and in the course of this, do not make decisions of merit concerning processes, but take action within the limits specified by the controller and according to its instructions qualify as processors. If they are competent to make decisions of merit on certain partial issues, or going beyond the scope of their mandate , they bring decisions of merit, they qualify as controllers in this part and, depending on the circumstances of the case, they may qualify as joint controllers, or they may be responsible for their activities as independent controllers.

The Authority recommends to review Guidelines 07/2020 of the European Data Protection Board on the concepts of controller and processor in the GDPR[9].

2. "Evaluation of the activities of financial intermediaries (and insurance brokers): can intermediaries (brokers) be regarded as independent controllers because of their independent activity of intermediation carried out in a business-like manner (whether dependent or independent intermediaries according to the banking act)."

In general, insurance brokerage activity qualifies as processing activity so long as the broker takes action in order to perform the obligations undertaken in the contract concluded with the insurer basically within the framework of the insurer's instructions.

Thus, for instance, the insurance broker acts in the capacity of processor when entering into contract and keeping it on file, as well as in relation to the enforcement of claims for damages related to the insurance contract provided that this is its task based on the contract concluded with the insurer and insofar as in these cases the insurance broker carries out the instructions of the insurer, it does not specify an independent processing purpose.

9 https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/guidelines-072020-concepts-controller-and_hu

If, however, for instance, the insurance broker has/may have access to the documents containing personal data in connection with its own commission through the insurer's portal, which is also a customer database, it will qualify as controller because it processes personal data for a purpose separate from its role as processor.

3. "Does a physician in vocational healthcare qualify as controller or as processor?"

Primarily, the quality of controller is determined by whoever determines the purpose and means of processing. The relevant legal regulations (Labour Code, Decree of the Ministry of National Economy, Decree of the Minister of Health) specify not the purpose but data processing itself, according to the position of the Authority. Typically, this type of processing is among the mandatory processing operations according to Article 6(1)(c) of the General Data Protection Regulation, so the lawfulness of processing is related to the fact that it is required by legal regulation.

The legal regulations referred to make it compulsory to carry out the medical examination, but to whom the examination specifically applies, i.e. whom a particular employer employs and under what working conditions, i.e. for instance whether the person is employed in a carcinogenic working environment, is a matter for the employer to decide, and at the same time, it is the employer that specifies the purpose. According to the Authority's opinion, the employer qualifies as controller since the employer makes the decision on whom it employs and whether such examinations are necessary, i.e. who the employer sends for examinations in vocational healthcare, in other words, the employer specifies the purpose tailored to the person, and it is the employer that selects the service provider to carry out the necessary examinations. In addition, the employer processes the employees' identification data, as well as the information based on the results of the examinations, whether a person is "suitable" or "unsuitable" for the given job.

In this process, the healthcare provider will not be a processor but a controller as it independently chooses the devices used for the examination, and only it can access the health-related data, it stores them and not the employer.

4. "Can relatives obtain information by phone from the ambulance service on which institution their relative was taken to ?"

Pursuant to Section 25 of the Healthcare Act, a patient is entitled to specify the circle of persons to whom information may be given about his/her illness or its expected outcome; there is, however, an exception from this rule, as the patient's health-related data must be disclosed even in the absence of the patient's consent, if it is required by law or it is necessary for the protection of the life and limb and health of others, or to prevent further damage to the health of the patient.

In the absence of authorisation by law, the provision of information by the ambulance service on the personal and special category data of the patient concerned would require his/her written consent. At the same time, the Authority acknowledges the fair demand of interested and worried relatives to obtain information about the whereabouts of their loved ones, and in the case of emergency care, it is not realistic for the ambulance unit to obtain the written consent of the data subject for forwarding the data, while caring for the patient.

Thus, the Authority is of the opinion that if it is likely that the interested person is indeed a relative – knows exactly the name and age of the data subject – the fact of transportation and the name of the receiving institution can be disclosed on the basis of GDPR Article 6(1)(c) and Article 9(2)(c).

Providing any further information to the relative on the state of health of the patients is within the scope of authority of the specific institution, hence information on the status of the patient and a detailed description of the care provided by the ambulance service is not part of the information that may be disclosed by phone. If it is unlikely that the person is a relative, information on the institution receiving the patient cannot be provided to other interested parties, including journalists.

A satisfactory solution from the point of view of data protection and the protection of the rights of the data subjects is for the relatives to find out the name of the receiving institution by asking the ambulance service, and then the institution can inform them following the rules laid down in its own privacy policy, taking into account whether the person concerned is entitled to any further information.

5. "What information may the hospital disclose on the state of health of a patient to a relative asking by phone, if no personal data of the relative suitable for identification have been recorded in the patient's documentation beforehand (starting from the transportation of the patient)?"

The scope of the GDPR, as set out in Article 2(1), covers data processing that is automated or forms part of a filing system, including paper-based filing systems. According to the definitions in the GDPR, communication is also processing; this, however, applies to data already recorded by the controller.

If processing takes place, it must comply with other conditions, such as lawful purpose, compliance with other principles, etc., it must have a legal basis as set forth in GDPR Article 6. In addition to a legal basis, the processing of health-related data requires compliance with the conditions of lawfulness as set forth in Article 9. Pursuant to Article 9(1), the main rule is that the processing of health-related data is prohibited, except if a condition set forth in paragraph (2) is met.

Pursuant to the definition in Section 3(d) of the Health Data Act, medical confidentiality covers any health-related and personal identification data that have come to the knowledge of the controller in the course of providing treatment, and any other data related to necessary treatment, treatment in progress or completed treatment, and any data learned in relation to treatment.

Pursuant to Section 7(1) of the Health Data Act, the controller and the processor must abide by medical confidentiality , including the confidential treatment of any health-related and personal identification data that have come to their knowledge. Pursuant to Section 138(1) of the Healthcare Act, the confidentiality obligation applies not only to physicians but to all healthcare providers, covering all health-related and identification data of the patient concerned.

Pursuant to Section 138(2) of the Healthcare Act, the confidentiality obligation does not apply to the case when this has been waived by the patient, or legal regulation requires that the data be disclosed.

Pursuant to Section 7 of the Healthcare Act, patients have the right to decide during their stay in hospital who can be informed of their hospitalisation and changes in their health condition. If the patient names a person to be informed, the hospital must inform him of his hospitalisation and of any significant change in the patient's health.

There is no doubt that the corona-virus emergency poses a major challenge to the operation of health care providers; this, however, does not exempt them from their confidentiality obligation and ensuring the rights of their patients.

6. "Does the fact of participation in a screening test/examination by a specialist as use of a specific health service qualify as health-related data?"

According to the interpretation by the Authority, the fact of attending medical treatment at a specialist may itself be an indication of the health status of the data subject. Appearing at a screening test may be a less significant indication of the health status of the data subject, because the purpose of a screening test is precisely the prevention of the more serious consequences of a disease, but it may be possible to draw either accurate or inaccurate conclusions from this fact.

The second sentence of GDPR Recital (35) refers to data pertaining to clinical treatment as data carrying information on the health condition of the data subject. Data are health-related if they refer to the healthcare service used and at the same time conclusions or information can also be drawn from them as to the patient's health status (data on whether the patient has received treatment, visited a given care provider, e.g. whether he is registered with a psychiatric care provider). GDPR Recital (53) expressly refers to a health-related purpose.

A further analysis of the issue requires studying GDPR. The principle set forth in GDPR Article 5 is the principle of purpose limitation according to which data may be processed only for clear and lawful purposes. GDPR declares that health-related data as personal data requiring higher protection may be processed for health-related purposes only if these were necessary to achieve those purposes for the benefit of natural persons and society as a whole (Recital (53)).

Summarising the above, according to the position of the Authority, health-related data are processed, if the controller draws conclusions as to the state of health of the data subject from the fact that the data subject has received some form of health care.

Thus, for instance, if a shop camera records that a customer walks with crutches, it does not mean that health-related data were processed with all its aspects because merely the fact that the camera records some data related to a health condition, the purpose of processing is not to make deductions or conclusions concerning state of health.

At the same time, if the shop uses the data referring to a health condition in the camera recordings for profiling or marketing purposes – e.g. is it worthwhile to open a shop selling medical aides in the shopping centre because based on camera recordings many people with disability come here, then the data is clearly health-related data and its processing must comply with the provisions of Article 9(2).

7. "Can the purpose of processing, processing operation be separated from the purpose of the legal relationship to which it is related? (For instance, the purpose of purchase and sale is the transfer of property, the purpose of the invoice issued on the purchase and sale is the ability to verify the tax liability)?"

The same personal data may processed for several purposes, but in this case the individual processing purposes must be clearly distinguished and a separate legal basis must be independently specified for each processing purpose. The conditions under GDPR Article 13(1)-(2) and Article 14(1)-(2) must be separately presented for each processing purpose and presentation in a table format is recommended in the Privacy Statement for easier comprehension.

GDPR allows for processing for a purpose other than that for which the personal data have been collected; its detailed rules are set forth in GDPR Article 6(4). Pursuant to Article 5(1)(b) and Article 6(4) of the General Data Protection Regulation, this different use (referred to as further processing) can be lawful only, if it is compatible with the purpose for which the personal data are initially collected. The controller must take several criteria into consideration, of which GDPR Article 6(4) underlines the circumstances in a list of examples, whose consideration is regarded to be the most important.

8. "Which national regulation other than the GDPR is to be applied to websites, which are in Hungarian or which also have a Hungarian version and the centre of activities of the organisation pursuing the processing activities related to the website is in the European Union? Is it the one where the centre of activities is, or the one in the language of which the service is provided? What can be done against companies whose websites do not include any Privacy Policy or Privacy Notice?"

The Authority points out that a Privacy Policy is not identical, and hence not to be mixed up, with a Privacy Notice. Not every controller is under an obligation to produce a Privacy Policy: based on GDPR Article 24(1)-(2), the controller taking into account the nature, scope, context and purpose of processing, as well as

the risks of varying likelihood and severity for the rights and freedoms of natural persons shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this regulation. The controller shall review and update these measures as necessary. As part of these measures, and provided that it is proportionate to the specific processing activity, the controller will also apply appropriate internal data protection rules, so that in each case the controller must decide whether or not to draw up an (internal) privacy policy based on an assessment of the circumstances of the specific processing.

Contrary to the above, the controller must provide information on the processing activities carried out by it, in the manner set forth in GDPR Article 12 with the data content according to GDPR Articles 13-14. The Guidelines of the European Data Protection Board on Transparency, WP 260 rev.01[10] (hereinafter: Guidelines) recommend as good practice that every controller, which also operates a website, publish the Privacy Policy drawn up by it also on the website. Furthermore, in cases when it is possible to communicate personal data to the controller on the controller's website (e.g. sending messages, submitting orders, etc.), the Guidelines of the European Data Protection Board recommend that the Privacy Policy is made accessible on the page identical with the page used for the communication of the data[11]. According to the Guidelines, the Privacy Policy to the data subjects must be drawn up in all the languages of the target language group of the data controller, and the addressees can be inferred, for example, from country-specific preferences or the currency accepted.[12]. According to the Authority's position it follows that if there are national data protection regulations in a Member State, which go beyond the provisions of GDPR, the controller must also abide by these rules, if it offers its services also to the residents of this Member State.

As the main rule, the supervisory authority of the Member State, in the territory of competence of which the controller's main establishment is located, takes action against controllers that failed to meet their obligation to inform data subjects or did so deficiently and inadequately. Complaints related to this can be lodged with the supervisory authority, which is then transferred to the lead supervisory authority pursuant to GDPR Article 56(1).

10 https://ec.europa.eu/newsroom/article29/items/622227

11 WP 260 rev.01 Paragraph 11 in the English version (in the 'Example' in the box).

12 WP 260 rev.01 Paragraph 13 in the English version and footnote 15 thereto.

9. "According to the position of the Authority, can GDPR Article 6(2)(b) be applied in the course of the processing of special category personal data subject to the condition set forth in Article 9? This is because, according to EDPB Guidelines 2/2019 (page 8) controllers cannot do so."

It is not applicable because the guidelines referred to in the question contain the following:

21. In relation to the processing of special categories of personal data, in the guidelines on consent, WP 29 has also observed that:

Article 9(2) does not recognize "necessary for the performance of a contract" as an exception to the general prohibition to process special categories of data. Therefore controllers and Member States that deal with this situation should explore the specific exceptions in Article 9(2) subparagraph (b) to (j). Should none of the exceptions (b) to (j) apply, obtaining explicit consent in accordance with the conditions for valid consent in the GDPR remains the only possible lawful exception to process such data."

Following these Guidelines, EDPB issued new guidelines on consent under No. 5/2020, Paragraph 99 of which (page 24) repeats the above.

10."Presentation of typical cases and good practices in relation to the Privacy Policy""

It is highly important that the Privacy Policy is properly structured, particularly in the case of more complex processing operations; and that the scope of the data processed, the source of the data, the legal basis for the processing and the duration of the processing can be transparently indicated for each processing purpose.. Transparency can also be enhanced by publishing this information in a table form in the Privacy Policy, either by presenting it explicitly in this form or by including it in table form as an additional aid.

The frequent error, and one that cannot be sufficiently underlined, is that the purposes of processing must be formulated as accurately as possible. In other words:

- a real purpose must be indicated, if the data are processed for the purpose of recommending and selling products, it is inappropriate to indicate these as

data necessary for carrying out medical examinations in the given case covering these activities (see product demonstration);
- general terms, such as “are processed for marketing purposes” must be avoided, and the modes of contact, which the data subject has to expect when giving his consent must be specified in concrete terms, such as “sending advertisements by e-mail” or “recommending products through phone calls”;
- to ensure comprehensibility, the use of technical terms should be avoided in the wording of the purpose of processing as well as in the content of Privacy Policy.

Another frequent problem is also related to comprehensibility, namely many controllers repeat the text of GDPR verbatim in their Privacy Policy, although in most cases this does not provide adequate information, because legal provisions tends to be brief, concise and lean texts, the interpretation of which requires knowledge of the entire legal regulation, as well as the principles of the given area of law, which most data subjects do not have.

The Authority also highlights the frequent deficiency seen in the case of providing information of processing using cameras, namely the inadequacy of first level information. It is insufficient to merely hang an icon in front of the area under surveillance, first level information requires a warning displaying essential information on a board from which the data subject may recognise the most important circumstances of processing, namely the person of the controller, its contact data, the purpose of processing, the data subject’s rights and the accessibility of the more detailed second level information (see: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_hu.pdf)

II.1.4. Guidelines by the Authority in connection with the corona-virus and its procedures and consultations conducted due to corona-virus-related data processing

The protective measures introduced in relation to the various waives of the corona-virus pandemic and the regulatory environment changing continuously during the emergency posed a number of data protection legal challenges to controllers. The Authority received more than a hundred submissions expressly concerning the processing of personal data both from data subjects and controllers, organisations participating in the protective measures, constituting a separate group of cases. In addition, the Authority rejected a number of notifications based on their content establishing the absence of its powers and responsibility

in issues expressly related to the organisation of vaccinations and the presumed discrimination of the notifier.

1. Information on the employer’s knowledge of the fact that an employee is protected against corona-virus

The Authority has received numerous notifications from both public and private sectors organisations as employers as to whether they are entitled to process (have access to or record) data on the fact of the immunisation of employees against the new type of corona-virus (SARS-CoV-2 virus, corona-virus or COVID-19) verifiable under the provisions of Government Decree 60/2021. (II. 12.) on the verification of immunisation against corona-virus(hereinafter: Government Decree).

For this reason, on 1 April 2021, the Authority published a guidance (hereinafter: Guidance) on the accessibility of the fact of the employees’ immunisation against corona-virus by the employer in legal relationships subject to Act I of 2012 on the Labour Code (hereinafter: Labour Code) during the third wave of the pandemic. (NAIH-3903-1/2021)

The Guidance governs legal relationships subject to the Labour Code and it can only be applied to the pandemic situation existing at the time of its issue. At the same time, according to the Authority’s position, it is warranted and necessary that the legislator uniformly stipulate the requirements related to the verification of the fact of immunisation in legal relationships aimed at the performance of work (for instance in legal relationships of assignment or entrepreneurship according to Act V of 2013 on the Civil Code; employment based on sectoral legal regulations in the public sector).

The Authority expounded that pursuant to the data protection rules in force, the controller, i.e. the employer, wishing to have access to the fact of immunisation is responsible for the lawfulness of processing. The employer as controller must first determine the accurate purpose of the processing of personal data (the processing of data concerning the employees’ immunisation against corona-virus), and the legal basis substantiating the lawfulness of processing. In relation to the legal basis, the Authority notes that the fact of immunisation, i.e. either the recovery from the COVID-19 disease or the fact of vaccination, qualify as health-related data belonging to the special categories of personal data according to GDPR Article 4(15). The lawfulness of processing data requires therefore that one of the legal bases in GDPR Article 6(1) and the additional conditions set forth

in GDPR Article 9(2) – in the case affected by this Guidance's points (b), (h), or (i) – obtains as verified by the controller, in the absence of which the processing of health-related data is prohibited under GDPR Article 9(1).

Based on the joint interpretation of Articles 9(2), 10(1), 51(4) of the Labour Code and Section 54(7)(b) and (h) and Section 60(3) of Act XCIII of 1993 on Health and Safety at the Workplace, it is NAIH's position that access by the employer to the fact of immunisation of the employee against corona-virus may qualify as a necessary and proportionate measure for the purposes of labour law, health and safety at the workplace, vocational healthcare and work organisation underlining within this the risk analysis carried out based on objective criteria concerning the survey of biological exposure at the workplace jeopardizing the health and safety of employees in order to protect the life and health of the protected employee on the one hand and the other employees on the other hand, and third persons (customers) that may potentially be in contact with the employee and in relation to this, compliance with the employer's obligation. In addition, such processing by the employer also serves an epidemiological interest as a significant public interest.

The Authority underlined in the Guidance that the only purpose of processing may be for the employer to be able to take and do take the necessary measures to comply with the rules of labour law, health and safety at the workplace, vocational health care and work organisation, and to achieve this purpose be entitled to have access to the fact of the immunisation of employees against corona-virus. Here the Authority highlighted that the purpose must be real, to be verifiable by the employer (i.e., if the employer decides to request such data, it then has to take measures in possession and on the basis of them, and it will have to document these measures); also, it is an important expectation that the range of data processed must be suitable for achieving this purpose.

Processing must be designed taking into account compliance with the data protection principles, particularly the principle of accountability.

In addition to the above, the principle of data minimisation must not be overlooked, which requires that only those data can be lawfully processed, which is strictly necessary and proportionate for the achievement of the purpose.

According to the Authority's position, therefore, the employer may – within the legal framework in force – only process the data of the application and the immunisation certificate as a public deed specified in the government decree; it may not

lawfully collect and process any other data for the purpose of verifying immunisation against the corona-virus.

In terms of necessity, the Authority underlined that the employer has to carry out the survey by job or categories of employees. Thus, for instance in the case of certain low risk jobs (for instance distance work of a permanent nature) necessity can obviously not be established. At the same time, processing can be regarded as necessary, for instance if the employer's activities include the repair and maintenance of medical, technical and other devices installed in the COVID-19 wards of hospitals, and it requests verification of the fact of immunisation in the interest of the protection of employees in order that only immunised employees be sent to the location of the work. Similarly, necessity can be established also if the employer is a welfare institution where it is necessary to know (and to process the data) that the employee performing work in the institution is immunised, in order to protect the institution's residents.

In order to comply with the principle of proportionality, the employer may only request the employee to display the application or show the immunisation certificate; it may not make copies of them, it may not store them in any form and in any way and is not authorised to forward them to any third person, all that it is authorised to record is that the employee concerned has verified the fact of his immunisation against the corona-virus, and if it can be established in the course of presenting the certificate, the duration of his immunisation.

Over and above, controllers must provide for the transparency of processing, as well as the accuracy and security of the data.

2. Verification of the fact of immunity against corona-virus in theatres, as a condition of accommodation in dormitories and in baths

Numerous controllers and data subjects asked for a statement from the Authority in relation to the interpretation of the rules applicable to events specified in Government Decree 484/2020. (XI. 10.) and other events, and the lawfulness of processing related to checking the fact of immunisation against the corona-virus, particularly in the case of admission to theatres or baths.

In addition to responding to requests for consultation, the Authority issued several guidelines concerning access to the fact of immunisation against corona-virus, however the continuously changing legal environment as a result of the various

waves of protection against the corona-virus posed numerous legal challenges of data protection to controllers.

A) In its statement No. NAIH-7050-2/2021, the Authority expounded that according to the text of Government Decree 484/2020. (XI. 10.) in force from July 2021, the *"theatrical performances" referred to in the application are not included in the notion of "event" as specifically defined in legal regulation, and there are no requirements in the legal environment in force for theatrical data controllers to mandatorily verify the fact of immunisation, hence in their case, neither of the conditions of GDPR 9(2) obtain, hence they cannot lawfully call upon the data subjects to present such verification."*

Because of this, according to the position of the Authority, if a theatre would wish to have its performances included in the notion of "event" defined in Government Decree 484/2020. (XI. 10.) and make the verification of the fact of immunisation against corona-virus a precondition to admission to its performances, it must turn to the legislator with a view to amending the legal regulations.

B) Both controllers and data subjects submitted numerous notifications to the Authority concerning admission to the dormitories provided by institutions of higher education subject to the verification of the fact of immunisation against corona-virus and in view of the great interest on the part of society, the press also addressed the issue on several occasions. On 2 September 2021, the Authority published its statement *"Communiqué concerning the lawfulness of processing related to the verification of immunisation against the corona-virus as precondition to admission to dormitories of institutions of higher education"* (hereinafter: Communiqué).

The Communiqué pointed out that in its responses to the consultation requests of universities published in the summer of 2021 and also published on its website (NAIH-6148/2021. and NAIH-6298/2021.), the Authority has repeatedly clarified that the fact of immunity from corona-virus or the lack thereof constitutes health data and therefore special category data, and the conditions for the lawful processing of such personal data are defined by the General Data Protection Regulation and the supplementary domestic legislation.

Of the conditions required for the processing of health-related data according to GDPR Article 9(2), processing by dormitories may not be based on the consent of the data subject as a data subject is not in a position to give his consent voluntarily as he would suffer direct disadvantage in the absence of it. Apart from the cases related to contracts concluded with a healthcare provider according to GDPR Article 9(2)(h), the processing of health-related data requires safeguards specified in the law of the Member States or the European Union. Mandatory processing containing such safeguards can be prescribed by the express provision of EU or Member State law, while at the time of the publication of the Communiqué, there was no such legal regulation applicable to dormitory accommodation; accommodation cannot be regarded as an event, hence reference to Government Decree 484/2020. (XI. 10.) is not acceptable. According to the position of the Authority, institutes of higher education cannot lawfully request verification of the fact of immunisation against corona-virus as a condition of accommodation in a dormitory until the entry into force such safeguards and it recommended to initiate legislation on the issue, if considered as warranted.

C) On 22 December 2021, the Authority published the Communiqué on checking immunisation in the course of admission to the area of baths. According to the Authority's position taken in accordance with the conditions prevailing at the time, in the case of baths, where other common forms of protection not involving personal data processing, such as frequent ventilation or wearing masks, are unrealistic, at the same time, where the requirements for keeping a distance can only be enforced in a limited way, also in view of the spreading of the Omicron variant of the corona-virus, it may be appropriate and acceptable, as well as necessary and proportionate at the time of the publication of the Communiqué, for the operator of the bath to make admission to the bath conditional on the verification of the fact of immunisation against the corona-virus.

D) A municipality as operator asked the Authority whether the provisions of the Communiqué on baths can be applied by analogy to theatres and cinemas operated by the municipality. According to the position of the Authority, a number of modes of protection not involving personal data processing can be applied in the case of theatres, *"a bath cannot be identified as a theatre or cinema. In the case of theatres, it is possible to broadcast performances online, but a theatre cannot be compared to a bath even in the case of a performance held in the presence of an audience, not even in terms of wearing masks. The Authority sees no legal impediment to having breaks in the performance, if necessary, to allow for the replacement of masks not only at the one-and-a-half hour intervals included in the submission, but at shorter intervals, which could even be made mandatory by the theatrical or cinema controllers."* The Authority again recommended to the notifier that if it is does not agree with the interpretation enabled by the legal regulations in force, it should turn to the legislator with a view to amending the legal regulations.

3. Sending government newsletters to data subjects registered for COVID-19 vaccination

In 2021, the Authority received a number of notifications in which the notifiers complained that they received government information not only in relation to the corona-virus pandemic and protection against it to their e-mail addresses provided in the course of registration to the site: https://vakcinainfo.gov.hu/. The Authority informed the notifiers that the Privacy Statement related to registration for vaccination disclosed that by consenting to the option "I wish to remain in contact with Hungary's Government" and registration for vaccination two processing operations were implemented with different purposes.

In every case, the Authority called the attention of the complainants to the fact that in the course of online registration, it was possible to give consent to processing for the individual purposes by ticking two different boxes and the consent that could be given to additional maintenance of contact with a view to having the Prime Minister's Cabinet Office forward government newsletters was not a precondition to valid registration for vaccination against the corona-virus. If in the course of his registration, the data subject ticked off the former option, he gave his voluntary consent to the Prime Minister's Cabinet Office processing his contact data on behalf of Hungary's Government for the purpose of maintaining additional contact, asking for opinion, providing information and sending e-mails until consent was withdrawn. A data subject may exercise his right to withdraw his consent to processing for the purpose of maintaining contact and to erase his personal data processed for this processing purpose by exercising his data subject's rights with the controller (NAIH-3616/2021., NAIH-4485/2021., NAIH-4139/2021., NAIH-8634/2021.).

The investigations of the Authority launched on the same subject did not find that the relevant Privacy Statement would have used a restrictive interpretation, exclusively indicating the sending of newsletters on the corona-virus as the purpose of the intended processing, because in actual fact, it requested the consent of the data subject for the general maintenance of contact.

According to the Authority's position, if the complainant no longer wishes to receive such government newsletters and information, he is directly entitled to exercise the right to erasure (right to be forgotten) according to GDPR Article 17 vis-á-vis the controller.

4. Non-addressee use of the application form for persons entitled to retirement benefits, transmission of personal data contained therein

In a request for a statement in February 2021 (NAIH-2529/2021.), the Hungarian State Treasury (hereinafter: MÁK) asked the Authority whether MÁK is authorised to forward the personal data provided by its natural person clients, who requested the registration for vaccination against the corona-virus in informal letters to the Nemzeti Egészségbiztosítási Alapkezelő (National Health Insurance Fund Manager, NEAK) keeping the register of vaccination registrations. MÁK also asked if individuals request application forms for persons entitled to a pension, who are outside the range of addressees for these application forms as set forth in legal regulation can MÁK send application forms to such data subjects and if they return it, can it accept them and process them in a manner identical with the other application forms.

In its answer, the Authority emphasised that according to its position, registration for vaccination is acceptable only if it is implemented through the dedicated online interface, or if the person entitled to a pension indicates his request for registration by sending the form introduced by MÁK by mail.

MÁK has to process the registration requests received informally by mail or e-mail in accordance with the relevant filing rules and its own policies, but in view of the fact that they cannot be regarded as official registrations, there is no legal basis for forwarding the personal data included in them to NEAK.

The Authority also expounded that if persons other than the addressees of the application forms specified in legal regulation request such forms from MÁK, it is not possible to lawfully meet this request, because in this case MÁK *"has no legal basis either for sending the application form, or for forwarding the data of a person other than the addressees specified in legal regulation to NEAK"*

5. Immunity certificate erroneously issued to a minor

In a submission sent to the Authority in May 2021, the legal representative of a minor objected to the fact that an immunity certificate verifying the fact of vaccination was issued for his child, even though the child has not been vaccinated; at that time the Hungarian legal regulations did not allow the vaccination of people below the age of eighteen (NAIH-4949/2021.).

An investigation was launched based on the notification, in the course of which the Authority contacted the issuer of the erroneous immunity certificate, the Government Office of Budapest, the National Hospital Directorate General as the operator of the Electronic Healthcare Services Space (hereinafter: EESZT), finally the healthcare provider where the erroneous health-related data were recorded in the EESZT system.

In the course of the inquiry procedure, the healthcare provider informed the Authority that a person wishing to be vaccinated provided an erroneous TAJ (social security) number, which the healthcare provider failed to check prior to recording in EESZT. The healthcare provider erased the erroneously recorded data from the EESZT system.

The Authority drew the attention of the healthcare institution to the fact that, in accordance with the basic principle of the GDPR, i.e. the principle of accuracy, it should pay more attention to the verification of TAJ numbers in the future.

6. Making access to public education establishments and attendance at parent-teacher meetings conditional on proof of immunity from corona-virus

In the autumn of 2021, the Authority received several notifications, in which data subjects objected to the processing of data by various education institutions, as they made entry to their premises and visits to parent-teacher meetings conditional on presenting the immunity certificate (NAIH-8454/2021., NAIH-8456-2/2021., and NAIH-8485/2021.). The Authority found that the fact of immunisation against corona-virus is health-related data, which can only be processed, if in addition to a legal basis set forth in GDPR Article 6(1), the condition according to GDPR Article 9(2) also obtains for the processing.

Such a guarantee condition laid down in the law of the Member States is provided by Section 51(4)(a) of Act CXXVIII of 2011 on Disaster Prevention and the Amendment of Certain Related, according to which the Minister in charge of education may specify in a specific decision a task related to the operation of public education establishments and the organisation of the academic year in an emergency, and by the Decision 29/2021. (XI. 19.) by the Minister of Human Resources on the protective measures in public education during the period of epidemic adopted on that basis, which mandatorily requires public education establishments to check the immunity certificate (application, EU digital Covid certificate, international vaccination certificate, proof of immunisation) in the case of persons intending to enter public education establishments.

The legal basis for health-related data processing related to participation in parent-teacher meeting and other school events was created by Section 6/C(3) of Government Decree 27/2021. (I. 29.) on the promulgation of an emergency and the entry into force of emergency measures, according to which *"if an other event is held in a closed space, exclusively persons immunised against corona-virus and minors below the age of eighteen under their supervision may participate in the other events in addition to those employed there".*

The Authority stated that the above legal regulations established the appropriate legal basis for a school to lawfully request verification of the fact of immunisation for entry or participation in a parent-teacher meeting, there was no infringement, there was no imminent risk of infringement and the Authority closed the investigation.

II.1.5. Media, press and online publicity in the Authority's practice

In the Authority's consistent view, the reference to journalism as an activity in the public interest cannot be accepted as a legal basis for the processing of personal data. The rules for this specific processing are governed by GDPR Article 85, which gives Member States considerable leeway in drawing the boundaries around the right to the protection of personal data under this Regulation and the rights to the freedom of expression and information. However, the Hungarian legislator did not provide for any exceptions or exemptions from the obligations of the General Data Protection Regulation, including Article 6(1)(f), in relation to journalism. It follows from all this that all the processing related to journalism not based on consent may be carried out on the legal basis of legitimate interest according to Article 6(1)(f) of the General Data Protection Regulation. The application of this legal basis has been confirmed by final judgments of the courts reviewing a specific NAIH decision[13], and the precedent of the Curia of 2 March 2022 explicitly adopted this practice and interpretation of the law.

According to the Authority's position, when publishing articles containing personal data by press products, the interest assessment must take into account the specific features of the particular communication and specifically reflect on them. An interest assessment carried out in general disregarding the specific personal data and the characteristics of processing fails to comply with the requirements of the General Data Protection Regulation.

13 Judgements Nos 105.K.704.375/2021/6. and 104.K.701.309/2021/15 by Fővárosi Törvényszék.

Therefore, in the absence of consent by the data subject, processing by the journalist is lawful, if the interest assessment test carried out leads to the conclusion that the legitimate interest of the media or a third party enjoys priority vis-a-vis the rights of the data subject to the protection of personal data. If a public figure is involved, then the interest assessment has to have, inter alia, a clear reference to this and the extent to which the processing is related to the public discussion of a public affair. In these cases, therefore, the central issue is the analysis of the applicability of the notions of "public affair" and "public figure" in accordance with the facts. As in most cases, data subjects initiate a authority procedure for data protection with reference to a breach of their privacy, the formalised framework of the procedure creates a sound basis for doing so.

1. Publication of photos and videos

The article complained against was about a topical issue of public life at the time of publication, the use of the public funds spent on vaccine and ventilator procurement in relation to combating the corona-virus epidemic and the exploration of the circles of interest linked to the procurements. In view of this, they named the person of the Petitioner and used the photo showing him to illustrate the article. Based on the data available on public websites, the presentation of the complainant and the article complained against, the Authority found that because of the complainant's profession, his activities in the pharmaceutical industry and his positions in the state hierarchy, he has been a public figure until the recent past, while currently he is the head of one of the largest media corporations of Hungary, thus according to the Authority's position, it follows from Constitutional Court Decision 3145/2018. (V. 7.) AB, that he is a public figure even at present. The photo used is accessible in the MTI photo bank without restriction. According to the decision of the Authority, the name and the photo used in the article complained against qualify as personal data accessible on the grounds of public interest in accordance with Section 26(2) of the Privacy Act, which can be used without the consent of the public figure who is the data subject in the current article related to the use of public funds. *(NAIH-4807/2021)*

In another case, the yellow press harassed a former public figure, who had officially retired from public life, against his express wish, in his private home, during his household activities, photographed him and published these data, in such a way that the published article was only meant to satisfy the idle curiosity of the public and could not be associated with the discussion of any public affair at all. By imposing a large fine, the Authority aims to preventively set limits to *"paparazzo"* journalism that severely violates privacy. *(NAIH-6952/2021)*

The Authority reprimanded a local internet news portal for similar reasons when it reported on the car accident of a former sports star giving his name and the number of his license plate. According to the position of the Authority, the fact that he was party to an accident was not related to public affairs, it had nothing to do with the public activities of the sportsman, i.e. his professional past or current public activities. Although the article mentioned the sportsman's achievements and his activity as a specialist commentator, its primary content and main statement was that a celebrity crashed a car. A substantial part of the content was about the person of the complainant and was meant primarily to satisfy the public's hunger for gossip and not information on the accident. The fact in itself that a news portal reports on an accident may command public interest, but the related report can fulfil its goal, even without publishing personal data. *(NAIH-3119/2021)*

2. Data processing in schools

A highly important statement was made concerning the processing of personal data of children by public education establishments. In the case complained against, a school video recording was made of the performance of a group of children, which was then uploaded to an "unlisted" institutional channel established on a video sharing portal, then the video's access route was electronically sent to all the parents in a legal relationship with the establishment and the link was made accessible to anyone in the establishment's own website. According to the Authority's position, the video recording of children and its publication through the school website and the video sharing portal qualify as separate processing operations, hence specific parent consent based on the appropriate information is necessary in the case of every processing. With regard to the data processing by the establishment recording the activities of the children, the Authority underlines: it is of the utmost importance that the controller public education establishment should consciously consider the range of activities and events planned for the given academic year, involving data processing, as in this way it is able to bear in mind not only the interest of individuals, but also that of the community and the interest of all the children. In the course of the operation of public education institutions, the institutional events indicated in the schedule for the academic year necessarily concomitant with the processing of personal data are increasingly recorded in the public scene on the Internet. There is no doubt that the establishments are able to present the results of the work carried out by them through the individual and community actions of the children, of which events photo and video recordings are frequently made. The Authority also notes that during the pandemic, the difficulties in maintaining direct contact reinforced the

application of alternative means and possibilities of communication. In this case, the video recording was made of a Christmas play and the purpose of sharing the recording was to let the families connected to the establishment see the performance of the children, the Christmas welcoming address in line with tradition.

In several cases, the Authority encounters a common practice in Hungarian public education, whereby the controller institutions request the legal representatives of the minor children to give their general consent to data processing at the beginning of each academic year (generally at the first parents meeting). This practice, however, does not exempt educational institutions from the obligation of providing detailed information to the legal representatives (parents) on the processing operations related to events necessarily concomitant with the processing of the personal data of the children taking place in the course of the academic year, emphasising the possibility of withdrawing consent, whose exercise they must ensure easily without impediment. In the case of sharing recordings of children with the unlimited public of the Internet, it is no longer sufficient to ensure the exercise of the right to object for parents and legal representatives – which is guaranteed in any case – here an active decision-making position must be guaranteed for the parents because of the unlimited access by anyone to the data of their underage children, it is why in such cases of processing obtaining an informed consent in writing and in advance is necessary. In the case of a video recording of a show or performance requiring the participation of one or more children, or specifically of a group of children, the video recording can be made by assessing the parents' intentions from the very beginning, so as to enable the lawful recording of the performance of children whose parents consent to the recording and its eventual sharing. Careful design can ensure that the children of parents who do not consent to the recording can also act appropriately in the programme, because it is not in the interest of the children, if they are left out of their community performance for reasons of data protection .*(NAIH-4822/2021)*

3. The right to be forgotten

Similarly to other data subject rights, the right to erasure set forth in GDPR Article 17 is not absolute, hence it can be subject to the restrictions with appropriate guarantees. Compliance with an unfounded or excessive request can be rejected, and EU or national law may also include restrictions; also, the General Data Protection Regulation specifies certain case types when the obligation to erase does not prevail: continued processing may be regarded as lawful, if it is necessary for the exercise of the fundamental rights and freedoms of others. One of them is the freedom of expression and the right to be informed.

A widow turned to the Authority because the data of the already terminated undertaking of her deceased husband, including the phone number of the undertaking, which is at the same time the home phone number of the notifier herself, are accessible in a Google application. The widow approached Google first, but her request to erase the phone number was rejected on the grounds that the display of the data was warranted by the overriding interest of the public in the accessibility of the data. The Authority successfully called upon the controller to remove the phone number from its platforms because the undertaking in question has already ceased to function, thus there was no public interest whatsoever in the accessibility of the data. *(NAIH-7037/2021)*

In another case, the notifier requested the Authority to order Google to erase the 7 links indicated by him from among the hits for his name because the content accessible through the links were no longer up to date, he had terminated his activity as a performing artist, moreover it was in conflict with his current office work, it had unpleasant consequences for him, moreover he had never given his consent to sharing the recordings. According to the Authority's position, none of the Internet sources indicated contains offensive data that would have a detrimental impact on the notifier's reputation or employment relationship. When the data subject participated in public events where he acted as a performing artist, he became party to cultural public life and had to reckon with the fact that video and audio recordings would be made accessible to a wider public. The current employment relationship of the notifier does not justify the erasure of the content, there are no conflict of interest requirements in this respect, thus the Authority accepted Google's negative response to the request for erasure *(NAIH-4647/2021)*

4. Social media

In addition to natural persons, an increasing number of people discharging public duties use the various platforms of social media for expressing their opinions and to make their views widely known in the context of their public responsibilities.

The Authority conducted an investigation into a case involving the mayors of a joint local government and its former and current municipal executives, when their documents were published on the Internet without the consent of the data subjects, which – according to the complaint – made offensive comments related to the office of the data subjects as well as decision-support documents and other public data not accessible on the grounds of public interest accessible to anyone. In general, it can be stated that criticism related to the position of a mayor

and its disclosure to the public must be tolerated by the person exercising public power. At the same time, decision-support documents containing personal data may become accessible only with the consent of the data subject. *(NAIH-5465/2021., NAIH-5466/2021)*

Social media was used also by a parent to try and find his minor child not under his supervision. In these posts, in addition to a photo of his child, the personal data of professionals discharging child protection duties were also disclosed. To remedy an infringement implemented by the disclosure, the legal representative of the underage child has to take action to exercise the data subject's rights: first, he has to contact the posting controller and if this is not successful, then the intermediary service provider providing the Internet platform. In addition, Section 13(13) of Act CVIII of 2001 on certain issues of electronic commercial services and services related to the information society provides an opportunity for having data content in breach of the personality rights of minor children removed. *(NAIH-5483/2021)*

Following a successful investigation, an Internet news portal removed the missing person's wanted post from its newsfeed after the original purpose of finding the missing person had been achieved *(NAIH-5727/2021)* Based on a complaint, the Authority investigated a mayor's order regulating the managing directors of businesses fully held by the municipality, representing them before the press and the media and making statements and communications in any public forum. Since the majority of the fora that shape public opinion are the press and the social media platforms, and the authorisation of a statement or comment in writing, as required by the order, is a time-consuming process, the businesses concerned are unable to fully meet their obligation according to Section 32 of the Privacy Act to provide accurate and prompt information, which may violate the enforcement of the fundamental right to the freedom of information. Prior to the Authority's procedure, the Commissioner of Fundamental Rights also conducted an investigation, as a result of which an infringement of the fundamental right to the free expression of opinion was found. *(NAIH-2845/2021)*

Several submissions were received concerning the media interfaces created by entities and persons discharging public tasks on social portals for the purposes of communication: the possibilities of complainants to comment and to express their opinions were restricted in several cases without justification on the official sites and public groups complained about. The Authority does not have jurisdiction to evaluate these complaints. *(NAIH-8722/2021)*

II.2. Processing personal data subject to the Privacy Act: procedures related to the processing of personal data for the purposes of law enforcement, defence and national security

II.2.1. Investigation of the "Pegasus" spyware in Hungary

Based on Section 51/A(1) of the Privacy Act, the Authority launched an ex officio investigation into the use of the Pegasus spyware in Hungary, once news appeared in the press according to which the software of an Israeli company called NSO suitable for tracking smartphones was alleged to be unlawfully deployed against Hungarian target persons. It was reported that an international group of investigative journalists, together with the human rights organisation Amnesty International, obtained access to a database containing the phone numbers of 50,000 target persons related to the activities of NSO clients which, according to the article on the Direkt36 investigative portal, included the personal data of 300 Hungarian citizens. According to the fact-finding article, the circumstances indicated that Hungarian authorities used the spyware against targets in Hungary, in their view, unlawfully for the surveillance of journalists, human rights advocates, opposition politicians, lawyers and businessmen.

The Authority was responsible to investigate whether in the course of applying the means and methods according to Section 56 of Act CXXV of 1995 (hereinafter: the National Security Services Act), data processing by the bodies authorised to gather intelligence secretly by the minister in charge of justice affairs operates in compliance with legal regulations and whether intelligence was secretly gathered in the case of the persons made public and, if so, whether it was done lawfully.

The Authority first requested statistical reports from the Specialised National Security Service supplying the means and methods according to Section 56 of the National Security Services Act, then requested the transfer of the file and authorisation numbers of all the cases related to the use of the tool from the ordering bodies (controllers). The Authority checked all the files and documentation on the file list, compiled from the file and authorisation numbers received from the ordering bodies, during on-site inspections at each national security body (data controller). Using the list of disclosed persons and the list of case numbers sorted by sampling, the Authority examined the conformity of a total of nearly 100 submissions and related decisions of the minister of justice during the pro-

cedure. The Authority also contacted the International Secretariat of Amnesty International and requested that it provide the Authority with a list of the personal details and telephone numbers of the allegedly Hungarian data subjects concerned, based on information published in the press in connection with the investigation.

The Authority examined whether the legal conditions concerning the secret gathering of intelligence prevailed. When investigating the lawfulness of external authorisation, the Authority examined whether there was adequate verification of the fact in the submission that the secret gathering of intelligence was necessary for national security interests. So, the Authority's investigation therefore extended to the existence and the nature of the interest of national security. Section 74(a) of the National Security Services Act defines the interpretation of "interest of national security"; by comparison with the given facts of the case, it can be established or excluded whether interest of national security obtains.

As the Authority may examine with regard to every data processing operation whether it restricts the right of the data subjects to informational self-determination to the necessary and proportionate extent, therefore, even where the interest of national security is invoked, it must be examined whether the enforcement of the interest of national security in the given case restricts the right of the data subjects concerned to informational self-determination and the right to privacy to a necessary and proportionate extent by the secret information gathering.

The Authority also examined whether there was sufficient verification in the submission concerning the external authorisation of the secret information gathering that the purpose of data processing cannot be achieved without it and whether the use of the means and method requested by it was necessary. The submission is also to verify whether the secret information gathering is indispensably necessary for the requested period, and the Authority examined whether the authorisation was requested for a maximum of ninety days or, if the period of the secret information gathering was extended by another ninety days, it was done via a new submission and justification as required by law.

The Authority was also responsible for examining whether the decision of the minister in charge of justice affairs causally follows from the facts set forth in the submission. The minister adopts the decision on whether to approve the submission or reject it in case it is unfounded within 72 hours from its receipt. So, the Authority examined not only the formal and procedural requirements of the submission, but also the decisions made by the minister in charge of justice affairs on the individual submissions.

It is important to examine in the case of every decision whether the minister in charge of justice affairs justifies the granting of the external authorisation in view of the facts and circumstances detailed in the given submission. The authorisation by the minister in charge of justice affairs must include detailed justification enabling the Authority to examine the facts and circumstances taken into account in the course of the decision-making, as well as the compliance of the content of the decision on the occasion of the Authority's subsequent control.

It is important to note that Section 58(2) of the National Security Services Act expressly refers the powers of authorisation to the powers of the minister in charge of justice affairs and does not authorise the transfer of the authorisation powers.

As the minister in charge of justice affairs had previously stated that *"the authorisations are outsourced, they are signed by the state secretary, it is Pál Völner, the state secretary, who grants or refuses authorisations"*, the Authority contacted Dr Pál Völner, state secretary of the Ministry of Justice, in relation to the decisions of the Ministry of Justice under investigation. The state secretary stated in his response that *"in the case of the authorisation of the file numbers listed in the request of the Authority, the authorisations were signed within the powers of substitution because the minister was held up elsewhere"*.

A public summary of the Authority's investigation has been produced, which includes the Authority's findings. However, before examining the findings one by one, it is important to state with respect to the conditions of using the secret gathering of information subject to external authorisation that the Hungarian law in force does not differentiate by vocations or professional activities, i.e. it does not restrict the authorisation of the National Security Services to carry out the activities under Section 56 of the National Security Services Act for any profession (e.g. "journalist, human rights activist, opposition politician, lawyer and businessman").

In the course of the Authority's investigation, no information was found that the bodies authorised to secretly gather information subject to external authorisation according to Section 56 of the National Security Services Act would have used the spyware for any purpose other than those specified by the manufacturer (prevention and detection of criminal acts and acts of terrorism) and the discharge of the duties specified by law. Based on the data made available to

the Authority, it can be established that in Hungary, the Specialised National Security Service used the tool constituting the subject matter of the investigation. The task of the Specialised National Security Service specified by law is to support the work of organisations authorised to use the tools and methods of covert information gathering and covert tools, by way of providing special services. In the cases under investigation, the Authority did not find unlawfulness with regard to the data processing by the controllers (ordering bodies).

In the course of its investigation, the International Secretariat of Amnesty International did not make available to the Authority the list containing the 300 phone numbers referred to in the news, so the Authority was not in a position to ascertain its existence or the range of data subjects mentioned in it in the course of its investigation. It follows that in the course of its investigation, the Authority carried out procedural acts in relation to those data subjects whose being affected by the use of the software was made public in the press. It can be established on the basis of the data of the investigation that secret gathering of information subject to authorisation by the court or the minister in charge of justice affairs according to Section 56 of the National Security Services Act was carried out with respect to several of the persons identified as being subjects of the use of the "Pegasus" spyware in the press.

Regrettably, the investigation was inconclusive as to how the telephone numbers linked to Hungarian persons, which Amnesty International's Security Lab unit found to have been infected by the spyware, could have been disclosed in the course of the so-called Pegasus Project fact-finding investigation, and the Authority was unable to prove beyond reasonable doubt or rule out the possibility that a data breach had occurred at the controllers subject to its investigation. As the perpetration of criminal acts cannot be excluded, so the Authority was initiating the launching of a criminal procedure pursuant to Section 70(1) of the Privacy Act at the investigative authority. *(NAIH-6583/2021.)*

II.2.2. Procedure by the National Security Service in connection with requests to exercise the right of access

In its data protection procedure launched upon request, the Authority investigated the lawfulness of the procedural practice of a national security service (hereinafter: controller) related to requests for the enforcement of the right to access.

The petitioner requested information from the controller based on Sections 14(b) and 17(1)-(2) of the Privacy Act about whether his personal data are processed

by the controller itself, or a processor acting on its behalf or its order, and he asked that the information related to the processing of the data be made available to him. In its response, the controller told the petitioner in relation to the processing of personal data that it was not engaged in unlawful processing.

In its response sent to the Authority, the controller underlined that according to its position even the refusal of granting the request according to the Privacy Act provides additional information on the fact that the controller was actually processing data in relation to the petitioner. Furthermore, according to its interpretation, only an answer given in full compliance of the controller's obligation detailed in Section 17(2) of the Privacy Act can be considered as exclusively lawful information, i.e. the controller must provide information to the petitioner on the fact of processing and other related information. Having considered the circumstances, the controller decided in the present case that it did not wish to inform the petitioner even of the fact of processing, hence it refused to grant the request without reference to the relevant provisions of the Privacy Act.

The Authority disagreed with the controller's practice of providing information and the justification set forth in its response. Under the legal regulations referred to, the controller truly has the powers to restrict or deny the granting of requests aimed at the enforcement of the right to access for ensuring national security interests provided that conditions set forth in law obtain. Under Section 17(4) of the Privacy Act, in the event of the restriction or denial of a request aimed at the enforcement of the right to access, the controller may even waive and information containing legal and factual reasons for denial to ensure national security interests.

However, even when refusing to grant requests aimed at the enforcement of the right to access for the purpose of ensuring national security interests, Article I(3) of the Fundamental Law must still be taken into account, which means that the data subject's right to access may be restricted only to the extent strictly necessary and proportionate to the purpose to be achieved, respecting its essential content.

Based on the practice of the Constitutional Court, any legal regulation that provides for the processing of personal data has to contain safeguards, so that the data subject is able to trace the route of the data in the course of processing and to enforce his rights. The underlying legal instruments should therefore ensure that the data subject gives his consent to the processing, or they should contain accurate safeguards for the exceptional cases when processing may take place

without the data subject's consent and eventual knowledge. These legal safeguards should limit the flow of data, also for the sake of controllability.[14] Since the processing of data by national security services is typically carried out without the consent or knowledge of the data subject, the legal safeguards guaranteeing the protection of personal data are of particular importance. Such a legal safeguard is provided by the provisions of Section 17 of the Privacy Act, which sets forth the rules of granting, restricting or denying requests for the enforcement of the right to access.

According to the position of the Authority, under the provisions of the Privacy Act, the rights of the controller guaranteed in the Privacy Act extends not only to the denial of information on the personal data processed – if the conditions set forth in law exist – but also to restrict the content of the response specified in detail in Section 17(2) of the Privacy Act – provided that it is strictly necessary for ensuring an interest specified in Section 16(3)(a)-(f) of the Privacy Act and to grant the data subject's request only with respect to some of its elements restricting the enforcement of the data subject's right to access. Therefore, not only the answer given in the case of full compliance with the controller's obligation detailed in Section 17(2) of the Privacy Act can be considered as exclusively lawful information.

The scope of the Privacy Act also extends to processing for the purposes of national security; hence the controller must apply the relevant provisions of the Privacy Act when responding to requests to enforce the right to access. The restriction or denial to grant requests for the enforcement of the right to access restricts the right to the protection of personal data as a fundamental right. The controller's practice to provide information disregarded the legal safeguards ensuring the protection of personal data in the Privacy Act, hence it disrespected the essential content of a fundamental right.

The Authority found that the response of the controller to the petitioner's request to enforce his right to access fails to meet the legal provision set forth in Section 17 of the Privacy Act concerning the provision of information or its restriction or denial to the petitioner, which must function as a legal safeguard ensuring the protection of personal data.

In the course of the procedure, the controller was found to have violated the petitioner's right to access under Section 14(b) of the Privacy Act, as well as its

14 Decision 2/2014. (I.21.) AB

Section 17, as it did not respond to the petitioner's request to enforce his right to access in accordance with the provisions of the Privacy Act. Because of this, the Authority ordered the controller to meet the petitioner's request for access in accordance with Section 17 of the Privacy Act, or to notify him on the restriction or denial to grant the request in accordance with the Privacy Act. The controller took note of the decision and implemented it. *(NAIH-433-2021)*

II.2.3. Deployment of a camera system with facial recognition technology for public area surveillance

The Authority learned from news in the press that the Municipality of the City of Siófok intended to install a camera system of 39 cameras with artificial intelligence capable of facial recognition on the Petőfi Promenade in Siófok to monitor the public area. As the operation of systems capable of facial recognition raises numerous data protection concerns, the Authority launched an investigation in the case.

According to the facts of the case explored in the course of the investigation, a camera system has been in operation in Siófok in public areas since 2014, which they began to develop further in 2020. From 15 June 2021, newly procured cameras equipped with a facial recognition function were installed and their operation was tested too, although the test mode did not extend to facial recognition.

The Municipality of the City of Siófok justified the use of artificial intelligence by the fact that during the summer season, and especially on weekends, a great many people – several thousands of them – visit the nightclubs on Petőfi Promenade in the evenings. This involves a drastic increase in the number of criminal acts and misdemeanours. The prevention and detection of criminal acts and misdemeanours would become more successful using the camera system using artificial intelligence. According to their arguments, the fact that a perpetrator disappears in the crowd of people is a regular problem for the investigative authority, which could be avoided using the new technology. Reviewing the camera recordings takes a tremendous amount of time, while this time could be shortened using artificial intelligence.

The Authority deemed that the case constituting the subject matter of the investigation could not be clarified under such an inquiry procedure, hence it was closed and the authority launched an ex officio procedure against the Municipality of the City of Siófok. On 26 August 2021, the Authority's staff held an on-site inspection at the seat of the Municipality of the City of Siófok and in the camera cham-

ber of the City Guard and the Siófok Police. Based on the data obtained in the Authority's data protection procedure, it was established excluding any doubt that the Municipality of the City of Siófok does not qualify as controller or joint controller or even processor. In view of the above, the Authority terminated its data protection procedure conducted with the Municipality of the City of Siófok being concerned as client and launched its data protection procedure against the Siófok Joint Municipal Office and the Siófok Police, in which it used the documents of the preceding procedure. Based on the data and statements obtained in the course of its procedure, it was established that Techno-Tel Távközlési és Informatikai, Kivitelező és Szolgáltató Kft. also participated in the processing operations as processor, hence the Authority included them as well in the procedure as client.

Based on the clients' statements and the data obtained from the camera system at the time of the on-site inspection, the Authority arrived at the conclusion in its procedure that the clients had not used artificial intelligence capable of facial recognition until the date of the on-site inspection. At the same time, the Authority called the attention of the clients to fact that the legal regulations in force do not allow the operation of any public area surveillance system processing biometric data in Hungary.

The Authority established that the Siófok Joint Municipal Office and the Siófok Police qualify as joint controllers. The Police participated in bringing the decision on the expansion of the camera system by collaborating in the choice of the devices to be procured, i.e. in making the decision concerning the means of processing. On the other hand, it carries out specific processing operations through surveillance taking place in the camera chamber operated at its own headquarters. Nevertheless, there was no agreement between the parties, which would settle the tasks and responsibilities related to meeting the obligations of a controller, including the issues of operation, data security, exercise of data subjects' rights, keeping records and managing data breaches.

The Authority found that the obligation set forth in Section 25/F(4) of the Privacy Act, according to which the data recorded in the controllers' and the processors' records and in electronic logs must be retained for ten years after the erasure of the processed data was not met, because the activities of the users can only be viewed for 30 days. This unlawful practice, in violation of the principle of accountability, has resulted in the impossibility for the Authority to audit processing with regard to the fact that the activities of the clients was not documented, and

therefore neither that the activities, nor the statements of the clients can be audited in accordance with the law.

In the course of the procedure, the Authority fund that an employee of the processor infringed a provision of the Privacy Act, according to which the processor may carry out its activities exclusively on the basis of the written instructions of the controller through modifying, deleting and creating roles without the knowledge and instructions of the controllers between the completion of the on-site inspection by the Authority at the seat of the Siófok Joint Municipal Office and the commencement of the on-site inspection at the headquarters of the Siófok Police. In view of all the circumstances of the case, the Authority decided to impose a fine on the processor in order to protect personal data in the future, and therefore ordered the processor to pay a data protection fine of 500,000 forints, for its unlawful activities in the processing system. *(NAIH-6212/2021.)*

II.2.4. Practice for responding to requests for the exercise of the right of access

The petitioner submitted a petition to the Police (hereinafter: controller) related to the exercise of data subject's rights based on Section 14(a) and (b) of the Privacy Act- In his complaint lodged with the Authority, he objected to the fact that the controller first informed him that the Operative Services Division of the Department for Personal Register and Administration of the Ministry of the Interior was authorised to respond to his petition, and that he did not get the information concerning the personal data processed by the controller and the information related to them within the period specified in Section 15(1)(b) of the Privacy Act.

Upon request, the Operative Services Division of the Department for Personal Register and Administration of the Ministry of the Interior may provide information to citizens from the register of data reported pursuant to Section 31 of Act LXVI of 1992 on the Register of the Personal Data and Addresses of Citizens, in its capacity as the manager of various registers, about the data reported on them. However, information from the register of data reported does not necessarily coincide with the personal data processed by the controller and in terms of its content, it does not exhaust the range of personal data processed by the controller on the data subject and the information related to their processing. The Police headquarters as controller is not exempted from the obligation to provide information by the fact that the Operative Services Division of the Department

for Personal Register and Administration of the Ministry of the Interior may also be requested to provide information on certain personal data.

In the course of the procedure, the Authority found that at first the controller provided erroneous and misleading information to the petitioner when communicating that the Operative Services Division of the Department for Personal Register and Administration of the Ministry of the Interior is authorised to provide information on the processing of the petitioner's personal data. It was only later that the controller realised – on the basis of the petitioner1s response – that the petition related only to the exercise of the data subject's rights related to the data processed by the controller.

The Authority also examined the information provided by the controller to the petitioner on the processing of his personal data and found that the controller failed to provide comprehensive information to the petitioner on the data processed by it, because its response did not include the general reference to the personal data which the controller processes in relation to the specific misdemeanour.

According to the position of the controller, it met the petitioner's request for the exercise of the data subject's rights within the period specified by the law, as the period open for meeting the request begins with accommodating the call to supplement the petition. Pursuant to Section 15(1)(b) of the Privacy Act, the controller has to deal with the petition within the shortest possible time from its submission, but not later than twenty-five days. In other words, it is the date of submission of the petition, and not the date of accommodating the request to supplement the petition that is relevant for calculating the time allowed by law to deal with the petition.

The Authority established the infringement of the provisions of Section 15(1)(b) and Section 17(2)(c) of the Privacy Act as the controller failed to meet the petitioner's request to exercise his data subject's rights within the period open for this as specified by the law and the information provided by the controller to the petitioner was not comprehensive, there was no reference to the personal data processed in relation to the given misdemeanour among the personal data processed.

Based on Section 61(1)(bf) of the Privacy Act, the Authority ordered the controller to supplement the information provided to the petitioner with the reference to the personal data processed in relation to the given misdemeanour. In accordance with the decision, the controller provided the supplementary information. *(NAIH-1014/2021)*

II.2.5. Fulfilling the obligation to provide prior information by acting Public Area Surveillance officers

In his petition, the petitioner stated that he was driving his car when the staff members of the Public Area Surveillance (hereinafter: controller) stopped him and initiated action against him because of turning left irregularly. In the course of their action, a photo was also taken, which he found excessive and, furthermore, he objected to not being informed of making the photo, and thus he had no opportunity to exercise his data subject's rights. In addition, he also had concerns about the compliance of the controller with data security measures, and he had several questions in relation to the privacy policy of the controller regarding the details of processing, to which he did not receive any satisfactory answer until the submission of his petition.

In the course of that action, 2 photos were made, which the controller forwarded to the competent Police Department in order to conduct an infringement misdemeanour procedure. The petitioner cannot be recognised from the photographs, but his car concerned in the misdemeanour could be identified unambiguously, which in relation to the measures taken against him corresponds to the notion of information on the data subject, i.e. it qualifies as personal data under Section 3(2) of the Privacy Act. The photos are suitable for providing evidence on the circumstances of the measures taken by the Public Area Surveillance officers, and to some extent also on the scene of the misdemeanour and the vehicle as the means of perpetration. Section 7(2) of Act LXIII of 1999 on the Public Area Surveillance (hereinafter: Public Area Surveillance Act) provides separate authorisation to the controller for making photos.

The Authority found that the public area surveillance officers acted lawfully when they made photos of the scene, the circumstances and the object essential from the viewpoint of the measures taken. However, information on the photos was omitted from the document entitled "Information on the imposition of an administrative fine" because the section concerning the technical means recording the evidence that support the facts of the case, its description and identification data was not filled in. Information on the matters listed in Section 16 of the Privacy Act was also missing, which means that the controller's procedure did not comply with the provisions of Section 16(1) and (2) of the Privacy Act.

In the course of its investigation, the Authority established that the controller failed to properly fulfil its obligation to provide prior information in accordance with Section 16 of the Privacy Act to the data subject, and inappropriate legal references were included in its Privacy Statement.

The Authority also examined the data security provisions in force at the controller. From the responses of the controller, the Authority noted that recordings verifying the measures taken by public area surveillance officers are saved on a separate technical device and they are uploaded to the server of the controller at the end of their scheduled duty. The technical device is continuously under the supervision of the officers, so unauthorised persons cannot have access to it. After the backup, no recording remains on the technical device as all data are transferred to the server. Only a restricted number of persons, including the head of the institution, his deputy and the supervisor in charge of customer service are authorised to access the data stored on the server. Their access is password protected. The physical security of the personal data subject to the procedure is also ensured. The Authority found that the data security measures applied by the controller are adequate in terms of Section 25/I(1) of the Privacy Act and Section 7/A(1) of the Public Area Surveillance Act.

Pursuant to Section 56(1) of the Privacy Act, the Authority called upon the controller to provide information in the future on the personal data processed by the public area surveillance authority in the course of the measures taken, as well as on the recordings containing personal data for those concerned by the measures taken; to refer to the Privacy Act by correcting the reference to the legal regulation mentioned as the legal basis of processing in the documents concerning its processing operations for the purpose of protecting public order, and to delete the data subject's right to object from the list of the rights to which data subjects are entitled.

The controller notified the Authority that it agreed with the Authority's call and it took the necessary measures. It sent the corrected document (Data protection and data security information on the use of body cameras, Data protection and data security information on the processing of personal data) to the Authority and it is taking measures to publish these documents on its websites and for the prior information to be provided to the data subjects in the future.

The Authority established that its call was fully complied with and no circumstances arose that would justify the continuation of the investigation, hence the

Authority terminated the investigation pursuant to Section 53(5)(b) of the Privacy Act. *(NAIH-89/2021)*

II.2.6. Surveillance cameras operated by the Municipality of Sáránd

Based on a notification, the Authority launched an investigation concerning surveillance cameras installed in Petőfi Park in Sáránd. According to the notification, the rules concerning the operation of the surveillance cameras was adopted a few weeks after the installation of the cameras and the content of the rules was not published, hence the data subjects could not have access to it, while the images streamed by the camera could be followed on a screen located in a cupboard in the mayor's office. According to the notifier, the camera by virtue of its location could be suitable for observing the voters of the municipal election of 13 October 2019.

In the course of its investigation, the Authority found that the operation of the surveillance cameras by the Municipality of Sáránd did indeed result in an infringement of the exercise of the rights stipulated in the Privacy Act. The surveillance cameras operated without a decision by the body of representatives, meaning unlawful operation between 21 September and 5 November 2019 and their live stream could be continuously followed from the Mayor's Office. At the same time, the Authority established that this unlawful situation no longer existed at the time of the investigation and there was nothing to indicate that the voters of the municipal election would have been monitored. The Municipality published the information on the location of the cameras and the area under surveillance as required by Section 7(4) of the Public Area Surveillance Act on its website. In addition, the Authority found that the post on the Facebook page of the Municipality of Sáránd was accompanied by an image, which was a surveillance camera image, and thus access to the image and its publication on the social media site as processing did not have a lawful purpose. With regard to the rules of data processing, it was found that it was not fully in compliance with the requirements of the Public Area Surveillance Act, and even contained provisions expressly contrary to that Act.

Based on all this, the Authority called upon the municipal executive of Sáránd to remove the image associated with the post on Facebook on 20 March 2020 and to amend the Rules of Data Processing in accordance with the requirements of the Public Area Surveillance Act. As the municipal executive complied with this, the Authority terminated the investigation. *(NAIH-5296/2021.)*

II.2.7. Public surveillance by a camera on board of a municipality vehicle in Tatabánya

The Authority received a notification, according to which a municipality was continuously making camera recordings from a parked vehicle, presumably with a view to protecting a traffic board that had earlier been damaged. According to the notifier, although there was a sheet of paper with the inscription “Area under camera surveillance” visible behind the windscreen of the vehicle, it could be seen only when stepping close to the car. The controller did not produce any information on the most important aspects of processing, such as the purpose of surveillance, its legal basis and the period of retaining the recordings.

In the course of the Authority’s investigations, it was found that the municipality’s public area surveillance unit processed the data on the basis of the provisions of the Public Area Surveillance Act. The authorisation set forth in Section 7(3) of the Public Area Surveillance Act – the surveillance authority may install cameras and make recordings in public areas for the purposes of public security or crime prevention in a manner that is obviously perceptible to anyone; decision on the placement of the camera and the designation of the public area under surveillance by the camera is made by the body of representatives upon the submission of the surveillance authority – does not exclude the possibility of surveillance by camera from a vehicle, but information must be provided of this on the website.

The warning about the use of the camera as an indication of the fact of data processing is part of the exercise of the right to prior information, which should be closely linked to the Privacy Statement accessible on the website. All these together guarantee the exercise of data subject’s rights as the warning assists in making the data subjects aware that processing was taking place in the given area, of the details of which information can be found on the website.

The Authority has required the controller to provide the vehicle with clear and prominent signs (e.g. pictograms) and information (e.g. link to the Privacy Statement) on all sides of the vehicle, – while retaining the information sheet currently placed in the vehicle, which ensures the right of the data subjects to be informed. In the course of its investigation, the Authority pointed out that the Privacy Statement wrongly included that prior information is given upon request because in this way this right of the data subjects could never be exercised. The

Authority also called upon the controller to show the name and contact data of the data protection officer as an element of content of the prior information in its Privacy Statement.

The controller acted in accordance with the call of the Authority and took the necessary actions, which is verified by documents. *(NAIH-486/2021.)*

II.2.8. Disclosure of the identity of the reporting person and of data generated in the course of criminal proceedings to unauthorised persons

The Authority received a notification in relation to criminal procedures conducted by a police department, according to which the documents generated in the course of the investigation, including the personal data listed in them, have become accessible to unauthorized persons.

In terms of the powers of the Authority, the notification contained that the investigative documents of a criminal procedure launched by a police department (hereinafter: controller) were unlawfully accessed by unauthorized persons. To substantiate all this, the notification contained an e-mail, which the injured parties received from another person. The letter included a reference to the person whose report started of the investigation, but the author of the e-mail could not have lawfully accessed these personal data in a criminal case. By considering the data obtained in the course of its investigation, the Authority arrived at the conclusion that the police officers collecting the data informed a person staying at the crime scene of who reported it.

Furthermore, according to the notification in another criminal procedure, the person in charge of the case made statements by witnesses unlawfully available to the injured parties, and the content of the submission of the injured party to the witnesses, sharing personal data unlawfully. In this respect, however, the Authority did not note any infringement of the data protection regulations as the persons concerned in a criminal procedure had access to the personal data based on the rights they had in the course of a criminal procedure.

The controller conducted an internal investigation and found that the documents generated or used in the course of the investigation have not become accessible to unauthorized persons. The Authority requested and checked the data of the electronic log of the police administration system, which substantiated all this. The notifier referred to the controller’s rules on making copies, which stipu-

lated that it includes the party with opposing interest from the viewpoint of the criminal procedure as a person – in general – entitled to make copies. However, no conclusion could be drawn from this fact in itself, which would have indicated that this person would have actually accessed the documents of the investigation. The Authority also interviewed the person, who disclosed certain details of the criminal procedure to the notifier in an e-mail. This person explained in what way he had access to the data and the Authority checked the statement by contacting the controller.

The prosecutor's office also launched an investigation in the case. With the means at its disposal, all that the Authority could establish was that the police officers of the controller, who were taking action in the criminal procedure in question disclosed criminal personal data to an unauthorized person present at the procedural act, by naming the person who reported the criminal case.

The Authority called upon the controller to take measures, so that the police officers on its staff do not provide information on personal data in a criminal affair to unauthorised persons. The controller provided training to professional staff on the extent of information that may be provided in the course of police action, in order to avoid the unjustified or unnecessary provision of information on personal data in criminal cases for unauthorised persons in the future. *(NAIH-130/2021.)*

II.2.9. Processing of personal data generated in the course of the execution of sentences

The Hungarian Prison Service contacted the Authority to request a proper interpretation of the law on personal data processed by the Prison Service and asked for the Authority's opinion. In its position paper, the Authority examined in particular when the provisions of the General Data Protection Regulation and the Privacy Act transposing the Data Protection Law Enforcement Directive should be applied to the processing of data by the Prison Service units.

For a processing operation to fall within the scope of the Data Protection Law Enforcement Directive, it must meet two conditions:

- the purpose of data processing may be the following: prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including, among others, the safeguarding against and the prevention of threats to public security

- the controller is the competent authority defined in the Directive.

Pursuant to Recital (11) and Article 9(1) and (2) of the Data Protection Law Enforcement Directive, if the competent authorities process personal data for purposes other than those of the Directive, the General Data Protection Regulation shall apply. So, there may be data processing when the competent authority is the controller, yet the data processing activity is subject to the scope not of the Directive but of the General Data Protection Regulation, in view of the fact that the purpose of processing does not correspond to the purposes of the Directive.

By reason of its responsibilities and public powers, the Prison Service unit meets the notion of competent authority according to the Data Protection Law Enforcement Directive. In view of the fact that its task is the enforcement of penalties, data processing operations carried out as part of this basic duty are subject to the Directive and the Privacy Act, which transposes the Directive into national law. Prison Service units also carry out data processing operations which are subject to the General Data Protection Regulation, but such processing cannot be envisaged in relation to prisoners, but in their role as employer or some other capacity, and not in the course of discharging a core duty.

In the case of health data generated in the Prison Service, the provisions of Act XLVII of 1997 on the Control and Protection of Health and Related Personal Data (Health Data Act) regulate data processing, in addition to the Privacy Act and the Directive. When a prisoner receives health care in the prison, that health care is part of the enforcement of the penalty, and the processing of the data generated in its course is subject to the Directive. However, when processing health data, the provisions of the Health Data Act must always be borne in mind, as well as the fact that it is data processing subject to the Directive, which may not lead to a restriction of the exercise of the data subject's rights as far as his health data are concerned.

If the prisoner is treated in a hospital, i.e. he needs health care that the Prison Service unit cannot provide and because of this the services of a health care institution are used, that health care still remains part of the enforcement of his sentence. The data thus generated, which are therefore not processed by the Prison Service unit but by the hospital, are not covered by the Directive because the healthcare provider does not meet the definition of competent authority. This

processing is, therefore, subject to the rules of the General Data Protection Directive. *(NAIH-5728/2021.)*

II.2.10. Introduction of the InNOVA form at the National Police Headquarters, replacing the e-Paper form

A defence attorney (hereinafter: notifier) lodged a complainant with the Authority objecting to the processing of personal data in criminal procedures by a police department (hereinafter: Police Department). With reference to Section 53(5)(b) of the Privacy Act, the Authority terminated the investigation against the Police Department and informed the notifier that it contacted the Secretary of State of the Ministry of Justice in charge of coordinating the preparation of legislation and the enactment of public law (hereinafter: Deputy State Secretary).

In its submission, the Authority recommended based on Section 38(4)(a) of the Privacy Act, that the provisions concerning closed processing be supplemented when next amending Act XC of 2017 on Criminal Procedures (Criminal Procedures Act), so as to regulate the protection of the personal data of a defence attorney not related to the case in the course of the exercise of the right to inspect documents in a criminal procedure, so that they are not accessible to other stakeholders and parties to the procedure entitled to inspect documents in accordance with the regulatory requirements of the restriction of the fundamental right to information. In its letter, the Authority requested the Deputy State Secretary to inform the Authority on the position of the Ministry of Justice related to the above.

In his response, the Deputy State Secretary informed the Authority that he did not regard the amendment of the Criminal Procedures Act recommended by the Authority warranted, because the e-paper application automatically generates a submission and a so-called “front page”, which contains the personal data of the defence attorney in a non-editable format. Hence, the display of personal data is the result of a specific features of IT development, it does not take place because of the collaboration of the data subject or because of legal regulations. The Deputy State Secretary also informed the Authority that by reason of examining the regulation of e-administration, the Authority’s letter was transferred to the Ministry of the Interior.

In his letter, the Administrative State Secretary of the Ministry of the Interior informed the Authority that as a new technical solution, the National Police Headquarters introduced the InNOVA form developed by them as of 31 July 2020, in which no personal identification data are shown in the documents generated on the basis of the completed form. The National Tax and Customs Administration (NAV) also carries out investigations in criminal procedures. As the NAV uses Robotzsaru, the development carried out by the National Police Headquarters, resolves the problem for this organisation also.

The Authority contacted the National Police Commissioner and asked him whether based on the data protection criteria presented, the introduction of the InNOVA form proved to be successful.

In his response, the National Police Commissioner informed the Authority that the cases, which may be administered electronically within the remit and powers of the Police are accessible in 13 thematic groups in the Police Administration Portal (hereinafter: Portal) at https://ugyintezes.police.hu, using the option of *Ügyintézés* (Administration) after *Új ügy indítása* (Launching a new case). The electronic forms of acts of criminal administration can be found under *Bűnügyi szakterület* (Criminal area), including the InNOVA form named *Bűncselekményekkel kapcsolatos beadványok* (Submissions related to criminal acts) under identification No. IN-100016 replacing the e-Paper form earlier used by defence attorneys (report, motion, complaint, notification, submission), for which client information is available in Hungarian and in English.

Logging into the portal is ensured by the central electronic administration service called Central Identification Agent (hereinafter: KAÜ). When logging in, KAÜ makes available the 4T data (name, place and date of birth, mother’s name) of the logged-in natural person, which it offers for the InNOVA forms following the principle of interoperability. If the submission of a form is done not on behalf of a natural person, but through a company gateway hosting, the reporting person is not a subject of the administration of the case, because the business organisation is to be regarded as client in this case. In order to manage this contradiction, a logical examination is part of the operation of the forms, as a result of which – if the person making the report intends to submit the form from a company gateway–the 4T data of the person making the report disappear both from the interface and the .pdf document generated from the form. The .pdf document generated from the form transferred to the specialised system applied by the authorities (police, tax administration) only shows the name of the person submitting the form for information.

The 4T data of the person submitting the form will still be available in .xml format among the meta data of the form, which will be used to perform an eligibility

check in the course of submitting the form to verify that the natural person representative is indeed authorised to submit the form from the company gateway of the business organisation. Following successful submission, the specialised system stores the data of the representative making the report at meta data level among the persons to the case, so as to enable subsequent checking.

The National Police Commissioner also informed the Authority that the National Police Headquarters informed the Hungarian Bar Association under No. 29000/31688-1/2019 of the withdrawal of its forms provided through the e-Paper service and, in parallel, of the introduction of the new InNOVA forms as of 1 February 2020 on 5 December 2019, also explaining the intended development concerning the InNOVA forms. In accordance with the preliminary plans, the Police cancelled the former e-Paper service; currently, a form is available to defence attorneys, based on the above logic, which provides a higher level of protection in terms of purpose limitation of personal data.

Finally, the National Police Commissioner called attention to the human factor, because the IT solution presented above does not, in itself, achieve the desired objective without the mindful selection and completion of the form. Using and selecting the appropriate form depends on the decision of the client, in the present case the defence attorney, who also has to pay attention to appropriately completing the form and submitting it not from his own client gateway, but making use of a company gateway. *(NAIH-1192/2021.)*

II.3. Reporting data breaches

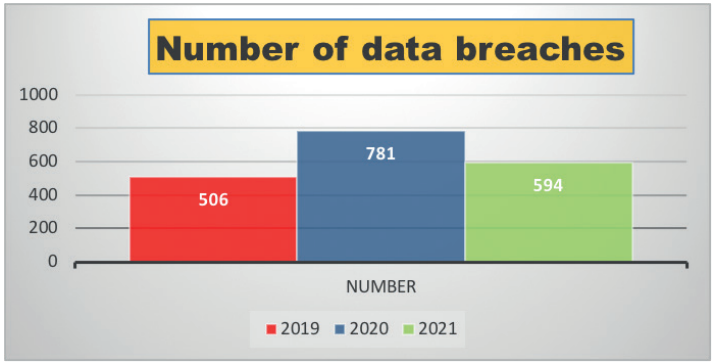
The Authority paid particular attention to compliance with GDPR Articles 33-34 also in 2021, including checking the notification of data breaches to the Authority and informing data subjects of the data breaches.

In the course of procedures related to data breaches, the infringement of data security requirements set forth in GDPR, i.e. Article 32, is also raised with increasing frequency.

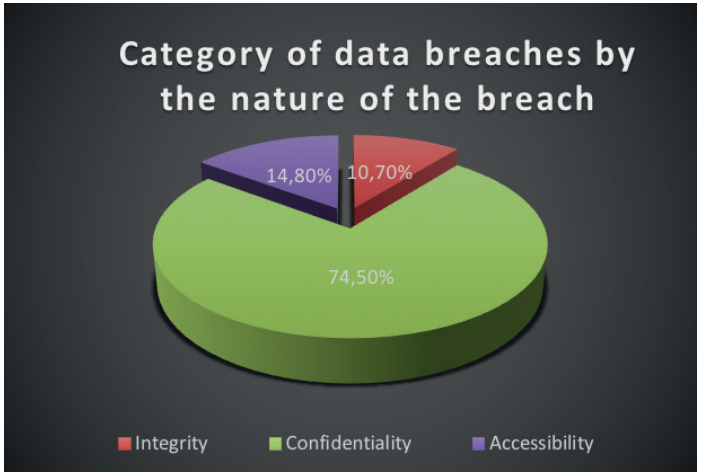
Data breaches in themselves may constitute data protection infringements; it is, however, important to underline that they may also be symptoms or signs of vulnerabilities, obsolete or poorly developed systems.

Accordingly, controllers have to map out the reasons leading to the data breach and adopt appropriate measures to do away with the vulnerability causing the data breach or, if necessary, they have to protect the system with reasonable data security measures.

In 2021, the Authority received altogether 594 data breach notifications, which figure decreased over the notifications received in the preceding year.



Data breaches may result in the violation of the principles of integrity, confidentiality and availability. In 2021, a substantial part of the data breaches (74.5%) resulted in a violation of confidentiality; relative to this, substantially fewer data breaches (14.8%) violated the principle of availability, while only about 10% of the notified data breaches (10.7%) led to the violation of the principle of integrity.



II.3.1. Major data breaches covered by the General Data Protection Regulation

1. The Authority received a notification in the public interest from the e-mail address of a private individual, to which the notifier attached an e-mail message forwarded to him and an Excel file that was the annex to the e-mail message. The Excel table attached to the e-mail message contained personal data of patients (name, birth date, address, contact data), their complaints, test results including the results of the Covid-19 rapid test in 1,153 lines. Originally, the e-mail was sent by a Budapest Government Office (hereinafter: Office) to all the district physicians and district paediatricians of three Budapest districts. The sender drew the attention of the originally addressed physicians the confidentially of the data, but the Excel file was not provided with access protection (e.g. password).

In its data protection procedure launched ex officio in relation to the personal data breach, the Authority established in its decision of 24 March 2021 that the Office infringed GDPR Article 32(1)(a)-(b) and (2) when it failed to apply data security measures proportionate to the risk of forwarding health-related data: it forwarded the database containing the exceedingly detailed and accurate health-related and contact data processed in relation to the Covid-19 rapid test in an Excel file without sorting them by districts and without access protection or encryption to safeguard the confidentiality of the data in a simple e-mail to the addressee district physicians. Furthermore, the Office also infringed GDPR Article 33(1) when notification to the authority of the high-risk data breach that took place was deemed unnecessary, and finally it infringed GDPR Article 34(1) when it did not wish to notify the data subjects of this high-risk personal data breach.

The Authority's decision ordered the Client to pay a data protection fine of HUF 10,000,000 for the above infringements. *(NAIH-2894/2021)*

2. A complainant launched a complainant with the Authority in which he objected to a website where after entering the TAJ [social security] number and date of birth, the system simply displayed the name, mobile phone number and permanent address of the citizen. According to the complaint, the system is accessible to the public without client gateway or any other authentication or authorization. There is no anti-robot check on the website and the system does not block the user's additional attempts even after entering erroneous data several times, so the automated queering of all the combinations (all the TAJ numbers * all the birth dates) would become possible using an application developed for this purpose even in possession of minimal programming skills.

The Authority investigated the complaint first under the inquiry procedure and then under the ex officio procedure.

The Ministry identified as controller informed the Authority that as a result of the Authority's inquiry, log-in to the website was modified, supplementing the identification required for log-in with a new field (mother's *surname*). All three items of personal data have to be entered correctly for logging into the administrative interface of the portal.

According to the Authority's IT expert, as the web application does not have a possibility for registration, nor is there log-in by password, it is recommended to take other security measures and introduce additional user authentication solutions so as *to prevent unauthorized persons having access to the system using the very common brute force attack technique.*

Article 32 of the General Data Protection Regulation specifies general requirements for the security of processing. Accordingly, the controller has to take appropriate technical and organizational measures to guarantee data security commensurate with the level of risk, including, among others, ensuring the continuous confidentiality, integrity, availability and resilience of the systems and services used to process personal data. With respect to a specific processing operation, it is therefore the controller's job – taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk for the rights and freedoms of natural persons – to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. This follows from the principle set forth in Article 5(1)(f) of the Regulation, which requires that processing be carried out in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage.

According to the Authority's assessment, the website's data security design, in particular, the resilience of the systems and services used to process personal data was not up to the level of data security proportionate to the risks of processing prior to the procedure. Without applying the appropriate protection, it is not possible to guarantee protection against unlawful or unauthorised access to the

personal data processed at a level sufficient from the viewpoint of state-of-the-art science and technology.

The controller acknowledged the fundamental data protection deficiencies of the portal in its very first response and its subsequent measures taken to remedy them – implementation of "captcha" check, the need to fill in the "mother's maiden surname" field, the blocking of the user for at least 2 hours after five unsuccessful attempts at log- – are compliant with the possible measures outlined in the Authority's IT security opinion to resolve the problem. The Authority checked that the modifications to the website were actually implemented as indicated by the controller.

According to the Authority's position, the deficiencies of information security mentioned in the complaint (*"there is no anti-robot check on the website, the system fails to block [users] after entering erroneous data several times, thus all the combinations could be run even with a minimal knowledge of programming"*) were genuine and the risks to data security caused by them (the possibility of building up a database) were substantial. With its measures taken in the course of the Authority's procedure, the controller took the minimally expected steps necessary for the website to qualify as acceptable from a data security point of view as assessed by the Authority, but according to its responses, the controller was also aware that the design of the website was, even in its current form, unsuitable for solving the problem over the long term.

Based on the above, the Authority stated in its decision that the controller failed to meet its obligation according to Article 32(1)(b) of the General Data Protection Regulation with its data security solutions provided with regard to the personal data, hence it imposed a data protection fine of HUF 2,000,000, i.e. two million forints on the controller. Furthermore, the Authority ordered the controller to take the necessary measures to begin the development of a new system enabling KAÜ log-in within 30 days from the decision becoming final and notify the Authority on the status of the development of the new system. *(NAIH-2414/2021)*

3. The Authority imposed a data protection fine on a commercial company because of its data processing related to checking the employee's e-mail accounts and the use of work tools. When checking a computer used for performing work by an employee, whose employment was earlier terminated, the employer had access to the privately used e-mail account and came to know personal data there.

In its decision, the Authority established that the company checked the employee's computer used for performing work in a manner that clashes with the principle of fair processing, it processed the content of the e-mail account used for performing work after the termination of employment without providing appropriate information in advance, nor did it provide prior information to the employee about the checking.

The company did not have separate rules for the use of e-mail accounts and work tools, therefore the Authority established that by infringing the requirement of data protection by design as set forth in Article 25(1) of the General Data Protection Regulation, it failed to take the appropriate technical and organisational measures to ensure the protection of personal data and the enforcement of the principles of processing in relation to the use of e-mail accounts and IT devices provided to employees and in the course of their checking, and it failed to provide appropriate information to the employee with regard to processing related to checking. The Authority imposed a data protection fine of HUF 2,000,000 on the company. *(NAIH-3644/2021)*

4. On 12 March 2021, a Mayor's Office learned that one of the municipal representatives shared data concerning the wages of municipal employees using the mobile phone of another representative. The data were downloaded from the database of the Hungarian State Treasury (MÁK) and they were forwarded to persons unauthorised to access them. The controller notified the Authority of the data breach on 29 April 2021, after which the Authority ex officio launched its audit.

The Authority's audit revealed that access to the MÁK database was enabled uniformly using the municipal executive's password, which was known to his colleagues and six employees other than the municipal executive were authorised to use that password exclusively during working hours. Altogether, 4 unlawful downloads were identified, each of them after working hours. The password protection was qualified as "weak" as the password consisted of the name and postal code of the settlement. The data breach affected the personal identity related data, contact data and economic and financial data of altogether 88 people. None of the employees of the controller acknowledged disclosing the password to unauthorised persons.

It was found in the course of the procedure that the controller did have rules of IT security; it, however, claimed that they did not apply to MÁK's electronic system. The controller did not have internal rules for the management of data breaches,

but as a subsequent measure it set a stronger password and also pressed criminal charges.

To further investigate the alleged infringement, the Authority initiated its data protection procedure ex officio. In the course of its data protection procedure, the Authority found that the controller was late in notifying the data breach as it learned of it on 12 March 2021, but notified it only on 29 April 2021, infringing Article 33(1) of the General Data Protection Regulation.

Furthermore, the Authority established that the controller infringed Article 34(1) of the General Data Protection Regulation because it failed to notify the data subjects of the data breach. The controller justified its decision by stating that most of the data subjects were public employees, hence in their case providing information to them could give rise to misunderstanding because of their low level of education, particularly with regard to the fact that the data subjects' trust in the employer would be shaken.

The Authority did not accept this argumentation, because the task of the controller is precisely to formulate the information in a way that it can be understood by the data subjects. In relation to this, Article 34(2) of the General Data Protection Regulation stipulates the obligation to provide information in a clear and plain language. For this reason, the controller could not have waived providing information lawfully. Nor is it sufficient reason that the trust of the employees would be shaken, because the data subjects have the right to know that their data were affected in a data breach and so they may be aware of the circumstances of the data breach. For all these reasons, the Authority ordered the controller to meet its obligation to inform the data subjects subsequently.

The Authority also found that the controller infringed Article 32(1) of the General Data Protection Regulation concerning the security of processing, because it failed to use a password of sufficient strength and failed to issue access authorisations.

For the above infringements, the Authority ordered the controller to pay a data protection fine of HUF 100,000. *(NAIH/4616-2/2021)*

5. The Authority received a notification in the public interest from a private individual, in which he called the attention of the Authority to a message sent to him to his private e-mail address. The sender of the e-mail was the district office of a Government Office, to which altogether five decisions were annexed in a .pdf format, which were decisions ordering epidemic isolation and epidemic surveillance related to the Covid-19 epidemic, including the identification and health-related data of five data subjects (two adults and three children).

According to the statement of the notifier, the e-mail was presumably not for him, it was erroneously delivered to him by the administrator of the district office, because he had had no contact to this controller before and did not know the data subjects.

The Authority launched an administrative inquiry and subsequently a data protection authority procedure in the case and found the following.

The sending of decisions containing health-related data to an erroneous e-mail address is due to the fact that a member of customer service staff of the district office asked for the e-mail address for entry into the epidemic data form from the data subject by phone and he accidentally mistyped and so recorded it erroneously. After this, the erroneous e-mail address was again erroneously recorded in the decision, because the administrator drafting the decision entered a .com ending instead of a .hu ending to the end of the e-mail address. Despite inquiries by phone by both the data subject and the erroneous addressee, the decisions were never sent to the correct e-mail address, the data subject never received the decisions by e-mail and learned of their content only orally when contacting the office by phone.

The controller district office did not classify the case as a personal data breach and did not handle it as such, even thought the leadership was aware of it because of the phone reports by both the data subject and the notifier in the public interest. In this way, the controller infringed Article 33(1) of the General Data Protection Regulation because even though it learned of it, it did not classify it as a personal data breach, hence it was unable to meet its notification obligation. In addition, it infringed Article 34(1) of the Regulation, because it also failed to notify the data subjects in an adequate and verifiable manner.

Furthermore, the Authority established in its decision that the sender should have protected the decisions containing health-related data with a technical measure restricting access (e.g. password protection) prior to sending them, to ensure that the data subject only has access to the content of documents concerning himself and to minimise the risks from an eventual missending. By forwarding data without data security measures, the district office infringed Article 32(1)(a)-(b) and (2) of the General Data Protection Regulation.

The Authority ordered the district office to pay a data protection fine of HUF 1,000,000 for the above infringements. *(NAIH-3647/2021)*

II.3.2. Major data breaches covered by the Privacy Act

1. Handling data breaches, criteria for establishing high risk

According to the notification of the data breach, an unknown person with the username and password of a member of the regular staff of the controller logged into the register of personal data and addresses through the Integrated Portal-based Querying System from a computer located in the premises managed by the controller, and queried personal data by specifying the address of a real property. He accessed the place and date of birth and mother's name of the person affected by the data breach. The controller learned of the data breach after the event in the course of responding to the request of the data subject aimed at the enforcement of his right to access submitted to the Ministry of the Interior.

Based on the investigation by the commander, the controller established that an unknown person obtained the login identifier of an authorised person in a manner that could not be explored within the framework of the commander's investigation and by logging in from a workstation, which could not be subsequently identified, carried out an unlawful query. In view of the results of this investigation, the commander of the controller lodged a report against an unknown perpetrator on 16 November 2020.

When handling the data breach, the controller failed to notify the data subject of the breach. It did not consider the data breach high-risk, it did not identify a consequence that would substantially affect the enforcement of a fundamental right and decided that delaying the notification of the data subject was justified with a view to protecting the interest according to Section 16(3)(b) of Act CXII of 2011 on the Right to Informational Self-Determination and the Freedom of Information (hereinafter: Privacy Act).

According to the Authority's position, knowing that the establishment of the exact circumstances of perpetration and the facts of the case was subject to an ongoing criminal procedure, the conditions set forth in Section 25/K(1) of the Privacy Act can be established, and hence high risk also exists. In the event of high risk, the controller has to notify the data subject without delay in accordance with the provisions of Section 25/K(1) of the Privacy Act.

The condition of establishing high risk is that the data breach may be concomitant with consequences substantially influencing the enforcement of a fundamental right to which the data subject is entitled. Among the factors to be considered when assessing the risk, the probability and severity of the risk should be equally examined and the risk must be assessed according to objective evaluation. In the case referred to, it can be establishing examining the circumstances of the data breach that the breach was the result of a malevolent action within an organisation, which could have unpleasant circumstances for the data subject as the querying person had direct access to his address and personal data. These personal identification data enable the data subject to be clearly identified in the same way for everyone, and the loss of control over the personal data and access to address data raises the possibility not only of the infringement of the right to the protection of personal data, but also the fundamental right to the protection of privacy, family life and the home. In terms of the severity of the consequences affecting the data subject, the detrimental consequences that may be associated with an eventual theft of identity, which are as yet unknown but whose possibility cannot be unambiguously excluded, cannot be disregarded. Furthermore, the client itself lodged a criminal report because of the criminal acts of abuse of personal data and violation of an information system or data. The elements of the facts of a case of misuse of personal data includes causing substantial violation of interest or perpetration with a view to unlawful gain. In view of all this, the Authority qualified the data breach as high risk.

The Authority also examined the client's reference to Section 16(3)(b) of the Privacy Act, according to which meeting the obligation to notify data subjects can be delayed, restricted or waived on account of the public interest in the efficient and successful prevention and detection of criminal acts. The client was unable to identify a specific case in progress. Furthermore, in the case of a high risk data breach, it is not enough to refer to a reason set forth in Section 16(3) of the Privacy Act in itself for being exempted from the obligation to notify the data subject of the breach, because according to Section 25/K(2)(d) and (6), the controller is exempted from the obligation to notify the data subject, if the law requires the exclusion, restriction or delay of notifying the data subject under the conditions and for the reasons set forth in Section 16(3) of the Privacy Act. In its response, the client did not refer to such a legal provision. In the case referred to, the Authority did not establish the existence of any of the circumstances set forth in Section 25/K(2) of the Privacy Act, hence the client was not exempted from its obligation to notify the data subject.

In view of the above, the Authority established the fact of the unlawful processing of personal data according to Section 61(1)(ba) of the Privacy Act, because of the unlawfulness of the management of the personal data breach taking place while processing the data by the client and called the client's attention to Section 25/K(4) of the Privacy Act, on the basis of which the client must notify the data subjects of the breach without delay with the content set forth in Section 25/K(3) of the Privacy Act. (*NAIH-8076/2021*)

2. Service of documents in a criminal case to an unauthorised person (defendant in another procedure)

The notifier was questioned at the prosecutor's office as a suspect, after which he was given the entire investigative documentation of the criminal procedure on an electronic data carrier. The data carrier given to him, however, also contained the documents of another criminal case launched on the basis of a foreign authority request for legal aid and it was not related to the notifier in any way, so he had access to some of its data (witness statements and their personal data, correspondence between authorities, etc.). The defence attorney of the notifier also received the investigative documentation of this other criminal case.

According to the response of the prosecutor's office acting in this case (hereinafter: controller) sent when contacted by the Authority, the electronic copies of the documents of the other criminal case were included among the documents handed over to the notifier and his defence attorney because of an error made in the course of the digitalisation of the documents of the investigation. According to the controller's information, the electronic file correctly containing the full documentation of the investigation was sent repeatedly to the notifier and his defence attorney and they were requested to return or destroy the erroneously sent electronic data carrier. The controller did not notify the data breach taking place because in its view, the provisions of Section 25/J(2) of the Privacy Act can be established, namely a data breach need not be notified, if it is probable that it carries no risk with respect to the enforcement of the data subject's rights. It based its position on the fact that the personal data concerned were unlawfully forwarded only to two persons and because of the measures taken immediately, the data breach posed no risk to the enforcement of the data subjects' rights.

However, according to the position of the Authority, the data breach posed a risk to the enforcement of the data subjects' rights. It could be established that the personal data of the data subjects including their personal data in a criminal case were accessed by persons not authorised to do so. Furthermore, one

of the persons who accessed the personal and contact data of the data subjects (witnesses in a criminal procedure) even contacted them to call their attention to the data breach.

The controller presented that it did not meet its obligation to notify the judicial authority of another EEA Member State as controller as set forth in Section 25/J(7) of the Privacy Act, because there were no personal data related to a criminal case in the course of the data breach, which the Latvian authority as controller would have forwarded to the Hungarian authority; also, the data breach affected data processing by the Hungarian authorities. According to its position, the data breach did not have any effect on the processing, protection and usability of the data forwarded to the foreign prosecutor's office asking for legal aid.

The Authority established unlawful processing because the controller failed to notify the controller of the EEA Member State to which it forwarded the data affected in the data breach, in spite of its obligation set forth in Section 25/J(7) of the Privacy Act; it registered the data breach with a delay; and erroneously identified that the data breach posed no risk with regard to the rights of data subjects. The reason for the Authority's decision is that a controller of the EEA Member State concerned has to be notified according to the Privacy Act not only if the data concerned by the breach are data which the other EEA Member State has forwarded to the Hungarian controller concerned by the breach, but also if the data concerned by the breach are data which the Hungarian controller has forwarded to the state concerned. Furthermore, the Act does not allow the controller to consider how the data breach may have affected the processing and protection of the forwarded data in an EEA state.

Having taken all the circumstances of the case into account, the Authority did not establish that the data breach would have been of high risk. The reason for this is that according to the information available to the Authority, a very narrow range, altogether two people had access to the personal data. One of these persons was accused in a criminal procedure who, having noticed the forwarding of the data causing the data breach, made the notification to the Authority; the other person was the defence attorney of the accused, who by virtue of the attorney client privilege is under an obligation to keep secrets. The Authority did not learn of any fact or circumstance, according to which there would have been any misuse of the data or they would have been used for any purpose other than calling the attention of the data subjects to the breach. In view of the fact that the Authority did not establish high risk, it did not order the controller to inform the data subjects in this case. It should be noted that the data subjects have learned

of the fact of the data breach from the notifier. In view of the above, the controller was not under an obligation to communicate additional information. (*NAIH-5188/2021.*)

II.4. Data protection certification procedures

Pursuant to GDPR Article 41, without prejudice to the tasks and powers of the competent supervisory authority, the monitoring of compliance with a code of conduct may be carried out by a body, which has an appropriate level of expertise in relation to the subject matter of the code and is accredited for that purpose by the competent supervisory authority. In accordance with the consistency mechanism, the Authority invited the opinion of the body on the draft of its criteria related to the accreditation of such organisations; the document is expected to be published early in 2022.

Pursuant to GDPR Article 43, without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, certification bodies, which have an appropriate level of expertise in relation to data protection shall, after informing the supervisory authority in order to allow it to exercise its powers pursuant to point (h) of Article 58(2) were necessary, issue and renew certification. In this context, it should be noted that of the options offered by the regulation in Article 43(1) the Hungarian solution implements the one under point (b), i.e. accreditation will be carried out by the National Accreditation Authority (NAA) in accordance with the EN-ISO/IEC 17065/2012 standard, in line with Regulation (EC) No. 765/2008 of the European Parliament and of the Council, and with the additional requirements established by the Authority. The document drafted by the Authority containing the additional requirements mentioned is expected to be published early in 2022.

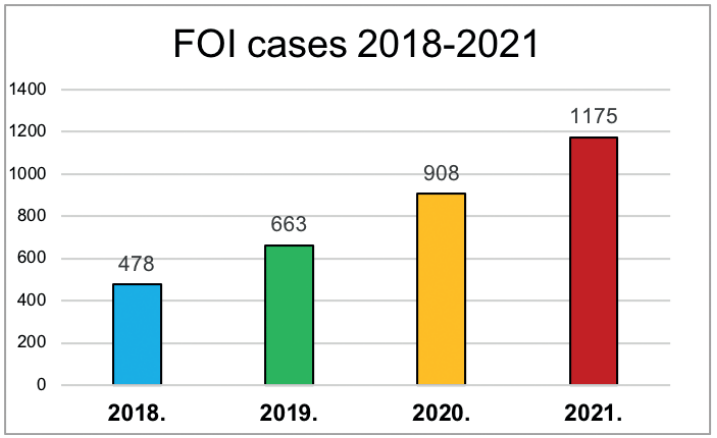
In 2021, the Authority completed a substantial part of its procedure to approve the first Binding Corporate Rules (BCRs) submitted since GDPR became applicable, following the procedures set forth in Document 263 of the WP Working Party. The issue of the Board's opinion on BCR and after that the adoption of BCR is expected in the first half of 2022.

III. Freedom of information

III.1. Introduction

The annual number of cases handled by the Freedom of Information Department has increased again: in 2021, we handled nearly 1,200 cases (not counting notifications of so-called rejected requests).[15]

Cases of the Freedom of Information Department 2018-2021



A large percentage of data requests were on the pandemic, but there continued to be vivid interest for old "hot topics" such as the cost and mode of travel by public officials, or the cost of exhibitions and other events organised using public funds.

15 Pursuant to the second sentence of Article 30(3) of the Privacy Act, the controller keeps a register of rejected requests and the reasons for such rejections and it informs the Authority of the information contained therein by 31 January each year.

Unfortunately, it happens frequently that it is difficult to identify the public authority handling the data even in cases of genuine public interest.[16] This is evidenced by a NAIH report where the requested organisation declined to forward the requested data even to the Authority in the case subject to the report, stating that NAIH was not authorised to access them.[17]

The most important "undertaking" in the life of the Supervisory Authority and the Department in 2021 (and 2022) is the launch and implementation of the Freedom of Information project. As beneficiary of the EU-funded priority project KÖFOP-2.2.6-VEKOP-18-2019-00001 "Mapping out and improving the efficiency of the Hungarian practice of the freedom of information" actual research work could begin at last in January 2021.

The contractors involved in the implementation of the project work under the professional guidance of NAIH, mobilising a team of around 60 experts. The research methodology and tools include: website analysis, pilot data request, online questionnaire, in-depth interviews, desk research and other background analysis (e.g. organisational analysis, international benchmarks, etc.). Situation assessment has been carried out in 2021 in each of the research areas and the results will be used as a basis for the research design and results. The four identified research areas are:

A. Access to information on municipalities

The full survey of the freedom of information practices of the roughly 3,200 local governments (of settlements and regions) operating in Hungary, as well as of the 13 national self-governments of ethnic minorities will be carried out; in addition, summary statements will be made for the 61 regional and 2,197 local level self-governments of ethnic minorities.

16 When asked who decides, and on what basis, on the additional corrective supplementary pension increase the amount of which is determined by a government decree, the complainant received the answer from four government bodies that they are not competent, and when contacted by NAIH, the Pension Payment Directorate of the Hungarian State Treasury could only inform them that they are only executors. Factual data on general consumer price increases and pensioner price increases for the first eight months of the year under review are contained in the September bulletin of the HCSO for the month of September of the year under review, and the annual general and pensioner price increases expected on the basis of these data are included in the forecast provided by the Ministry of Finance. All these figures are included in the government's proposal drafted for the autumn of the year under review, prepared by the Minister without portfolio responsible for families in the Prime Minister's Office and the predecessor Ministry of Human Resources. Eventually, NAIH referred the data request to the Minister without portfolio responsible for families (*NAIH-1017/2021*)

17 https://naih.hu/files/Infoszab_jelentes_NAIH-5567-8-2021.pdf

B. Access to information on central public administration

In accordance with NAIH's expectation, the most important research subjects are the agencies of central governmental administration including the ministries, but hospitals and vocational training centres as well as other agencies of the judiciary and the representations abroad are to be separately examined. The sector-specific focus areas were also designated (including the use of public funds, the transparency of applications, the transparency of legislation, the transparency of health care, and the enforcement of publication obligations related to typical employment relationships and public education.

C. Access to information on the activities of entities outside public administration, but managing public funds and/or discharging public duties

The research plan aims to review the websites of some 1,000 organisations, sending test data requests and online questionnaires to the target group with a uniform content and making at least 50 in-depth interviews. In addition, a series of focus group interviews are to be made involving citizens, NGOs and the representatives of the press experienced in data requests, and a detailed case study will be made, drawing deeper conclusions from the practice of several specific data request cases, with particular emphasis on the issues of trade secrets and copyrights and delineation of the range of subjects subject to the obligation of providing data.

D. And legal instruments and mechanisms which can facilitate (enforce) full access to data of public interest and data accessible on the grounds of public interest

The core issues of research include the provision of general information; the obligation of the parties to cooperate; self-reflection of agencies discharging public duties; the role of the press, NGOs and representatives; disclosure obligations; the private law elements of data requests; the content of data requests; the response of the controller; the rejection of fulfilment; the name and person of those requesting data; fulfilment of the disclosure of data and the issue of due dates; the mode of providing data; cost reimbursement; reasons for rejection; NAIH's organisation, role and powers, the provision of evidence and the outcome of litigation in court procedures, fora of legal remedy and their nature (civil or administrative litigation); court distraint; the role of and interpretation of the law by the Constitutional Court; systemic problems of legal regulation; international law harmonisation; special regulation concerning environmental information.

The research places great emphasis on the examination of the so-called proper exercise of rights. As stated in Section 30(7) of the Privacy Act, a comprehensive, account-level audit of the management of a public body constitutes a limitation on the request for data of public interest, by analogy, a series of data requests aimed at a systemic review of a public body or resulting in the impossibility of daily work are not compatible with the constitutional purpose of a request for data of public interest, since the legislator has assigned this task and competence to the body responsible for oversight of the legality of the exercise of public authority. International conventions, such as the Aarhus and Tromsø Conventions, apply a general rule of unreasonableness to such cases.

III.2. Access to information on the obligations of model-changing universities in relation to data of public interest

As from 1 August 2021, numerous Hungarian universities were transformed from a budgetary body into institutions maintained by foundations. Based on Section 4(1)(d) of Act CCIV of 2011 on National Higher Education (hereinafter: Higher Education Act), foundations, asset management foundations, public foundations or religious associations registered in Hungary may independently or together with another authorised entity found an institution of higher education. The transformed organisation is no longer a public university, but a private institution of higher education maintained by a foundation, which is maintained and owned by the foundation. Pursuant to Section 5(1) of the Higher Education Act, the institution of higher education and the organisational unit of the institution of higher education specified in Section 94(2)(c) are legal entities. Pursuant to Section 94(2)(c) of the Higher Education Act: *"The founding charter of the private higher education institution may pronounce the organisational unit of the private higher education institution – not including public education institutions and vocational training institutions operated as organisational units that are legal entities based on law pursuant to Section 14(3) – to be a legal entity. The organisational unit obtains its capacity as legal entity through the registration of the founding charter or its amendment by the Office of Education."*

A further consequence of the change of ownership is that the university is no longer directly part of the central subsystem of general government. Section 95(3) of the Higher Education Act also sets forth that: *"Private education institutions shall manage the assets placed at their disposal autonomously within the limits of their own budget as set out in their founding charters, or if public assets are at their disposal in compliance with the requirements applying to public finances".* The transformation of financial management was concomitant with a number of practical changes (including if a commercial bank became the account managing financial institution of the university concerned).

The primary purpose of the freedom of information is transparency of the operation of the state and the use of public funds. Section 3(5) of the Privacy Act states that the data concerning the financial management of an organ or person performing state or local government duties and other public duties defined by law qualify as data of public interest. Pursuant to Section 26(1) of the Privacy Act, any organ performing public duties shall allow any person to have free access to data of public interest and data accessible on public interest grounds under its control, if so requested, with the exceptions provided for in this Act.

Pursuant to Section 2(2) of the Higher Education Act, the state shall be responsible for ensuring the operation of the system of higher education, while the responsibility of ensuring the operation of higher education institutions shall lie with their maintainers.

The goals and principles of the Act on Public Interest Asset Management Foundations Discharging Public Duties (hereinafter: Public Interest Asset Management Foundation Act) include that:

(1) The state recognizes the role of public interest asset management foundations discharging public duties in creating social value and supports them in discharging public tasks and the implementation of their goals.

(2) In order to enforce the provisions of paragraph (1), the state protects the legal institution of public interest asset management foundations discharging public duties as particular legal subjects of private law and their autonomy according to private law and ensures the legal environment needed for their operation, including their organisational, financial and operational independence.

(3) When establishing a public interest asset management foundation discharging public tasks, the founder and the joiner ensure the asset elements and means of funding needed for the discharge of the public task.

(4) When designing Hungary's budget at all times ensuring the financing conditions directly needed for the discharge of public tasks and by way of asset management by the public interest asset management foundations discharging public tasks shall always enjoy priority."

Within its powers granted by Section 1 of Act XIII of 2021 on the contribution of assets and Section 1 (1a) of Act LXV of 2006 based on Section 3 of the Public Interest Asset Management Foundations Act, Government Decision 1413/2021. (VI.30.) on ensuring the conditions and funding necessary for the operation of certain higher education institutions and certain public interest foundations discharging public tasks in force since 30 June 2021 established the various foundations assigned to the various universities.

Pursuant to Section 5(1) of the Public Interest Asset Management Foundations Act, a foundation subject to this act may only be established for a purpose in the public interest. Additional details are settled by independent legal regulations in the case of every foundation, but Section 1(1) of the individual legal regulations include that "based on the Public Interest Asset Management Foundations Act, Parliament calls upon the Government to take the necessary measures to establish the foundation belonging to the university.

(2) In the course of the establishment of the Foundation, the minister in charge of education with regard to responsibilities and powers related to higher education (hereinafter: minister) takes action to represent the state."

Pursuant to Section 4(1) of the same act, assets amounting to at least 600 million forints (minimum capital) must be contributed to the foundation for its establishment.

Based on the legal regulations presented, it can be established that the model changing universities qualify as bodies founded and maintained by public funds on the one hand, and they continue to qualify as bodies unambiguously discharging public tasks, on the other hand. Their maintainers are public interest asset management foundations discharging public tasks founded by the Hungarian State in accordance with the authorisation granted in the Public Interest Asset Management Foundations Act. The foundation is also founded by public funds, it manages public funds and discharges public tasks, hence it is an organisation subject to the Privacy Act,

It follows that there is a legal obligation to provide general information to publish the required information electronically and to respond to requests for data of public interest.

In view of the legal definition of public tasks, the number of students who pursue their studies at the university on a self-financed basis each year is irrelevant. If a university maintained by a foundation receives a request for data of public interest and the institution receiving the request processes the data, the university has to grant the request. If data are requested which can only be found in the possession of the foundation as maintainer, the university is expected to notify the person requesting the data of this.

NAIH has consistently underlined the above statements also in the course of international investigations addressing issues of the rule of law in Hungary.

III.3. Important decisions by the Constitutional Court

Constitutional Court Decision 4/2021. (I. 22.) AB: Members of Parliament requested the Constitutional Court to declare Section 5 of Act VII of 2015 on the Investment Related to the Maintenance of the Capacity of the Paks Nuclear Power Plant and the amendment of certain acts related to it (Project Act) unconstitutional and its annulment with retroactive effect. This provision restricts access to both commercial and technical data and the data laying the foundations for decision related to this, whose access would infringe national security interests and rights to intellectual property for 30 years. The Constitutional Court did not find the motion well-grounded. Decision concerning the restriction of the freedom of information is made by the controller even in the most extreme cases, it does not set in by the power of the law; at the same time, a discretionary restriction of access is ab ovo anti-constitutional. The restriction of access intended to be achieved by the Project Act has a legitimate purpose justifiable because of international obligations and the nature of the investment. By the Project Act, the restriction of the freedom of information in order to protect national security interests and intellectual property rights is justified and necessary for the protection of the commercial and technical data. Provisions requiring blocking access for thirty years cannot be regarded as a disproportionate restriction as this is not an ex lege restriction, only a legal presumption. As the Project Act is to be interpreted in line with the Privacy Act, the controller has to carry out a "public interest test", thus the restriction may be applied, if it is of an overriding social interest.

Constitutional Court Decision 15/2021. (V. 13.) AB: The petitioner, a Member of Parliament, requested the Constitutional Court to declare Section 1 of Government Decree No. 521/2020 (XI. 25.) on derogation from certain data request provisions at times of emergency (Government Decree) unconstitutional and to annul it. Based on the contested provision, the organ discharging public task has to meet data requests within 45 days instead of the 15 days specified in

the Privacy Act, or in the case of an extension within 45+45 days, if meeting the request within 15 days would jeopardize the discharge of its public duties related to the emergency. The Constitutional Court declared that the contested provision complied with the conditions of restricting fundamental rights: combating the corona-virus pandemic, the reduction of its health-related social and economic impact and the mitigation of damage were purposes which constitutionally justify the restriction of the fundamental right and as such, they are proportionate to the disadvantage that the person requesting the data can obtain the requested information only within 45 or 90 days. At the same, it is a constitutional requirement that, when applying the Government Decree, the controller has to record the reasons, which make it probable that meeting the data request within the period set forth in the Privacy Act would have jeopardized the discharge of its public duties related to the emergency. Accordingly, when extending the deadline, it is not possible to refer to the pandemic in general, but the public task, which may remain unperformed, must actually be named.

Constitutional Court Decision 3293/2021. (VII. 22.) AB: The petitioner requested the declaration of the unconstitutionality of warrant 8.Pkf.25.611/2020/3. of the Fővárosi Ítélőtábla (Budapest High Court) and its annulment. In the base case, the petitioner submitted a request for data of public interest to the Prime Minister's Cabinet Office, from where he received an answer of refusal exceeding the period of 15 days open for this. Reacting to the submitted petition, the court terminated the procedure ex officio, stating that the petition was late because the period open for the petitioner to turn to the court begins when the controller falls into delay with meeting the data request. According to the governing judicial practice, the absence of a response is the first day of the period open for initiating a lawsuit and a subsequent response of rejection does not result in the reopening of the due date. The Constitutional Court rejected the petition because it could not examine whether the interpretation of the Privacy Act by the court was correct; as a result of the examination of constitutionality, however, it established that the petitioner's right to turn to the court was not violated by the fact that the court calculated the period open for initiating litigation from the day of failing to answer.

III.4. Important court decisions

Pfv.IV. 20.419/2021/6.: In its petition, the petitioner requested the issue of its own documents made available to the defendant for its earlier audits. The Curia deemed that this demand did not meet the requirements set for having access to data of public interest, it cannot be qualified as a request to access data of public interest, because the petitioner's demand for the issue of "documents" concerning itself does not and cannot serve the transparency of public affairs. In contrast to itself, through the data known to it, the purpose according to the Privacy Act cannot be interpreted, because it had already been obviously known to it how it used the public funds and other aid provided for its operation. So, the claim to be enforced in the course of the litigation cannot be reconciled with the social purpose of the fundamental right to access data of public interest.

Pf.20.053/2021/6.: The Ministry of Finance, having received the data request, called upon the person submitting it to clarify the request exceeding the 15-day period open for responding. Because of exceeding the period, the person requesting the data did not react to the call, but submitted a petition to the court of the first instance in due time, in which he requested that the court order the Ministry of Finance to issue the data. According to the judgment of the court of the first instance approved by the Fővárosi Ítélőtábla (Budapest High Court) the call for clarification was ungrounded as the data request was complete; also, the call was sent after the period open for this, hence the Ministry of Finance was ordered to issue the data according to the data request.

Pf.20.397/2021/4.: The controller charged the cost reimbursement beyond the 15-day deadline for response, thus it is considered late, hence the controller has to issue the data to the person requesting them without payment any cost, because missing the 15-day deadline for response according to Section 29(1) of the Privacy Act results in forfeiture of the right to charge cost reimbursement. Moreover, as the controller did not make use of the possibility to extend the deadline in accordance with Section 29(2) of the Privacy Act, one can justifiably draw the conclusion that in the controller's view meeting the data request does not entail a disproportionate use of the labour resources necessary for the performance of core duties of the body entrusted with public tasks, hence it may not claim cost reimbursement with reference to this. The Fővárosi Ítélőtábla upheld the judgment of the court of first instance.

Pf.20.056/2021/7.: Pursuant to Section 29(2)(a) of the Privacy Act, if the request for data involves data generated by an institution of the European Union or its Member States, the controller shall contact the institution of the European Union or the Member State concerned without delay and it informs the requesting party thereof. The Fővárosi Ítélőtábla declared that failing to do so in itself cannot result in an obligation to issue the data.

Pf.420.2021/5.: According to the Fővárosi Ítélőtábla it cannot be a barrier to issuing the data, if the controller continuously reviews and modifies the data it processes in the course of its operation. If, the circumstances impeding the issue of the data subsequently cease to exist, the court may also order the issue of data of public interest, whose issue the defendant has previously refused on reasonable grounds.

Pf.50.050/2021/3.: According to the opinion of the Győri Ítélőtábla (Győr High Court), the defendant's activity, which is only directed towards the technical and architectural implementation of the infrastructural background of some public task within the framework of a general contract, does not qualify as a public task, hence the issue of these data cannot be required from the entrepreneur.

Pf.20.234/2021/5.: Section 29(1a) of the Privacy Act provides for the refusability of data requests submitted within a year for the same set of data; however, the Fővárosi Ítélőtábla pointed out that as data of public interest may have several controllers, it is not an irregular exercise of rights, if the same person applies to several controllers with requests of the same content even simultaneously.

Pf.20.147/2021/6.: The information as to who drafted the information material of the ministry in question provides an opportunity for evaluating the work of a particular person. Data pointing to any special significance in the personal data requested to be disclosed with regard to the public activities of the persons concerned and their assessment did not arise in the course of the litigation, whereby public interest in disclosure would outweigh the individual interest in the protection of the privacy of the data subjects, therefore the Fővárosi Ítélőtábla did not order the controller to fulfil the data request.

Pf. 20.057/2021/7.: When the defendant controller refuses to fulfil a data request with reference to data compiled as part and in support of decision-making, regulated in Section 27(5) and (6) of Privacy Act, it must provide adequate justification. The total number of merit points obtained by applicants in the course of announced and adjudged job applications for judges and the obtained and opened merit points by the appointed judges constitute information on the data subject applicants qualifying as personal data. The argument that the number of merit points evaluates professional aptitude and is directly related to the discharge of public duties and hence data are accessible on the grounds of public interest cannot be substantiated by the final decision of the Fővárosi Ítélőtábla. The number of merit points received in the course of the job application for judges and the performance of judicial activity are not so closely related on the basis

of which the number of merit points could be regarded as other personal data related to the discharge of public duties and therefore data accessible on the grounds of public interest.

Pf.20.351/2021/5.: Pursuant to the correct interpretation of Section 28(1) of the Privacy Act, the request for the disclosure of data of public interest can only be directed at the disclosure of data which exist at the time when the controller receives the request and data generated thereafter are conceptually excluded from its scope. This also applies in the case of this litigation, all the more so, because the petitioner did not request the issue of documents generated under a given case number, but any document generated or received by the defendant in relation to the report of the State Audit Office, this request can only be fulfilled by disclosing already existing documents containing the data processed by the defendant. In addition to the above, the Fővárosi Ítélőtábla shared the position of the court of first instance insofar that it is indeed the responsibility of the petitioner to prove that the requested data exist and they are processed by the defendant, however, the person requesting the data is usually not capable of proving this beyond reasonable doubt, given that he is obviously not in possession of the information and has no overview of the internal administrative practice or document management by the controller, otherwise he would not make the data request. Therefore, the courts consider the existence of a convincing probability of the existence of data of public interest to be sufficient to order the disclosure of data for the purpose of Section 1 of the Privacy Act.

Pf.20.390/2021/4.: The Fővárosi Ítélőtábla shared the position of the court of first instance that the restriction of access to data of public interest can only be imposed for reasons indicated in the Privacy Act, taking into account the specific data and the reason for the restriction, while a general formal reference to the reason for restricting public access is unfounded.

*Pf.20.009/2021/4.: T*he Fővárosi Ítélőtábla upheld the judgment of the court of first instance, which stated that reference to trade secrets without any specificity is unacceptable. According to the facts of the case, the petitioner requested the disclosure of contracts by way of request for data of public interest, which the defendant concluded with two external companies with the subject matter "Transfer for further processing of fresh frozen plasma not needed for the purpose of transfusion". The defendant did not dispute that it was an organ discharging public tasks and acknowledged that the requested data were data of public interest with respect to which it was the controller; at the same time, it failed to substantiate what the proprietary information or business strategy was in the

contracts and their annexes requested to be disclosed (indicating the precise section of the contract and the provision), whose disclosure would violate or jeopardise its market interests, it only referred to “unusual contractual conditions more stringent than general”. According to judicial practice, where reference is made to a reason as ground for refusal to disclose data, such as trade secrets or data for decision support, the person making such a reference must allow the court to examine the merits of such a reason.

Pf.20.188/2021/9.: The fact in itself that the data of public interest requested to be disclosed is also used in a criminal procedure does not render the refusal to disclose the data lawful. The statement of the investigating authority may prove that the requested data are of such significance in the criminal procedure that it justifies a restriction on the disclosure of the data.

2.Pf.20.641/2021/4/II.: The court ordered the controller to provide detailed epidemiological statistical data in the format of an Excel table for the given day (e.g. altogether, how many confirmed SARS-CoV-2 cases were there in Hungary, what was the change relative to the preceding day; from how many districts were new cases reported over the preceding 7 days; number of symptom-free infected persons; number of patients with mild symptoms; number of patients with severe symptoms; number of patient on ventilators; number of patients in intensive care; total number of hospital beds reserved for the treatment of the Covid-19 disease; of this, intensive beds; number of free reserved beds and reserved beds in use; of these intensive, etc.). The defendant did not dispute that it was an organ discharging public tasks, nor that the data requested to be disclosed by the petitioner were data of public interest and that they were processed by it in an “bulk format”, at the same time, there were no grounds for its reference that meeting the petitioner’s data request would have placed an expressly major workload on its employees, in view of the fact that this is not a reason for refusal under the provisions of the Privacy Act. In the case under litigation, the data to be disclosed should be compiled using simple mathematical operations or systematic grouping out of the existing set of data, which does not mean the generation of qualitatively new data. The fact that this takes longer does not mean that the systematised data would be qualitatively new or different data. There are no public sources on the internet, where the data requested to be disclosed by the petitioner could be accessible in a daily breakdown. The fact that the petitioner could have requested some of the data of public interest even from the county government offices, also does not provide a basis to refuse the disclosure of the data, in view of the fact that these data were available to the defendant as an organ discharging public tasks.

III.5. Public access to data on the corona-virus pandemic

The Authority regularly updates its information to respond to any changes in legislation on requests for data of public interest in the light of the emergency. [18] At present, the rules of Government Decree 521/2020 (XI.25.) continue to apply to certain requests for data of public interest [the Constitutional Court examined this legislation in its Decision 15/2021 (13.V.) AB, already presented).

Important information:

1. A request for access to data of public interest may not be made orally, and it can be fulfilled in a form that does not involve the personal appearance of the data subject.

2. If it is likely that fulfilling the request within 15 days would jeopardise the performance of the public tasks of the public body performing the public task in relation to the emergency, the deadline for fulfilling the request may be extended by 45 days, and the applicant must be informed of this within 15 days of receipt of the request.

3. The 45-day time limit may be extended once for a further 45 days if meeting the request within 45 days would still jeopardise the performance of the public tasks of the public body performing the public task in relation to the emergency. The applicant must be informed of this before the first 45 days expire.

4. In the case of the assessment and payment of a fee, the request for data must be fulfilled within 45 days if it is likely that the fulfilment of the request within 15 days would jeopardise the performance of the public tasks of the body in relation to the emergency. In this case, the information shall be provided within 45 days on the following:

− the fulfilment of the data request would involve a disproportionate use of human resources necessary for the performance of the basic activities of the public sector body, or

− the document or part of a document for which a copy is requested is voluminous, and

18 https://naih.hu/dontesek-informacioszabadsag-tajekoztatok-kozlemenyek?download=473:tajekoztato-a-kozerdeku-adatigenylesek-teljesitesere-iranyado-rendelkezesek-jarvanyugyi-veszelyhelyzet-miatti-valtozasarol-2021-12-20-tol

− the extent of reimbursement and the possibility of providing the service without the need for copies.

5. In the cases mentioned, the deadline for filing a judicial remedy under Section 31(1) of the Privacy Act is also amended (45+45 days).

6. The provisions described above had to be applied also to requests for access to data of public interest already pending at the time of the entry into force of the Decree.

In all cases of complaints where the 45-day time limit was invoked, the Authority called on the public body to justify its reasons, and on several occasions the Authority did not consider the invocation to be justified because the body concerned did not have a direct epidemiological mission justifying the extension.

Since the spring of 2020, the Authority dealt with issues related to the pandemic in over 200 cases in the form of investigation, consultation, data request or its procedure. As evidenced by the complaint cases related to the freedom of information, most of the time those requesting data wish to access data concerning the number of infected, vaccinated, recovered and deceased persons, those in quarantine, those requiring hospital care, intensive therapy or ventilation, the number of those no longer ventilated and their distribution in many cases in a breakdown by having been vaccinated or not, and in a breakdown by vaccine type and the number of vaccinations.

NAIH also issued a communiqué concerning public access to the corona-virus infection data of settlements, which underlined that there was a substantial public interest in accessing the infection data of any settlement, the number of these figures was necessary for both mayors and residents in order to be able to make informed decisions concerning their defence against the epidemic. Mayors are important actors in the defence against the epidemic, hence it is the obligation of the competent government office to provide them with the relevant statistical data.

It is our frequent experience that those requesting data would have liked to learn from NAIH concrete information about the epidemic and its management and changes. In these cases, the Authority informed the persons requesting the data which organ discharging public tasks they can turn to (such as the National Public Health Centre, the National Hospital General Directorate or the various ministries).

In many cases, complainants objected to the fact that they did not receive a medical explanation to the professional health-related issues bothering them. Since the conceptual element of data of public interest is the fact that it is recorded and that the organ in question must handle such data, in these cases the organs discharging public tasks lawfully rejected the data requests, because they are not obliged to provide professional justification for their decisions or to express their professional opinion in the context of a data request of public interest.

A great deal of interest was expressed also with respect to the vaccine contracts. According to the statement of the Ministry of Foreign Affairs and Trade, the contract in question was concluded by the National Public Health Centre, the contract itself was not in their possession, at the same time, they saw no reason for restricting public access to the contract. Finally, the minister in charge of the Prime Minister's Office published the purchase and sale contracts concerning the vaccines stemming from Eastern sources (on its Facebook page[19]). *(NAIH-2963/2021)*

It should be noted that the issue of public access to the contracts concerning the procurement of vaccines by the EU was also a subject of criticism in 2021. The European Commission headed the negotiations on the procurement of the vaccines based on the negotiating principles approved by the Member States, which finally published a number of contracts with the agreement of the companies concerned, although the companies insisted on blocking out certain confidential business data.[20]

Another notifier wished to learn from the Ministry of Human Resources (hereinafter: EMMI), inter alia, who represented the Hungarian Government in the steering committee supervising vaccine procurements and whether the representative of the Hungarian Government raised any objection to the content or any part of the EU framework contract in the course of the procedure. The Authority called upon EMMI to disclose the requested data, because the name of a person discharging public tasks cannot qualify as data on which a decision is based. The data concerning the adoption of the preliminary framework contract is considered data of public interest, the requested contracts need to be disclosed, while information qualifying as trade secret, whose violation would constitute a disproportionate injury to the business activities of the contracting party, is to be blocked out. The

19 https://www.facebook.com/permalink.php?story_fbid=2853863864870374&id=1443632629226845

20 https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/public-health/eu-vaccines-strategy_en#transparency-and-authorisation-mechanism-for-exports-of-vaccines

ministry has not fulfilled the data request ever since and the Authority issued a report on the case[21].

There were objectionable examples also of disclosing health-related special category personal data in the social media. A mayor disclosed the full name of the notifier and the positive result of his Covid-19 test in the parents' closed Facebook group of a kindergarten. The Authority called upon the mayor to erase all the personal data in the Facebook group on the basis of which the data subject concerned in the comments shared in the group could be identified either directly or indirectly. *(NAIH-3418/2021)*.

A person requested the issue of a copy of the certificate on the vaccine administered to the President of the Republic showing the name, but "blocking any other personal data". In the data request, he expressly underlined that the President of the Republic was a public actor, who had earlier "disclosed by way of the MTI (Hungarian News Agency) that he was vaccinated with the Chinese vaccine". The "other personal data related to the discharge of public duties" mentioned in the Privacy Act can only refer to the set of data closely related to the discharge of the constitutional tasks of the President of the Republic and this definitely does not include the content of the vaccination certificate. Unless the data subject voluntarily and freely decides otherwise, access to his vaccination certificate may be lawfully rejected in the context of a request for data of public interest. *(NAIH-3356/2021)*

III.6. Administrative Procedures Act vs. Privacy Act

The 2018 annual report[22] already disclosed the problem of law interpretation, whose main question is whether the restriction stipulated in Section 27(2)(g) of the Privacy Act ("the right to access data of public interest or data accessible on public interest grounds may be restricted by an Act, if considered necessary for the purposes of court proceedings or administrative authority procedures") *can be applied to the accessibility and publicity of the documentation of administrative authority procedures, i.e. whether Act CL of 2016 on General Administrative Procedures (hereinafter: Administrative Procedures Act) and CLXXXV of 2010 on Media Services and Mass Communications (hereinafter: Communications Act) govern as lex specialis.*

21 https://naih.hu/files/Infoszab_jelentes_NAIH-694-1-2022.pdf

22 pp. 118-119

According to NAIH's position, this restriction does not apply to administrative authority proceedings that have already been concluded, all the more so as both the Administrative Procedures Act and the Communications Act require restrictions only in the case of personal and classified data, and no legal regulation has provided for the anonymisation of data of public interest or data accessible on public interest grounds.

In 2021, the civil lawsuits finally came to a final and binding end, which, inter alia, provided an answer – in line with the NAIH's position – to the question of the procedure and legal provisions under which third parties other than the clients may access the official documents of the authority generated in the proceedings related to the authorisation to provide media services. In a litigation launched to request disclosure of data of public interest, Fővárosi Törvényszék taking action in the first instance ordered the controller in its judgment 28.P.20.997/2019/8. to issue the full text of the requested media authority decisions to the petitioner within 15 days, but the remaining part of the petition was rejected. As a result of the examination of Section 33 of the Administrative Procedures Act and the Privacy Act, the court arrived at the conclusion that Section 33 of the Administrative Procedures Act narrows down the set of accessible data relative to the provisions of the Privacy Act and documents generated in official proceedings may be inspected only by the person entitled to do so, the client, in the context of the right of access to documents, but according to Section 33(5) of the Administrative Procedures Act, the decision is accessible to anyone without restriction. It drew the conclusion from this that, in the case of a request for a decision, there is no need for identification , the identity of the person requesting the data is irrelevant, hence the defendant cannot deny access to the decision even on the basis of the provisions of the Administrative Procedures Act it referred to. The Fővárosi Ítélőtábla taking action in the second instance in the litigation partially reversed the judgment of the court of first instance in its judgment 32.Pf.21.108/2018/8 and also ordered the controller to issue the submissions supporting the decisions related to the aforementioned decisions, since the request for issuing data of public interest in that litigation is to be adjudged exclusively in accordance with the provisions of the Privacy Act. In its judgment Pfv.IV.20.656/2020/4 adopted in a review procedure, the Curia annulled the final judgment – on procedural grounds – with regard to issuing the submissions, but otherwise upheld the judgment of the court of first instance.

III.7. On requests for data of public interest submitted to the NAIH

In 2021, the Authority received 58 submissions containing requests for data of public interest from 44 petitioners, which altogether contained 139 requests for data (in 2020, the 72 requests from 43 petitioners contained altogether 187 data requests). Similarly to the trend observed since 2015, it occurs that certain individuals pose several questions in their submissions.

According to our statistics, the data requests were concluded with the following results:

- 100 requests granted,
- 9 requests partially granted,
- 28 requests rejected,
- 2 requests not fulfilled for reasons attributable to the petitioner.

The most frequent reasons for rejections were the following:

- the data intended to be accessed were not data of public interest or data accessible on the grounds of public interest,
- the requested data were not available to the Authority,
- the requested data supported the option of a decision.

The most frequent subject matters of the data requests included requests for data concerning the Authority's activities in the context of the corona-virus pandemic (number and content of the relevant statements, investigations, etc.). Similarly to the past year, requests for data related to data protection procedures, data breach notifications and fines imposed were also typical. In addition, the petitioners submitted numerous questions to obtain information on the Authority's internal rules, practice of imposing fines and the application of the GDPR.

III.8. Reimbursement of costs

A proper implementation of the freedom of information requires transparency of the procedures for determining the reimbursement of costs (in addition, let us add that in rule of law investigations against Hungary, criticism if often made for the cost reimbursement charged for fulfilling requests for data of public interest). According to the statistics for this year, the Authority dealt with 27 such cases which – in addition to complaints – included consultation questions as well as cases left over from 2020 (altogether 6 cases). The controllers under investigation included municipalities, government offices, mayor's offices, various welfare institutions, ministries, police departments and foundations.

The number of relevant cases continues to be relatively low (2018: 39, 2019: 32, 2020: 23, 2021: 27) and as a result of NAIH's intervention, the organs discharging public tasks concerned issued the requested data in most cases free of charge, at the same time, because of certain high amounts, the positive trend of the previous years came to a halt. In 2021, the amount of the highest cost reimbursement was HUF 500,000 (in this case, it would have been necessary to manually examine over 11,000 files kept by a welfare institution of a municipality according to specific criteria), however, cost reimbursement set in amounts below HUF 100,000 were more typical.

There were two occasions when NAIH accepted substantial reduction in costs, in view of all circumstances of the case. In one case, the data were available partly electronically and partly in hard copy, so the data in the electronic system (file number, report) had to be reconciled with the hard copy documents in order to obtain the correct data. In view of this, we regarded the calculation reduced from 317,209 forints to 158,000 forints as acceptable. (*NAIH-2651/2021*)

A case that had begun in 2020 was successfully closed when following NAIH's call, the government office issued the data requested free of charge. The petitioner requested data on the guardianship authorities belonging to the territorial government office and was then informed that the time required to complete the data request was 22 hours and the labour cost/working hour was 2,202 forints, i.e. a total of 48,444 forints. Then, the petitioner requested the government office to provide details of the content of the cost reimbursement which, however, was never met. According to NAIH's position, they calculated amount for fulfilling the data request can be regarded as excessive and it is unrealistic that the government office does not store the documents electronically. (*NAIH-734/2021*)

A municipal executive asked for NAIH's position concerning a case when data requests are received from a petitioner daily on the same subject matter, could they be aggregated in terms of the number of working hours with regard to the cost reimbursement. According to NAIH's interpretation of the law, if the person of the petitioner and the subject matter of the data request are identical or there are only minimal differences in the subject matter in the case of data requests submitted within 15 days, a legitimate interest can be foreseen, on the basis of which the controller aggregates the data requests in order to improve their ad-

ministrative efficiency. NAIH emphasized that in the absence of the coexistence of these conditions it is not possible to aggregate the data requests under the legal regulations currently in force. (*NAIH-2450/2021*)

Partly related to the case presented above is the unlawful practice of a rural municipality which automatically attached cost reimbursement to fulfilling data requests. It is highly important to call attention to the fact that this practice is contrary to the spirit and the regulation of the fundamental right. Reacting to the practical problems of the application of cost reimbursement, NAIH published detailed guidance on its website23, which could assist organs discharging public duties in considering whether to charge cost reimbursement. The guidance discusses the calculation of due dates, the identification of the main cost elements and the applicability as well as the obligation to provide information and to anonymize. In addition, the obligation to cooperate is highly important on the part of both the petitioner and the organ discharging public tasks. Appropriate communication from both directions makes it simpler and easier to fulfil data requests and an accurate description of the subject matter of the request could greatly reduce the costs that may be incurred.

Additional cases concerning cost reimbursement will be presented in the subsection on *The transparency of environmental information*.

III.9. The transparency of municipalities

According to the Authority's case law, the organs of the body of representatives constitute a unit from the viewpoint of ensuring freedom of information, which means that when a request is submitted for data of public interest, the municipal executive cannot rely on the fact that request for data affecting the municipality was not submitted to him by the petitioner. The petitioner must not suffer a disadvantage and his request must not be rejected with reference to the absence of data, because his request was addressed to the appropriate organ of the body of representatives. If there are internal rules on fulfilling a data request, incoming data requests must be forwarded right away to the person obliged and authorised to evaluate and fulfil it, i.e. the appointment of an expert dealing with the rights to information in charge of freedom of information cases can provide a solution for such a situation.

23 https://naih.hu/dontesek-informacioszabadsag-tajekoztatok-kozlemenyek?download=392:tajekoztato-a-kozerdeku-adatigenyles-koltsegteriteserol

The basis of an investigation on the valuation of municipal assets as a basis for decision was that the meeting of representatives of the municipality had a valuation made with a view to potentially purchasing a real estate, but the preparatory work did not reach the stage of drafting the decision in terms of the purchase and sale of the real-estate in question. The real-estates were sold, but the meeting of representatives did not make a decision on the purchase of the property and did not submit an offer to buy. According to the Authority's position, a restriction, which prevents the public to access data in the case of a legal transaction, which has already been closed citing that the data may be used at an unspecified date cannot be regarded as being in line with the Fundamental Law in view of the enforcement of the right to access and disseminate data of public interest. (*NAIH-5801/2021*)

Linked to the meeting of the municipality' property management committee, a municipal representative requested access to general construction contracts, review protocols, valuer's opinions within the framework of requesting data of public interest. The investigation pointed out the "bad" practice pursued by municipal bodies, according to which a so-called general vote is held on discussing the points of the agenda in open or private meetings, regardless of their content. In its notice on the issue of business data and trade secrets, the Authority underlined that the data relating to decision-making on municipal assets are data accessible on public interest grounds, and they can only be classified as trade secrets within a narrow range of exceptional cases. (*NAIH-1170/2021*)

Last year, the Authority received several notifications concerning the infringement of the right to the protection of personal data without any intent to cause harm. In one case, an employee of the office of the municipality published an a local closure order for the bees of a local beekeeper on his private social networking site in a manner that made the personal data of the beekeeper accessible causing him damage. As a result of the investigation, the municipality created an official social media page which is edited and the content published there is monitored by the head of the local office, who has also required the civil servants of the office to participate in a data protection training course. (*NAIH-7586/2021*)

Section 29/A(3) of Government Decree 314/2012. (XI. 8.) on the conception of urban development, integrated urban development strategy and the instruments of settlement planning and certain specific legal institutions of settlement planning requires that preliminary proposals under partnership reconciliation must be published on the website of the municipality; this, however, does not mean the publication of the records of partnership proposals. The names and addresses of

those stating their opinion on the preliminary proposals are personal data, their publication on the municipality's website qualifies as processing personal data. Section 37(5) of the Privacy Act requires organs discharging public tasks to invite the opinion of the Authority, if an organ acting as a body corporate, entitled to disclosure (typically these include the bodies of representatives of local governments) seeks proactively to ensure wide-ranging access to data of public interest or data accessible on public interest grounds processed by them. Municipalities have defined the data to be disclosed in specific publication lists as data to be published for the registration of the statements of assets made by members of the municipal bodies (body of representatives and their committees), contracts of less than 5 million forints and tenders of less than 5 million forints. The accessibility of the data in the statement of assets of municipal representatives – in particular, the data concerning the occupation, place of work and monthly taxable income of the representative from his employment – arises as a recurrent question of consultation year after year. In this respect, the Authority has consistently represented the position that the data in the part on the statement of income are data to be provided mandatorily, hence these data may not be blocked when the statement of assets is accessed by a third person.

We also wish to call the attention of the municipalities to the fact that the purpose of the service provided through the e-mail address *@mail.lgov.hu* is to enable the Government to communicate with municipal executives and mayors through a uniform separate channel, thus this address cannot be indicated as a form of maintaining contact with citizens. (*NAIH-2650/2021*)

III.9.1. Personal data accessible on grounds of public interest in connection with the performance of public tasks

Last year, the Authority conducted several investigations into cases, in which the subject matter of the request for data of public interest was access to the job description of a manager in the employment of an institution of a municipality or public body. As the legal regulation governing employment does not contain specific provisions, therefore the controller discharging public tasks decides on these at its own discretion on the basis of Section 26(2) of the Privacy Act. According to the general definition, the job description covers the work processes and activities, tasks, functions and network of contacts of the employee, including the objectives, primary areas of responsibility, as well as the conditions under which the employee performs his work. The job description is indeed the detailed specification of the job. The employer lists in this document the tasks to be carried out and the tasks for which the employee is responsible. These include the powers and responsibilities, which may be exercised by the employee and which relate exclusively to the public task discharged by him, thus, in Authority's view, these are data accessible on public interest grounds. (*NAIH-1147/2021*)

In another case concerned in an investigation, the subject matter of the data request was the job description and remuneration of the secretary of an organ discharging public tasks, operating in the form of a public body. According to the Authority's position, even though the secretary's employment relationship is based on the Labour Code and his remuneration is not paid from public funds, but from other revenues of the public body, his primary task as a senior officer is to ensure the performance of the public tasks of the public body set forth in law at the highest possible standard, hence the data concerning his remuneration qualifies as other personal data related to the discharge of his public task, which is accessible to anyone through a request for data of public interest. (*NAIH-3655/2021*)

According to the position of the Authority, pursuant to Section 179 of Act CXCIX of 2011 on Public Service Officers (Public Service Officers Act), in addition to the data accessible on public interest grounds listed therein, the set of data on pay should be interpreted broadly, in view of the requirement of equal treatment set forth in Section 13 of the same Act, as it includes other dues and benefits received in connection with the public service relationship or in relation to it. Taking these into account, the jubilee award is a benefit linked to the public service relationship, which is financed out of public funds not with regard to events and life situations listed in Section 152(1) of the Public Service Officers Act associated with privacy. (*NAIH-4045/2021, NAIH-5224/2021*)

A petitioner requested access to documents generated in relation to the appointment, remuneration and bonus payments of a municipal executive retroactively for 13 years. In terms of disclosing the data retroactively to 2008 – with reference to the decision of the Supreme Court BH.2007/1/14. – in accordance with the Authority's interpretation of the law, the Privacy Act does not have retroactive effect. In addition, it is warranted to reasonably delineate the period concerning the municipal executive's remuneration (such as, for instance, the period of a given municipal cycle). On account of this case, the Authority drew attention of the evolution of a trend contrary to the original goal of the legislator with regard to the enforcement of the freedom of information, because the request to access the data concerning pay and other benefits of a single person retroactively for 13 years, raises the possibility of creating an itemised list of the personal data of the

person concerned in bulk, accessible on public interest grounds, and creating a new quality of data, a database. (*NAIH-3344/2021*)
Based on the argumentation, presented in Constitutional Court Decision 3145/2018. (V. 7.) AB, the name and the employment contract of the mayor's consultant, chief of cabinet, chief of protocol (while blocking protected personal data) are data accessible on public interest grounds. The persons, whose work is related to the responsibilities and powers of the municipality as an organ discharging public tasks, and hence their activity is capable of influencing managerial decisions, particularly those of the mayor and they have influence over changes in local public life, are identifiable by way of requesting data of public interest. According to the Authority's statement issued when contacted for consultation, the mayor's office is not authorised to have access to the data and documents of payments made to the employees of a business organisation owned by the municipality processed by that business organisation in a manner enabling the individual identification of the data subjects. As a business organisation manages its assets and the human resources it employs independently within the limits of the legal regulations and its deed of foundation, it qualifies as an independent controller with regard to the data processed by it, hence a relationship of controller and processor between the two organs is not applicable. In addition, legal regulations governing financial management also do not provide an appropriate legal basis for the lawful forwarding of personalised data. (*NAIH-3136/2021*)

III.9.2. Transparency of the operation of national minority self-governments

Last year, several notifications were received, so the Authority – jointly with the deputy commissioner in charge of the protection of the rights of ethnic minorities in Hungary – launched an investigation with a view to assessing the transparency of the operation of national minority self-governments and their improvement, if needed, the results of which are expected in 2022.

According to information provided by the secretary of state of the Prime Minister's Office in charge of regional public administration, there were no extraordinarily severe violations of the law in the period from the elections in the autumn of 2014 to 20 July 2021. In terms of the freedom of information, A common problem with meetings of the body [of representatives] is the misunderstanding of the issue of closed meetings.

The mandatory disclosure according to the Privacy Act is a highly important instrument of transparency. In relation to this, the information included that all the

national ethnic minority self-governments have their own websites; this, however, does not hold for the ethnic minority self-governments at regional and local level. Characteristically, ethnic minority self-governments publish their data of public interest and data accessible on public interest grounds on the websites maintained by local governments or national self-governments; the range of these data is typically minimal, covering mostly the basic data of the representatives and of the self-government only; in some cases, additional data, such as protocols, rules of organisation and operation are also accessible, but these data are rarely updated. (*NAIH-3383/2021*)

III.9.3. Disclosure of personal data during online public hearings

Many municipalities provided a possibility for citizens and the local community to participate in local affairs and the development of decisions even during the emergency and they held online public hearings using the live streaming function of social media.

Similarly to public hearings in person, in the course of the preparation of the online public hearing, interested persons could submit their questions and proposals to the mayor's office in writing, requesting a serial number. The complainant acted as described, but had not reckoned with the fact that in the course of the online public hearing, when his submission was read and discussed, his name and address was continuously displayed on the screen. He requested the erasure of these data from the video recording, as well as the protocol, but the municipality rejected his request on the grounds that the public hearing is a public meeting of the body of representatives, constituents – present there upon prior registration – state their names and their personal observations on local public affairs and they also indicate the area where they come from and eventually they provide their address. The lawfulness of the processing of personal data in the course of a public hearing is provided by GDPR Article 6(1)(e). A protocol is drawn up on the meeting, which is accessible to the public. According to the Authority's position, the fact that some personal data are mentioned at a public meeting of the body of representatives does not result in the personal data becoming accessible on grounds of public interest merely because of this fact.

Earlier in his statement issued under ABI-1332/A/2006-5, the Data Protection Commissioner explained that even their (formally) given consent does not provide a basis for the recording and disclosure of the personal data of data subjects interested in and present at the meeting of the body of representatives, as the processing of data does not comply with the principle of purpose limitation.

At the same time, a contributor concerned, if given the floor, has the right to decide whether they wish to speak anonymously or otherwise, and he needs to be informed in advance that his contribution will be recorded in the protocol. If the response to his contribution is sent in writing, it is not expedient to record and to store the name and address of the data subject in the protocol accessible to the public. According to the position of the Authority, the accessibility of the public hearing is assessed the same way as a public meeting of the body of representatives. Taking this into account and fully ensuring the protection of privacy, private secrets and personality rights, there is no obstacle to the live streaming of this special form of the meeting of the body of representatives whether through the official website of the municipality or on a social media page. The Authority shared the opinion of the municipality according to which there is no fundamental difference between the processing of data related to traditional public hearings with presence in person and online public hearings. However, the Authority underlined: a citizen participating in a public hearing in person can give his consent or object to displaying and disclosing his personal data in the protocol in person, while participants in the online space cannot enforce their right to informational self-determination or can do so only with difficulty. With regard to the processing of data related to an online public hearing, it is the express opinion of the Authority that the controller must act more carefully with regard to the enforcement of the right to informational self-determination, because citizens are in a much more exposed position in the online space than in the case of a traditional public hearing in terms of the processing of their personal data; it follows that information by the controller concerning the processing of the data and guaranteeing data subject rights are more important and have greater significance. (*NAIH-4447/2021*)

III.9.4. Electronic disclosure

In 2021, about 30% of the notifications sent to the Authority in cases related to the freedom of information concerned inadequate electronic disclosure by organs discharging public duties; most of the time, the websites of local governments and the websites of business organisations in municipal ownership were involved: the vast majority of the notifications concerned problematic disclosure of data related to the activities, operation and financial management of the organ (documents of the body of representatives, municipal decrees, contracts, public procurements, applications, etc.). In the course of its investigation, the Authority contacts the organ concerned in every case and whenever necessary calls upon it to immediately remedy the established infringement of the law, which is generally complied with sooner or later. It should, however, be mentioned that in view of the emergency caused by the virus, the bodies of representatives had no meetings for months in most settlements in 2021. In such cases, the municipalities notified the Authority that no meetings of the body of representatives took place in the period indicated, instead decisions by the mayor brought during the period of the emergency[24] are accessible on the websites.

III.10. Access to documents seized in criminal proceedings

A complainant objected to the fact that the National Tax and Customs Administration (hereinafter: NAV) did not fulfil his request for data of public interest when he wished to access documents seized in relation to the financial management of a municipality. When contacted by the Authority, NAV presented that with regard to the documents and data requested by the petitioner, the controller is the municipality, while NAV is the authority conducting the investigation in the case, and holds the documents as documents seized as evidence in accordance with the rules of Act CX of 2017 on Criminal Procedures (hereinafter: Criminal Procedures Act). Pursuant to Section 110(1) of the Criminal Procedures Act, information can be provided to whoever has a legal interest in the conduct of the procedure or its outcome; according to their position, the request for data of public interest by the petitioner cannot be regarded as a legal interest. Pursuant to Section 110(2) of the Criminal Procedures Act, permission to access the documents of the case or disclose of the requested information is authorised by the head of the public prosecutor's office before indictment and by the chair of the court acting in the case thereafter, once legal interest is verified. In view of this, even if the petitioner verified his legal interest, NAV would not be authorised to issue the documents, of which only the head of the public prosecutor's office could decide. NAV also explained that based on Section 313(3) of the Criminal Procedures Act, the municipality subject to the seizure is entitled to access the documents seized in the course of the criminal procedure in part or in full and to produce copies thereof to the extent and for the time necessary for the discharge of its tasks. In view of this, there is an opportunity for the municipality to request the investigative authority to access documents and to prepare copies, if it does not hold the hard copies or electronic copies of the documents constitut-

24 Pursuant to Article 46(4) of Act CXXVIII of 2011 on Disaster Management and the Amendment of Certain Related Acts, *"in an emergency, the duties and powers of the body of representatives of the municipal government, the metropolitan and county assemblies shall be exercised by the mayor, the Lord Mayor or the President of the county assembly. In this context, he may not take a position on the reorganisation, closure, scope of supply or services of a local government institution if the service also affects the municipality."*

ing the subject matter of the procedure for the purpose of meetings its obligation to issue data of public interest. This means that the controller municipality is authorised to issue the data of public interest or data accessible on public interest grounds included in the documents, but the municipality has to contact the investigative authority to see whether the issue of the requested data violates the public interest in successfully completing the criminal procedure. In the given case, the investigative authority stated that with respect to a certain part of the data, the interests of the investigation in progress would be substantially jeopardised based on the Privacy Act and Section 109(1)(e) of the Criminal Procedures Act, if the public was informed earlier of the relevant data than the persons affected in the criminal procedure. With regard to another part of the data (the contracts concluded by the municipality), the public interest in successfully completing the criminal procedure would not be violated by access to the data of public interest.

According to the governing court case law (Pfv. IV. 20.455/2015/4., 2.Pf.20.559/2011), the mere fact in relation to the data of public interest processed in the course of a criminal procedure that the investigation report requested to be issued containing data of public interest undisputedly processed by the organ discharging public duties was requested by the investigative authority and thus it became part of the criminal file may not automatically mean a restriction of access and the rejection of the request for data of public interest. The documents requested to be issued through the request for data of public interest were obviously not generated in the criminal procedure, instead they were the basis for lodging a report. The quality of independent data processed by the controller should not be influenced by the fact that they were used in a procedure. At the same time, they do not have the uniqueness, that would preclude disposal over these data because of their use in criminal proceedings.. The controller may not refer to the interests of a procedure conducted by a third person in relation to documents containing information in the public interest, because there is no legal regulation that would prohibit the issue of documents used in the given procedure but not generated in the same procedure by the original controller in response to a request for data of public interest. Therefore, the mere fact that simply because the data of public interest requested to be issued was seized and used in a criminal procedure does not mean that the data would lose its character of being in the public interest, hence it is not possible to restrict access to them and to reject their request for data by automatic reference to this,.

As according to NAV's statement, public interest in the successful completion of the criminal procedure would not be violated by public access to the contract requested by way of the request for data of public interest, these data can be accessed by the public and the municipality may request the investigative authority to make copies of the seized documents, the Authority called upon the municipality concerned to make the requested data available to the petitioner, unless there are other factors lawfully restricting public access. Having asked for copies of the documents requested in the request for data of public interest, the municipality sent the documents to the petitioner. (*NAIH-4003/2021*)

III.11. Public disclosure of environmental information

In the case of data on the environment, the protection of trade secrets is a highly frequent reference for restricting access. An association for the protection of the environment requested the documents Noise map and Action plan to reduce noise of the local gigantic plant from the county government office. Fulfilling the data request was rejected with reference to the protection of trade secrets (the cover sheet of the Noise map says that "The documentation contains information qualifying as trade secrets" and the header of each page included that "For use by the authorities only"), at the same time, nobody disputed that the Noise map contained data of public interest or data accessible on public interest grounds. According to the principle set forth in Section 30(1) of the Privacy Act and the consistent practice of the Authority and the courts, declaring entire documents automatically as trade secrets is unacceptable, instead the document must be examined and it must be established exactly which data count as trade secrets. Based on Article 4(4) of the Aarhus Convention promulgated with Section 2 of Act LXXXI of 2001 on the Promulgation of the Aarhus Convention, a request for environmental information may be refused, if the disclosure would adversely affect the confidentiality of commercial and industrial information where such confidentiality is protected by law in the light of a legitimate economic interest, in this context, however, information on emissions, which is relevant for the protection of the environment, must be disclosed, or the interests of a third party, which has supplied requested information without being under a duty or legal obligation to so , or giving consent to the release of the material.

However, these reasons are to be interpreted stricto sensu, taking into account the public interest in accessibility, as well as to what extent the information requested relates to emissions to the environment. The government office has therefore to consider the collision between the protection of the interest of the public and the protection of private interest. Section 30(5) of the Privacy Act states that the grounds for refusal must be interpreted restrictively and the request for access to data of public interest shall only be refused, if the underlying

public interest outweighs the public interest of allowing access to the data of public interest (overriding public interest test). Therefore, the government office violated the right of the notifier to access data of public interest and data accessible on public interest grounds, when it failed to fulfil the request for the action plan and furthermore when it automatically qualified the entire Noise map as a trade secret without its detailed examination, hence it could not possibly have carried out the assessment of data qualifying as trade secrets as required in Section 30(5) of the Privacy Act; for these reasons the Authority called upon it to immediately send the Action plan to the notifier and establish exactly which data of the Noise map qualify as trade secrets, if necessary, invite the statement of the company concerned and carry out the assessment as required in Section 30(5) of the Privacy Act, and comply with the request for data for which, as a result of the foregoing assessment, it concludes that disclosure cannot be restricted. The government office complied with the Authority's call and issued the Action plan to the notifier together with the public version of the Noise map, which is almost identical with the original version. (*NAIH-4011/2021*)

The Authority took successful action in two cases where environmental NGOs objected to the cost reimbursement charged for fulfilling their data requests. In the first case, the fact that the NGO requesting the data asked for environmental information from the competent government office paid an important role. The Authority found the cost reimbursement of 185,321 forints unjustified for several reasons. By far the greater part of the requested documents contained information concerning emissions to the environment, access to which according to Section 12(5) of Act LIII of 1995 on the General Rules of the Protection of the Environment cannot be refused on the grounds of being trade secrets. Furthermore, the 47 working hours calculated for filtering out inaccessible data in the documents requested by the petitioner was unjustified because the requested documents in actual fact contained very few pages where personal data could occur (they included largely tables, measurement data and protocols and the examination of such pages could not possibly take about 4 minutes per page). Finally, even in the case of expending 47 working hours as alleged, the disproportionate use of labour necessary for the discharge of the basic activities of the government office would not take place in view of the huge headcount of the government office. In its call, the Authority explained that if responding to data requests to be fulfilled causes disproportionate difficulties for an organisational unit while carrying out its basic activities, then first – if possible, particularly in the case of larger organisations – a solution to discharging both the basic activities and the free fulfilment of data requests has to be resolved through reorganisation within the organ. *(NAIH-5797/2021*)

In the case just presented, as well as in another case launched on the basis of the notification of another environmental NGO, unlawfully charging cost reimbursement was due, inter alia, to the wrong interpretation of the law according to which "if fulfilling a request for data of public interest exceeds 4 working hours that can be regarded as disproportionate". In its investigations, the Authority consistently underlines that the time taken to carry out a task qualifies as disproportionate not because it exceeds 4 hours, it is also necessary to make use of labour needed to discharging the basic activities to fulfil the data request and that should take place to a disproportionate extent. The use of labour is disproportionate, if it renders the discharge of the basic activities of the organ discharging public tasks substantially more difficult or impossible. (*NAIH-4508/2021*)

III.12. Publicity of applications

In 2021, there was a large number of complaints related to the transparency of investments and grants for the purposes of tourism. In the Authority's experience, the grounds for restricting access to applications was the recurrent reference to trade secrets or support for a decision.

III.12.1.Trade secret

A journalist requested from Kisfaludy2030 Turisztikai Fejlesztő Nonprofit Zrt. the entire application documentation of the winning applications on the decision list of projects winning grants in access of 1 billion forints and the development of high-capacity existing hotels and the establishment of new hotels. The company did not issue the data declaring them to be trade secrets. The company did not issue the list of the non-winning applications, not included in the decision list of *Kisfaludy accommodation development construction – Development of high-capacity existing hotels and the establishment of new hotels* (name of applicant, the identification of the project and the requested amount) to the notifier because in its view, no commitment according to Annex 1. Section III.4. of the Privacy Act took place

According to the consistent practice of the Authority and of the courts, the requested documents of the application must be examined one by one and established exactly which are data qualifying as trade secret, whose disclosure would give rise to disproportionate violation of interest. There is a substantial public in-

terest in the transparency of hotel development and hotel establishment applications and the application procedures involving substantial public funds are of great interest to the public, hence the public has a legitimate demand to have access to at least the basics on what taxpayers' money is spent, and whether the submitted applications meet the expectations published in the invitation to apply. The data requested on non-winning applications are also either data of public interest or data accessible on the grounds of public interest based on Section 3 of the State Aid Transparency Act.

Upon the Authority's call, the company finally asked the beneficiaries to provide information on which data of their application they qualify as trade secrets. In general, it was found that a very large number of the beneficiaries regarded the application datasheets, the executive summary of the business plan, the situation assessment, the objectives, the results expected, the section concerning the current status from the part presenting the project, the main figures of the project's budget and the scheduling of the project as accessible. In other words, the range of data assessed to be issuable by the beneficiaries was much wider than the range of data originally assessed as accessible to the public by the company – this was particularly spectacular in the case of the business plan.

As to fulfilling data requests in the future, the company has to draw the conclusion that instead of excluding public access to their full application documentation, the data thereof have to be examined in detail, statements of the beneficiaries have to be obtained, which is the only way to declare on reasonable grounds, public access to which data qualifying as trade secrets would result in disproportionate injury to commercial activities and all this has to be substantiated towards those requesting data with detailed justification. Finally, the company complied with the Authority's calls, however, the data never reached the person requesting them as his e-mail address changed in the meantime. The company did not send the data to the new e-mail address, because of this the Authority recommended that the person requesting the data submit the request again. (*NAIH-653/2021*)

There was another journalist, who submitted a request for data of public interest concerning the requests of specific companies sent to the invitation to participate in the Baross-19-NMG/2 project and their detailed documentation to CED Közép-európai Gazdaságfejlesztési Hálózat Nonprofit Kft. The company declared about all the application documentation that "they are not accessible to the public with regard to any of their parts". In its call, the Authority underlined that in addition to explaining which data of the requested application materials qualify as trade secret and why, it is also necessary to explain the disclosure of

which of the data qualifying as trade secret would cause disproportionate injury to the holder of the secrets. (*NAIH-6850/2021*)

III.12.2. Data for decision support

Organs discharging public duties frequently restrict access to data related to the evaluation of applications with reference to Section 27(5)-(6) of the Privacy Act, without giving adequately detailed justification for the refusal of the data request.

The mayor's office of a large rural town refused a data request on the application documentations, the number of those receiving personnel-related benefits in the projects and the amount of such benefits, justifying its refusal by referring to the relevant provision of the legislation only. In spite of being called upon by the Authority, they justified the restriction of access with regard to the blocked data as *"not relevant to the project"* in the documents subsequently sent to the person requesting the data. (*NAIH-1338/2021*)

The Authority called the attention of Emberi Erőforrás Támogatáskezelő (Human Resources Support Manager, hereinafter: EET) to the fact that the information provided to a person requesting data in relation to refusing to grant the request for data must contain the factual and legal reasons substantiating it. These reasons should be the results of examinations of form and content. A refusal supported with the appropriate reasons greatly contributes to the person requesting data becoming genuinely aware and understand why his request was not fulfilled. In addition, based on such information, he will be able to bring the right decision concerning an eventual legal remedy as well. The Authority established that EET did not act appropriately in refusing the request for data of public interest when it failed to provide a detailed justification. (*NAIH-272/2021*)

The Authority called the attention of the Ministry of Innovation and Technology (hereinafter: ITM) to the same issue in the case when the notifier complained that ITM did not fully meet his data requests related to OTKA applications submitted and evaluated in 2020. The data request concerned the list of applications reflecting the recommended order, submitted by OTKA main advisory board to ITM; also, the notifier requested the letters, memos and meeting protocols, which played a role in that the list of applications reflecting ITM's decision did not correspond with the list of applications submitted to ITM by the OTKA main advisory board. ITM justified the restriction of public access (already in the course of the investigation) by claiming that a public discussion on the collective profes-

sional opinion of expert groups would jeopardize the purity of future procedures and access to the internal correspondence concomitant with day-to-day operational work would jeopardise ITM's discharge of its tasks and exercise of its powers specified by law, free from unauthorized external influence and at the same time, the free expression of opinion by ITM employees when preparing for decisions, as well as the efficiency of the work in the future.

ITM failed to comply with the Authority's call; because of this, a NAIH report was published on the case[25], which underlined: access to the data on which decisions are founded can be restricted in properly justified cases; in the present case, however, substantial public interest was vested in the accessibility of the requested data, because the alteration of the order recommended by OTKA's main advisory board – and the usual procedural order – was of major interest to the public, as well as to the scientific community and the requested data were indispensable sources of the transparency of the procedure in this application procedure, particularly with regard to the protocols of meetings. Of the documents on which the decision was based, only the data concerning the methods of evaluation, the criteria of evaluation and the evaluation of the winning applications have to be issued and only those which would explain the differences from the order recommended by OTKA's main advisory board. The employees of organs discharging public tasks, acting within the responsibilities and powers of these organs, have good reason to expect that, since it is a principle laid down in the Fundamental Law, data concerning the method of evaluation of applications financed by public funds, the criteria of evaluation and the evaluation of the winning applications may be made accessible in the documents produced by them, particularly if they are the only sources of the requested information. (*NAIH-2329/2021*)

III.12.3. Disclosure of data concerning applications

A county self-government published a contract of support related to an EU application procedure, in which the name, position, signature, sign of the person signing the contract and the name, working place, phone number and e-mail address of the contact person were disclosed to the public. In its request for consultation, the self-government requested the Authority's statement whether the data subject signing the contract who was otherwise a senior employee of an organ discharging public tasks could request the blocking of the above data.

25 https://naih.hu/files/Infoszab_jelentes_NAIH-2329-2021.pdf

The person signing the contract representing an organ discharging public tasks carried out a public task when he signed the contract, hence the name, position, signature and sign of this person qualifies as personal data accessible on public interest grounds.

The name, working place, phone number and e-mail address of the contact person acting on behalf of the self-government can be regarded as data accessible on public interest grounds if he has a legal relationship of public service.

The publication of the contract containing personal data accessible on public interest grounds took place in accordance with the requirements of the Privacy Act, consequently the data subject may not request the blocking of these data. Act CXXII of 2009 on the More Economical Operation of Business Organisations in Public Ownership (hereinafter: Economical Operation Act) specifies the data, which the Széchenyi Programiroda Tanácsadó és Szolgáltató Nonprofit Kft. has to disclose. Based on Section 2(1) of the Economical Operation Act, the names, positions and signatures of the senior managers of this company are also data accessible on public interest grounds, while the data of the company's contact person have to be disclosed, if they were generated in relation to the discharge of public tasks, such as in this case in the course of concluding the contract. The Authority does not consider it necessary to display the contact data of the company's contact person on the website as. (*NAIH-6645/2021*)

A municipality intended to publish the records of contracts and applications of less than 5 million forints on the city's website in the form of individual disclosure and requested the Authority's position about its lawfulness. The Authority expounded that it greatly supports the decision of the municipality, regards it as exemplary from the viewpoint of enforcing the fundamental right to access data of public interest, and thinks that other municipalities should follow it. At the same time, it called attention to the fact that in the course of the disclosure, personal data, which do not qualify as data accessible on public interest grounds, classified data, data according to Act LIV of 2018 on the Protection of Trade Secrets and other data subject to restricted accessibility must be blocked. The Authority recommended that the decision be made by the municipality in the form of a municipal decree, perhaps within the same framework as the rules mandatorily enacted in accordance with Section 30(6) of the Privacy Act. (*NAIH-5630-2/2021*)

In another investigation, the complainant objected to the fact that the data concerning the Széchenyi 2020 project can only be downloaded in a limited way extending to 300 hits and not for the entire database on the website www.palyazat.

gov.hu in the supported project search function, hence he requested specific data of all the Széchenyi 2020 projects (operative programme, sub-measure, name of the applicant, project name, project description, settlement, date of the decision to support, brief summary of the project, aid awarded, source, country, intervention category, EU co-financing rate, total cost of the project, commencement and end of implementation) to be sent in .csv format.

The Prime Minister's Office refused to fulfil the request, because according to their position, the data request was governed by a statement in Constitutional Court Decision 13/2019 (IV.8) AB, according to which the controller is not under an obligation to create a new set of data filtered according to specific criteria and the person requesting the data may not demand that somebody else should collate the accessible data for him. According to the position of the Authority, however, Section 33(1) of the Privacy Act stipulates that access to data of the public interest, the publication of which is mandatory, shall be made available to the general public without personal identification on the internet website, without any restriction, in digital format, suitable for being printed or copied, without any partial loss or distortion of data, free of charge including perusal, downloading, printing, copying and transmitting through a network. (*NAIH-4539-13/2021*)

A Member of the European Parliament submitted a data request to Magyar Turisztikai Ügynökség Zrt. on which providers of accommodation benefited from the aid provided pursuant Government Decree 523/2020. (XI. 25.) on the partial compensation to accommodation providers for loss of revenue arising from to cancelled reservations and to what extent.

The company indicated the accessible source of the data, which is a list of beneficiaries, which included the beneficiaries of other applications also. The company gave the criteria of collation to the person requesting the data as follows: *"The data requested by the person can be collated from the list concerning the circle of applicants, objective and amounts of other support provided by Kisfaludy 2030 Turisztikai Fejlesztő Zrt., taking into account that the data that can be read from the invitations to apply published also on the website referred to"*.

In its call, the Authority underlined that it is not an obligation for the person requesting the data to search for the document, in which he may find the criteria on the basis of which, he may collate the requested data. If the person requesting the data is directed to a public data set, he must also be given unambiguous criteria for collation whereby he can select the requested data from the data set without consideration, simply and unambiguously. The Authority also emphasized that the accessibility of information concerning who gets public funds and how much as "basic data" relating to the spending of public funds is above any dispute. Finally, the company issued the requested data to the person who requested them in accordance with the Authority's calls. (*NAIH-2361/2021*)

III.13. Preparation for legislation

In 2021, NAIH received a group notification from a complainant, who objected to the practice of ten ministries in fulfilling data request on the one hand, and the 45-day deadline for providing information applicable during the period of the epidemic, on the other hand. Originally, the notifier requested the various ministries to disclose impact assessment reports concerning legal regulations relating to the 2014-2018 governmental cycle, as well as other impact assessment documents. Based on Decree 2/2016. (IV. 29.) MvM by the Prime Minister's Office on preliminary and subsequent impact assessments, an impact assessment is a process of collecting and analysing information whose primary goal is to improve the efficiency of regulation, including the examination of the likely consequences of the regulation, in sufficient detail adjusted to the assumed impacts of the regulation over a relevant time horizon and then summarising the results with a view to facilitating informed decision-making.

The ministries did not make the requested documents accessible. In their respective responses to being contacted by the Authority, it can be established that the Ministry of Human Resources, the Ministry of Justice, the Prime Minister's Cabinet Office and the Ministry of Foreign Affairs and Trade did not have the data of public interest requested by the notifier as they did not compile impact assessment reports.

The Ministry of the Interior argues that, based on assessing public interest in accessing the data and in excluding their accessibility, the content of the impact assessment reports also influences the decision-making processes of the legislator concerned, the minister and the Government, and these processes cannot be regarded as closed by the end of a year because in such cases, an informed decision can only be made through the comparison of data over several years and experiences, hence the data cannot be made available to the public even in their quantitative aspects. NAIH did not accept this justification as the impact assessment reports only contain aggregated statistics for the given year, the practical experiences concerning the preparation, use and utilisation of impact assessments and recommendations concerning the improvement of impact as-

sessment activities. Therefore, they should not be considered as a basis for one or more government decisions, particularly since the statistics are not used as a basis for decision-making or legislation.

The Prime Minister's Office refused to issue the impact assessment reports claiming that the data in the impact assessment reports qualify as data supporting the decisions related to the operation and improvement of the impact assessment system.

The Authority issued a report in the case based on Section 59(1) of the Privacy Act, particularly in view of the fact that the contacted ministries exhibited substantially different practices as learned in relation to the case under study.[26]

26 https://naih.hu/files/Infoszab_jelentes_NAIH_1227_7_2021.pdf

IV. Supervision of data classification, classified data and data with restricted access

In the course of the procedure of the secret supervisory authority, the establishment of the facts of the case means that the lawfulness of the classification of national classified data is checked. Classification means not only the decision of the classifier, but the entire classification procedure. The lawfulness of the classification of national classified data also includes that, following the classification procedure, the processing of the national classified data complies with the relevant legal regulations during the period of the validity of the classification. In addition, following the classification procedure, additional facts and circumstances may also influence the lawfulness of the classification of the data, such as the review of the classification by the classifier or its omission, or the possible disclosure of the data.

The classification is lawful if it complies with the formal and procedural rules set forth in Act CLV of 2009 on the Protection of Classified Data (hereinafter: Classified Data Act) and its implementing regulations, the principles of the Classified Data Act (Section 2 of the Act), the rules of classification (Sections 5 and 6 of the Act) and furthermore – as pointed out by Section 1 of Constitutional Court Decision 29/2014. (IX. 30.) AB –it is a requirement from the point of view of content that the classifier, when deciding whether to classify data of public interest or data accessible on public interest grounds, should take into account the public interest in the accessibility of the data to be classified in addition to the public interest in classification, and it should decide on the classification of the data only if the purpose to be achieved through classification is proportionate to the interest in the accessibility of the classified data.

IV.1. Lack of classification marking as defined in the legislation on classification of national classified information, succession of classifiers, review of classified information

In a lawsuit in front of the Fővárosi Törvényszék (Municipal Court of Budapest), the petitioner submitted a petition against the Prime Minister's Office as defendant requesting access to data of public interest. The Prime Minister's Office rejected the petitioner's request for data of public interest, citing the fact that the data were classified.

The Municipal Court of Budapest decided to suspend the hearing and in its warrant sent to the Authority initiated the Authority's secret supervisory procedure based on Section 31(6a) of the Privacy Act in relation to the lawsuit in progress in front of the Municipal Court of Budapest requesting the disclosure of data of public interest.

Upon the initiative of the court, the Authority launched its secret supervisory procedure to examine the lawfulness of the classification of national classified data.

Pursuant to Section 3(1)(a) of the Classified Data Act, data can be regarded as national classified data, if it contains the classification marking in accordance with the formal requirements set forth in the Classified Data Act and its implementing decree. Section 6(7) of the Classified Data Act provides that national classified data comes into being through classification by the classifier. For national classified data to come into being, the formal requirements of the classification marking must also be complied with.

Based on Section 3(1)(a) and Section 6(7) of the Classified Data Act, the Authority found an infringement of the legal regulations pertaining to the classification of national classified data as one of the documents constituting the subject matter of this case did not include the classification marking specified in the legal regulations concerning the classification of national classified data. In view of this, the Authority warned the classifier not to process the data on the data carrier examined as classified data because in their case the classification has not come into being because of a formal error.

With regard to the data carriers containing additional classified data constituting the subject matter of the procedure, the Authority established that based on the available documents, the classifier acted in accordance with the formal and procedural requirements of the legal regulations applicable to the classification of national classified data when it conducted a classification procedure with regard to the data concerned upon the generation of the data.

In the meantime, the classifier of the classified data constituting the subject matter of the procedure of the secret supervisory authority was replaced through legal succession. Pursuant to Section 8(1)-(2) of the Classified Data Act, the classifier has to review the national classified data produced by him, his legal predecessor or other classifier and falling within his remit and powers at the time of the review at least every five years, unless a shorter time limit is provided by law.

The classifier may involve an expert in the review. As a result of the review, the classifier or his legal successor shall:

a) maintain the classification of the national classified data within his remit and powers; if the conditions for its classification continue to obtain;

b) reduce the level of classification or modify the validity period of the classification, if there were changes in the conditions of classification;

c) terminate the classification, if its conditions no longer obtain.

The classifier carried out the review of the classified data in accordance with Section 8(1) of the Classified Data Act and reduced the level of classification to "Confidential" and also modified the period of validity of the classification accordingly. In accordance with Section 6(8) of the Classified Data Act, the classifier provided detailed justification for the classification of the data. The public interests necessitating the classification are Hungary's central financial and commercial activities, foreign affairs and international relations and ensuring the smooth functioning of its state free from undue influence as stated in Section 5(1)(d), (e) and (f) of the Classified Data Act. According to the justification provided by the classifier, the "Confidential" level of classification was established on the basis of Annex 1, Section 3 of the Classified Data Act, in view of the fact that *"the data of the legal relationship protected by classification becoming available to the public would have damaging consequences for Hungary's international relations, the states concerned in the legal relationship and for foreign relations globally and the economic activities of the country and it would make the discharge of the legitimate tasks of the state more difficult"*. Applying the severity/probability test the classifier arrived at the conclusion in the course of the classification review that accessibility of the data related to the legal relationship beyond the circle of the data manager would jeopardize the public interests to be protected through the classification. The Authority accepted the classifier's position and established that the classifier correctly arrived at the decision that the classification of the data needs to be continued, but the level of protection can be reduced to the "Confidential" level, because the interests in keeping the data secret can be ensured by this level of classification.

IV.2. Examination of the classification of the data processed by the Hungarian National Asset Management Inc. in the proceedings initiated by the Municipal Court of Budapest

In its transcript received by the Authority on 25 April 2016, the Municipal Court of Budapest initiated the secret supervisory authority procedure in relation to a lawsuit concerning a request to access data of public interest in progress before the Court. The subject matter of the lawsuit in progress before the Court was the following: the petitioner submitted a petition against the Hungarian National Asset Management Inc. (MNV) requesting access to data of public interest, in which he presented that he had submitted a request for data of public interest to the defendant, who had, however, informed him that the data requested by him were national classified data, hence it would refuse to disclose them.

The petitioner requested the Court to order the defendant to disclose the data requested by him, namely:

- Has MNV ever held, directly or indirectly, a bond bearing the XS0867086042 ISIN code?
- If so, what was its value?
- Who did they buy it from and for how much?
- Why did they obtain it?
- If they sold it on, who to and what did they get for it?

In its counter-petition, the defendant put forward the following argument about the reasons for refusing the data request as follows: pursuant to Section 3(1) of the Classified Data Act, it has to treat all the data, from which the data request could be answered or fulfilled, as national classified data. The data necessary to answer the data request are included in two resolutions to exercise shareholder's rights (hereinafter: RES) issued by the Ministry of National Development.

In accordance with the initiative of the Municipal Court of Budapest, the Authority launched its secret supervisory procedure. The subject matter of this procedure of the Authority was to check whether the classification of the national classified data was lawful. The procedure concerned those of the data constituting the subject matter of a lawsuit in progress before the Municipal Court of Budapest, of which MNV claimed that they were national classified data.

In this case, the Authority made use of a forensic expert and it brought its decision based on the opinion of the forensic expert and the classifier as client. First,

dr. Gábor Czepek, Administrative State Secretary of the Ministry for National Development took action as client in the procedure, then Andrea Bártfai-Mager, minister without portfolio in charge of the management of national assets, took over acting within the powers of the classifier later in the procedure.

In the course of its procedure, the Authority established that the RES referred to by the Ministry for National Development contained "For restricted distribution" national classified data and in the course of the classification of the RES of the cited number, the classifier acted in accordance with the legal regulations applicable to the classification of national classified data. The Authority provided for all this in a decision marked a "For restricted distribution", which included the justification of the decision, as well as additional details of the case. The Authority communicated its decision to the classifier, who did not challenge it within the 60-day period provided for this in the Privacy Act. (*NAIH-2262/2021.*)

IV.3. Examination of the classification of data concerning the procurement of military equipment of the Hungarian Defence Forces in the Authority's secret supervisory procedure initiated by the Municipal Court of Budapest

The Municipal Court of Budapest, in a pending litigation on the disclosure of data of public interest, initiated the Authority's secret supervisory procedure, while suspending the procedure and forwarding the documents of the litigationt.

The subject matter of the litigation was data concerning the procurement of military equipment affecting the capability development of the Hungarian Defence Forces within the framework of the Zrínyi 2026 Defence and Armed Forces Development Program, which became classified data as a result of five separate classification procedures, because of which the Authority had to examine the lawfulness of the classification of the various data in five separate secret supervisory procedurest.

The documents containing the individual classified data had been marked by file number by the defendant during the proceedings that were included in the case files of the lawsuit forwarded by the Municipal Court of Budapest. First, the Authority had to exactly identify the persons conducting the various classification procedures, because the client in the Authority's secret supervisory procedure is the classifier.

With regard to the data constituting the subject matter of the litigation, one classification procedure was conducted by the Administrative State Secretary of the Ministry of Defence, two by the Director General of the Office for Defence Economy in the Ministry of Defence, another one by the deputy head of the Department for Military Equipment Development at the Ministry of Defence, and one by one of the heads of department of the Military National Security Service.

In three of the five secret supervisory procedures, the person exercising the powers of the classifier and consequently the client in the Authority's procedure was changed because of the change in the person in the given position. The powers of the classifier are always linked to the discharge of the given public task, hence to the person whoever fills in that position or to a person filling the position from time to time, to whom the classifier transferred these powers in accordance with the legal regulations.

In another procedure, the person exercising the powers of the classifier, hence the client in the procedure remained the same, because he continues to be responsible for discharging the given public task, but as a result of the transformation of the organisation of the Hungarian Defence Forces, he holds these powers because of his position now filled in at another organisational unit of the Hungarian Defence Forces.

Pursuant to Section 63(1) of the Privacy Act, the Authority may opt for one of the following two decisions in its order in the course of the secret supervisory procedure:

) it may require the classifier to change the classification level or the period of applicability of the national classified data in accordance with the law or to declassify the information in the event a breach of the law on the classification of national classified data is found; or

b) it finds that the classifier has acted in accordance with the national legislation on classification of classified data.

AThe Authority found in the five secret supervisory authority procedures in question that the classifier acted in accordance with the legislation on the classification of national classified data..

The following specific features should be highlighted in connection with procedures referred to:

Of the five secret supervisory procedures, only one classifier, the head of department of the Military National Security Service (hereinafter: KNBSZ), sent the copies of document containing the data constituting the subject matter of the Authority's procedure, so that it included the entire data content of the original documents concerned.

The KNBSZ head of department classified the data in the generated document to be protected at the lowest classification level, i.e. "For restricted distribution" as a result of the classification procedure conducted, with a validity period not reaching the maximum of the validity period for this classification level. The classifier sent a detailed justification for the classification of the data with regard to the criteria set out in the Authority's order, and enclosed the copies of the documents.

According to the detailed justification of the classification, the data concerning the long-term development of the Hungarian Defence Forces influencing the future security situation of Hungary and the data presenting the situation providing the grounds for capability development are to be protected with the classification. The classifier indicated Hungary's defence and national security activities based on Section 5(1)(c) of the Classified Data Act as the public interest necessitating the classification.

As to why and how would disclosure of the classified data within the validity period, or access to them by unauthorized persons influence detrimentally the public interest to be protected with the classification, the classifier argued as follows:

"The circumstances decisively influencing Hungary's security and military defence capabilities require the development of military capabilities, for which a survey of the existing capabilities is indispensable. Disclosure of the data protected with the classification within the validity period or access to them by unauthorized persons would upset the operation of the Hungarian Defence Forces and would adversely affect its development, consequently it would adversely affect Hungary's security."

By way of a detailed justification of determining the classification level, he presented that the use of the "For restricted distribution" rating is warranted, because disclosure of the data within the period of validity, their unauthorized acquisition, modification or use, making them accessible to unauthorized persons or inaccessible to authorised persons would have a detrimental impact on defence interests. Disclosure of the need for capability development and its military assessment or making them accessible to parties with opposing interests

would allow the activities of the Hungarian Defence Forces to be substantially hampered, reducing the effectiveness of defence activities.

In the detailed justification for the validity period of the classification he mentioned that the maintenance of the classification for the validity period determined by him was justified because the data concerning the background to the specific development and the procedural order supporting it and the conclusions that may be drawn from them during the development in progress could have a negative influence on Hungary's defence interests.

Of the data involved in the five secret supervisory procedures, the data subject to this classification provide, in fact, a brief, not very detailed presentation of the situation that underpins the need for capability development against the background of the acquisition of military equipment. In the Authority's assessment, this also confirmed that, in contrast to the qualification of additional data on the details of this capability development in the other four procedures, it was sufficient in this case to apply the lowest qualification level by setting a shorter validity period than the maximum.

In justifying, why the public interest underpinning the classification is of greater weight than the public interest in accessing the data, the classifier claimed that disclosure of data that concern the capability development of the Hungarian Defence Forces and underpin it by an unauthorized party prior to the expiry of the validity period would result in a security risk. Because of the disproportionately greater injury to the defence interests, it is warranted to exclude the data from access on the grounds of public interest with this classification. He also mentioned that the public interest in accessing data will only be delayed; inspecting the documents during the classifications period of validity can be ensured for those authorized to do so with the appropriate restrictions.

With regard to the data classified by the KNBSZ head of department, the Authority was able to directly satisfy itself that the classifier complied with the formal and procedural requirements of the legal regulations concerning the classification of national classified data in the course of the classification procedure. Having inspected the document copies sent, the Authority established that it only contained the data types indicated in the detailed justification and it did not include other data with repeated classification markings.

In the other four procedures, the classifier sent the requested document copies to the Authority blocking a substantial part of the data content. This was justified by reference to the fact that they contained data subject to Section 71(3) of the Privacy Act, because this was a document according to Section 23(1)(a) of Act CXI of 2011 on the Commissioner for Fundamental Rights (hereinafter: Ombudsman Act) concerning a defence investment of outstanding importance for Hungary's defence and the development of the defence capabilities, of which the fact of the investment and of the essence of the development can be learned. In view of this, based on Section 71(3c) of the Privacy Act, they sent the document copies by making the data illegible, which the Authority is not authorized to access.

As in these four procedures, the clients made the content of the documents available to the Authority only by blocking a major and essential part of their content, the Authority was not able to learn the classified data to be examined to draw conclusions as to the lawfulness of the classification from them, or to make statements by way of direct inspection and perusal. According to the regulations in force, the Authority may invite the minister having the relevant responsibilities to examine the documents in its secret supervisory procedure under Section 71(3) of the Privacy Act and Section 23(7) of Ombudsman Act, hence in the four procedures mentioned the Authority called upon the minister to examine in detail the data content of the documents not accessible to the Authority.

In this procedure, the conclusions and statements of the Authority are based on the examination of the document's content by the Minister of Defence and the information sent by him to the Authority on its result with regard to most issues. The Authority was forced also to rely on the statement of the minister concerning the issue that the blocked parts of the documents contain the type of data and only those types of data direct access to which by the Authority is not permitted by law.

Also, in the case of these four secret supervisory procedures, the Authority arrived at the conclusion that the classifier acted in accordance with the formal and procedural requirements of the legal regulations concerning classification in the course of the classification procedure.

In examining the data content and classification of the blocked documents, it was of fundamental significance to assess whether all the parts of the data content of the documents under study contained classified data and whether there were other classified data among the data in the documents. If there are other classified data in the document, then the Authority has to examine their identification, separability and the use of repeated classification markings.

The examination of this is also of outstanding importance because data classified by other classifiers in additional documents constituting the subject matter of the litigation referred to above are closely related, in some cases they are of identical nature and subject matter. Nevertheless, different classification levels ("Secret", "Confidential" or even "For restricted distribution") and different validity periods were specified for the data in them.

Because of the substantial amount of the blocked data, the Authority was unable to directly determine whether the data in the documents containing data of different classifications (with regard to which separate secret supervisory procedures were launched) were identical; however, it drew the conclusion from the detailed justifications sent by the various classifiers in response to the call of the Authority that some of the classified data in the various documents might even be the same.

This question is essential from the viewpoint of adjudging the lawfulness of the classification, because if it can be established that several classifiers conducted classification procedures for the very same data in parallel, while setting different classification levels and validity periods as a result of these procedures, this would imply that at least one of the parallel classifications is not in line with the conditions of classification set forth in the Classified Data Act.

In order to enable the Authority to make a correct and informed decision through the ministerial examination of the data content inaccessible to the Authority, the Authority attempted to specify the criteria of the examination to be carried out by the minister in as much detail as possible taking everything into account for the minister when inviting him to carry out the examination.

In its warrants concerning all the four procedures in which the Authority had to invite the minister to carry out the examination, the Authority referred to the documents containing data classified by other classifiers constituting the subject matter of the litigation, informing the minister of defence about where they can be found.

In accordance with the Authority's request, the examination of the minister of defence therefore also extended to whether data classified in the course of another classification procedure were included in the document and if so, whether the identifiability and separability of the repeatedly classified data was ensured. Furthermore, in accordance with the call of the Authority, it also extended to whether the damage caused by an eventual breach of secrecy in view of the data

content would indeed reach the damage threshold associated with the classification according to Annex 2 of the Classified Data Act.

As to the results of his examination, the minister declared in all four cases that the documents examined by him did not contain any classified data that were classified earlier by another classifier. The damage caused by an eventual breach of secrecy reached the damage threshold associated with the given level of classification and the maintenance of the validity period established in the cases of the individual classifications were indispensable for the defence of the public interest indicated in the detailed justifications sent by the classifier to the Authority.

Pursuant to Section 1 of Constitutional Court Decision 29/2014. (IX. 30.) AB, it is a constitutional requirement arising from Article VI(2) of the Fundamental Law, the right to the freedom of information, that the classifier when making the decision on the classification of data of public interest or data accessible on public interest grounds should also take into account, in addition to the public interest in classification, the public interest in the accessibility of the data to be classified and decide on the classification of the data only if the purpose to be achieved by classification is proportionate to the public interest in the accessibility of the classified data. In other words, when making the classification, the weight of the interest underlying classification must be assessed against that of the public interest in the accessibility of the data.

Article 39 of the Fundamental Law applies to public funds. Pursuant to Article 39(2) of the Fundamental Law, every organisation managing public funds must account for its management of public funds in public. Public funds and national assets must be managed according to the principles of transparency and the purity of public life. Data relating to public funds and national assets constitute data of public interest. The Fundamental Law also specifies the requirement of the proper use of budgetary revenues at the level of the Fundamental Law by excluding the possibility of granting budgetary support to an organisation for free or for remuneration whose organisational or operational structure does not allow the lawful and justified use of public funds to be monitored and the path of the budgetary resources to be traced.

The Fundamental Law lays down the requirement of transparent management for both national assets and public funds, ensuring public access to them by classifying the data on them as data of public interest.

As regards the other public interest taken into account in the qualification, it should be emphasised that Article 45 of the Fundamental Law positions the Hungarian Defence Forces within the state organisational system. According to the functional definition, the basic tasks of the Hungarian Defence Forces are the military defence of Hungary's independence, territorial integrity and borders, the performance of joint defence and peacekeeping tasks arising from international treaties, and the performance of humanitarian activities in accordance with the rules of international law. In view of the unfortunate environmental and elemental disasters of recent decades, the tasks of the Hungarian Defence Forces also include participating in the prevention of disasters and the removal and elimination of the consequences of disasters.

In their detailed justifications, the classifiers explained in what respects, what harm could be caused by the disclosure of the data or access to them by unauthorised persons. The points made therein referred to the possible consequences on the basis of which the damage according to the corresponding point in Annex 1 of the Act on the Protection of Classified Data, relevant for the given level of classification, is assessed.

So, for example:

"It impedes or substantially hinders the proper functioning of the Hungarian Defence Forces, directly violates the interests of Hungary as defined by law, involves serious harm to the security of its citizens, significantly hinders the effectiveness of the defence activities, causes tension in Hungary's relations with other countries, and in the common security interests of Hungary with allied Member States."

"This directly violates the interests of Hungary as defined by law, involves serious harm to the security of its citizens, and significantly hinders the effectiveness of the defence activity, since the proper functioning of the Hungarian Defence Forces, which is the foundation of Hungary's sovereignty and the security of its citizens, requires the development of military capabilities based on the threats and the resulting capability requirements, in accordance with military criteria, free from external influencing factors. The need for capability development, or the disclosure of the professional assessment of soldiers to the public or to the knowledge of adverse parties, would also point to a vulnerability that would allow the activities of the Hungarian Defence Forces to be substantially impeded and hampered, reducing the effectiveness of the defence activity, seriously compromising the security of citizens."

With regard to the need to apply the classification level, the Authority, also relying on the findings of the ministerial inquiry, accepted, in the absence of knowledge of the specific data, that the detailed justification for the classifications was also correct in this respect and that the damage caused by the breach of secrecy in relation to the specific data in the document (which the Authority was not able to ascertain) would indeed reach the damage threshold for the classification level set out in the corresponding point of Annex 1 to the Act on the Protection of Classified Data.

In each of the procedures requiring ministerial examination, the Authority also made reference for the Minister of Defence to what appeared to be contradictory elements in the detailed justifications of the individual classifications. In the light of this, the Minister did not find any illegality in the examination of each classified data in relation to the level or the period of validity of the classifications.

The Authority only had at its disposal the statements made as a result of the ministerial examinations and the detailed justifications for the classifications given by the classifiers. Under the current legal framework, the Authority is not in a position to assess them against other evidence. Consequently, the Minister's statements on the data examined, in the light of the criteria set by the Authority, were accepted as evidence. On this basis, the Authority concluded that the qualification procedures were lawful.

General comments on the Authority's decision based on the findings of the ministerial examination under the current legislation, in view of the data content that cannot be disclosed to the Authority:

Pursuant to Article VI(3) of the Fundamental Law of Hungary, everyone has the right to the protection of his or her personal data and to accessing and disseminating data of public interest. Pursuant to Article VI(4) of the Fundamental Law, the enforcement of the right to the protection of personal data and access to data of public interest is supervised by an independent authority established by a cardinal law. This independent authority is the Nemzeti Adatvédelmi és Információszabadság Hatóság (Hungarian National Authority for Data Protection and Freedom of Information).

While the Fundamental Law protects personal data, it aims to ensure access and dissemination in the case of data of public interest, which is a prerequisite for participation in public affairs and public life. This has been confirmed by the Constitutional Court, which has ruled that free access to data of public interest

enables the control of the legality and efficiency of elected representative bodies, the executive and public administration, and it stimulates their democratic functioning. Because of the complexity of public affairs, citizens' control and influence over public decision-making and management can only be effective if the relevant bodies disclose the necessary information. [Decision 32/1992 (V. 29.) AB]

The importance of the Authority's independent monitoring role in the context of the Authority's secret supervisory procedure is also underlined by the fact that in the case of the above-mentioned secret supervisory procedures, the Authority's procedures were initiated on the basis of rules (see Section 31(6a) of the Privacy Act and Section 62(1a) of the Privacy Act) which were inserted into the Privacy Act because the Constitutional Court had previously held in Point 1 of its Decision No 4/2015 (II.13.) AB that there was an infringement of the Fundamental Law in the form of an omission due to the fact that, in the case of the classification of data of public interest or data accessible on the grounds of public interest, the legislator had not ensured that the fundamental right to access data of public interest [Article VI(2) of the Fundamental Law] could be directly enforced in the face of this restriction of public access by means of a procedure for reviewing the content of the data classification.

Contrary to the constitutional expectations described above, Sections 71(3)-(3c) of the Privacy Act currently in force deny the possibility from the Authority of accessing certain data as defined therein. These rules preclude the Authority, as an independent external supervisory body, from clarifying the facts in the context of the exercise of the right to the protection of personal data and the right of access to data of public interest by direct experience and knowledge of the data subject to the restriction on access. Instead, it must base a significant part of the answers to the questions raised in the course of clarifying the facts of the case on the outcome of the investigation carried out by the minister in charge. By virtue of his position, the minister in charge cannot be regarded as an independent external supervisory body since, in the present cases, he had to investigate the lawfulness of classification by a classifier acting under his delegated powers of classification. (In applying Section 71(3)-(3c) of the Privacy Act, a situation could arise ad absurdum where the minister in charge would have to carry out the investigation required by the Authority in his own case, i.e. regarding the lawfulness of a classification previously carried out by him, and the Authority would have to form an opinion on the lawfulness of the processing based on this.)

However, as a law enforcement body, the Authority must act in accordance with the legislation in force, and therefore it can adopt its decisions on the basis of the ministerial examination in such cases. (*NAIH-3532/2021; NAIH-4558/2021; NAIH-7913/2021; NAIH-7914/2021; NAIH-7915/2021.*)

V. Cases of litigation for the Authority

In 2021, the Authority had altogether 39 closed cases of administrative litigation at the Municipal Court of Budapest and the Curia.

Of these, the Authority won 26 cases in 100%, the court rejected the petition in 5 cases and terminated 2 lawsuits, the Authority partially won 3 lawsuits and lost litigation in 3 cases only.

Based on the Authority's experience with litigation, it can be stated that the emphasis of litigation shifted towards administrative lawsuits following data protection procedures launched upon request. It can also be established that administrative courts have to respond to increasingly complex and wide-ranging legal issues concerning data protection after the procedures of the data protection authority.

Challenging the data protection decisions induced by the Covid-19 pandemic can also be found among the administrative lawsuits arising typically from data breaches affecting the processing of health-related data. Because of contesting such decisions, there are several lawsuits in progress before the Municipal Court of Budapest, which began in 2021.

In line with the increasing number of cases of administrative litigation, there is a trend in both Hungarian and EU data protection litigation practice towards an increase in the number of preliminary rulings initiated in relation to the General Data Protection Regulation. In 2021, the Municipal Court of Budapest – on behalf of the Hungarian courts – made use of these powers in 2 cases as will be presented below. These cases are still in progress before the Court of Justice of the European Union.

Below, we highlight a few of the more interesting cases fundamentally affecting a wider range of data subjects.

V.1. „"Let us join the European Prosecutor's Office" initiative

In the course of the initiative entitled "Let us join the European Prosecutor's Office" (hereinafter: initiative) the petitioner, a Member of Parliament, collected the names, addresses, e-mail addresses, phone numbers and signatures (hereinafter jointly: personal data) of the data subjects on the sheet for expressing support for the initiative according to the Privacy Statement printed on the back of the sheet (hereinafter: Privacy Statement) in order to be able to provide information concerning his parliamentary activities.

Information on the primary purpose of data processing was provided on the front of the sheet and there was no indication at the individual data whether providing the data was mandatory or optional for supporting the initiative. Below the table for filling in the data, there was the following text: "I support Hungary's joining the Institution of the European Prosecution with my signature", information on the mode of returning the sheet and the following text: "Privacy Statement – I accept the Privacy Statement with my signature \[…] Privacy Statement on the personal data processed by the staff of \[…] and his colleagues." The information on the back of the sheet states that "The legal basis of processing is your express consent having read this Privacy Statement".

According to the information provided, the petitioner would submit the sheets at the latest on 31 May 2019 to the public notary, irrespective of the number of signatures collected. There was, however, no information about what was going to happen to the sheets and the data following their submission to the public notary, or if the number of signatures collected was insufficient.

During the period of signature collection, there was a possibility to upload the completed sheets online, for which it was necessary to provide the name, e-mail address, county, settlement and phone number and the Privacy Statement had to be accepted according to which the purpose of processing was to establish and maintain contact with those supporting the European Prosecution and informing the data subjects about activities, events, movements and signature collections in support of the European Prosecution.

In the course of the online uploading, the data subjects gave their consent to the processing of the data by providing their personal data in the fields whose completion was required and ticking the box beside the Privacy Statement. Without this, it was not possible to upload the sheets. Everybody had an opportunity to upload sheets online. In the case of online uploading, there was no separate opportunity to subscribe to the newsletter via the form whose completion was mandatory and there was no information on the period of processing of the data uploaded online.

Because of non-compliance with the repeated call for the erasure of personal data in the course of its inquiry procedure launched ex officio, the Authority launched its data protection procedure ex officio.

In its decision NAIH/2020/974/4 of 9 July 2020, the Authority

- established that the controller, by collecting the personal data of the data subjects without a legal basis for the purpose of maintaining contact related to the initiative called “Let us join the European Prosecution” in the period between 19 July 2018 and 30 May 2019, infringed GDPR Article 6(1) and Article 9(1);

- established that by not providing appropriate information on all the essential circumstances of processing, the controller infringed GDPR Article 5(1)(a), Article 5(2) and Article 13;

- ordered the controller to erase all the personal data collected from the data subjects for the purpose of maintaining contact in relation to the initiative called “Let us join the European Prosecution” between 19 July 2018 and 30 May 2019 within 30 days from the decision becoming final; and

- imposed a data protection fine of HUF 1,000,000 on the controller.

The petitioner requested the examination of the lawfulness of the decision from the Municipal Court of Budapest. According to his position, the qualification of contact data as special category personal data is excluded, so there is no need for an express consent for the processing of these data. With respect to the informed consent, he explained that for it suffices to provide the person of the controller and his purpose, other deficiencies of the information provided do not affect the legal basis. He claimed that the information provided complied with the provisions of GDPR Article 13(2)(a).

As to the part of the decision ordering erasure, he declared that the Authority may order the rectification or erasure of personal data or the restriction of data processing only in accordance with the provisions of GDPR Articles 16, 17 and 18 and the power of rectification according to Article 17 may be applied, if the data subject requests the erasure of his personal data making use of his rights according to this Article, hence the Authority exceeded its powers when requiring erasure in its decision.

In its judgment, the Municipal Court of Budapest annulled the point of NAIH/2020/974/4 concerning the order to erase personal data, beyond this, however, it rejected the petition of the petitioner in its entirety.

According to the justification of the judgment, the petitioner processed personal data for the purpose of providing information on his public activities pursued as a Member of Parliament and based on the demand for information on political activities and for maintaining contact with the politician, they hold identifiable political views by deduction, taking into account the purpose of the initiative and the demand for receiving information on the political activities of the petitioner while providing support for the initiative, these data qualify as data concerning political opinions. Because of this, the personal data were special category personal data, whose processing required the explicit consent of the data subject, in accordance with GDPR Article 9(2)(a), in addition to the consent required under GDPR Article 6(1)(a). The absence of express consent was substantiated by the circumstance that the signature of the data subject referred not to the processing of the data but to supporting the initiative and that he accepted the Privacy Statement with his signature. Providing the requested data in the sheet and accepting the Privacy Statement by signature in themselves do not mean an action unmistakably expressing confirmation of consent to the use of special category personal data.

In accordance with the position of the Authority, the Municipal Court of Budapest underlined that the data subjects’ consent may not be extended to additional purposes different from the original purpose of data processing affected by the consent. The signatures were collected not only to support the initiative because for this purpose, the petitioner only collected the data of name, address and signature. When the phone number and/or e-mail address were also provided, all the data have become the subject matter of data processing for an additional purpose, that of maintaining political contact.

According to the position of the Court, the Authority lawfully imposed the data protection fine on the petitioner. In this respect, it explained that the Authority appropriately assessed the relevant facts of the case when imposing the fine; the amount of the fine was not excessive relative to the amount of the remuneration the petitioner received as a Member of Parliament.

According to the justification of the order requiring the annihilation of the part concerning the erasure of the personal data, ordering the erasure of personal data is only possible based on the request of the data subject, the Authority

made its decision by infringing its powers and it was not authorised to order the petitioner to erase the personal data as a legal consequence of the established infringement. *(Fővárosi Törvényszék 105.K.706.125/2020/12.).*

In this context, the Authority launched a review procedure in front of the Curia, which accepted the petition for review. The Curia upheld judgement No. 105.K.706.125/2020/12 of the Municipal Court of Budapest. *(Kúria Kfv. II.37.001/2021/6.).*

The Authority filed a constitutional complaint in the case, which was accepted by the Office of the Constitutional Court according to its information of 23 June 2021.

In its decision, the Constitutional Court found that the judgments of the Curia and the Municipal Court of Budapest were contrary to the Fundamental Law and therefore annulled them.

The Constitutional Court established that pursuant to Section VI(4) of the Fundamental Law, the petitioner is an independent authority established by cardinal law, whose responsibilities under the Fundamental Law include the supervision of the enforcement of the right to the protection of personal data and access to data of public interest. The legal interpretation in the court decisions challenged concerns the operation of the petitioner in relation to the exercise of its powers, taking into account the provisions of the Fundamental Law, GDPR, which is directly applicable in the Member States of European Union, the Constitutional Court Act and the Privacy Act.

The Constitutional Court underlined that in the course of making their decisions and their considerations of the right to the protection of personal data, which are among the independent fundamental rights, the courts failed to recognise that a wide-range of control through a data protection supervisory authority was guaranteed based on the obligations arising from the Fundamental Law, EU law and international law, even prior to the GDPR. The responsibility of the Authority according to the Fundamental Law is to oversee the enforcement of the fundamental right for the protection of personal data. It exercises this supervision (constitutional responsibility) through its powers under the cardinal law. The purpose of the supervision is to ensure that personal data are protected during each processing operation. If the Authority finds during its supervision that the processing of personal data by the controller is unlawful, it follows from the effective protection of fundamental rights, which is the primary responsibility of the Authority, that it may not only inspect and detect unlawful processing of personal data but

– in order to protect the fundamental rights of third persons – it may also order the erasure of such data ex officio. Otherwise, in the absence of an effective protection of fundamental rights, the powers are limited and so is the discharge of this responsibility according to the Fundamental Law.

The protection of personal data is a “fundamental right of a protective type”, which requires effective legal protection by the Authority. Based on Article (E) (2) and (3) and Article VI(4) of the Fundamental Law and GDPR as the EU regulation for the uniform application of data protection and freedom of information, the Authority is authorised to order ex officio the erasure of unlawfully processed personal data even in the absence of the relevant request.

V.2. Uploading decisions in relation to the pandemic to third party gateway storage

The Authority was notified by a limited partnership not party to the lawsuit that the controller uploaded the pandemic decisions of 60 persons to the client gateway storage of the limited partnership, who were not its employees and were not in a relationship with it. According to the content of the decisions, the data subjects were either quarantined or the quarantine ordered for them was terminated. The limited partnership notified the controller of what happened, at the same time, the pandemic decisions continued to be accessible in the client gateway storage. Based on the notification, the Authority ex officio launched its audit to check compliance with the obligations set forth in GDPR Articles 33-34. In view of the fact that based on the information found, the controller probably infringed the provisions of GDPR, the defendant launched the authority procedure for data protection pursuant to Section 60(1) of the Privacy Act.

In response to the request for a statement, the controller explained that it had conducted proceedings against the limited partnership, at the end of which it had issued a decision and sent it to limited partnership via the Poszeidon system, whose contact details were still on the address list, which is why the forty pandemic decisions were sent to it. . As there is no way to suspend, stop or cancel sending in the Poszeidón system, the limited partnership was asked to erase the decisions from its storage. In relation to the decisions that were not downloaded, the limited partnership received a second notification on the 8th day following dispatch; on 1 December 2020, it downloaded two of these decisions. Then, the limited partnership notified the controller again of the erroneous sending of documents.

In the course of the procedure, the Authority called upon an employee of the Nemzeti Infokommunikációs és Szolgáltató Zrt. (hereinafter: NISZ Zrt.) to make a witness statement, according to which there was no function within the Cégkapu (Company gateway) service, which would enable the recall of letters, documents and annexes.

The Authority established that four of the decisions delivered were issued to order isolation because of the pandemic, of which the limited partnership downloaded one, four out of ten contact decisions and five of the twenty-six decisions concerning the termination of isolation because of the pandemic. The Authority established that the controller did not attempt to contact the limited partnership other than by a phone call; and did not contact NISZ Zrt. to withdraw the sending or to waive the second notification. The controller did not establish a personal data breach in relation to either the first or the second sending, all it did was to call upon the limited partnership to erase the decisions. The controller did have a data protection officer, whom it failed to notify of the case and it also failed to involve him in administering the case. The controller reminded of its employees only verbally to check the addressee list.

The order of the Authority

In its order, the Authority found that the controller had failed to comply with the following obligations concerning a data breach caused by the delivery of 40 decisions in relation to the pandemic containing personal data to an unauthorised entity:

- its notification obligation under GDPR Article 33(1),
- its registration obligation under GDPR Article 33(5) in relation to the data breach that has occurred,
- its obligation under GDPR Article 38(1) when it failed to involve the DPO in the management of the data breach "despite being under an obligation to designate a DPO".

The Authority has ordered the controller to enter the data breach in its data breach register within 30 days of the order becoming final and to take the necessary measures to ensure that any future data breach is notified within the time limit provided for in GDPR Article 33(1), and to inform the Authority within 10 days of the measures taken.

The Authority imposed a data protection fine of HUF 1,500,000 on the controller for the infringements found.

The petition

In its petition submitted against the order, the petitioning controller primarily requested… that an admonition be sent to him as a sanction instead of a fine. Secondarily, it requested a reduction in the amount of the fine imposed and thirdly, it requested the annulment of the order and ordering the defendant to conduct new proceedings.

Citing the provisions of GDPR 57(1)(22) and 58(2), the petitioner emphasized that the defendant failed to take action with sufficient circumspection when imposing the fine, when, following the clarification of the fact of the case, it wrongly arrived at the conclusion upon weighing the available facts and information that it was necessary to impose a data protection fine rather than issuing an admonition. It also stated that the criteria to be weighed when imposing the fine were laid down in GDPR Article 83(2) and the interpretation of the conditions for applying a fine was provided in the Guidelines on the application and setting of administrative fines for the purpose of Regulation 2016/679 by the Article 29 working group[27] (hereinafter: Guidelines). According to its position, the defendant exercised its powers to impose a fine violating the principles of proportionality and gradation, in particular with regard to the powers to issue an admonition under Section 75/A of the Privacy Act. It underlined that the defendant also qualified the infringement as less severe adding that, following the entry into force of GDPR on 25 May 2018, there have been no personal data breaches and the Authority did not carry out any data protection procedure, the defendant did not comply with its obligation to exercise discretion in accordance with legal regulations, and it failed to evaluate all the criteria according to GDPR Article 83(2).

In addition to this, it also objected to the fact that its cooperative behaviour was "not evaluated as an expressly mitigating circumstance", although it had cooperated throughout the entire procedure of the Authority and provided the requested information in due time.

27 https://www.naih.hu/files/wp253_HU_koezigazgatasi_birsag.pdf

Judgment of the Municipal Court of Budapest

On the basis of the above, the court had to decide whether the defendant lawfully applied a data protection fine for the petitioner's infringement and whether it was lawfully determined to the extent that it was justified by the circumstances that had to be taken into account.

In its petition, the petitioner cited first and foremost that the defendant should have issued an admonition instead of imposing a data protection fine on account of the infringement committed for the first time. In terms of this, the court pointed out that Section 61(1)(a) of the Privacy Act clearly allows the imposition of a fine as a sanction and according to the provision of Section 75=A of the Privacy Act quoted in the petition, it is the sanction to be applied "first". The legal text makes it clear that the defendant lawfully imposed a fine even in the case of the petitioner's infringement established for the first time. The order provided appropriate justification for this legal consequence by stating that the admonition was not regarded as proportionate to the infringement or a sanction of restraining force.

The petitioner did not dispute the fact and the defendant made the right assessment in the course of imposing the fine that health-related data belong to the special category of the data subject's personal data based on GDPR Article 83(2)(g). The defendant imposed the fine in relation to the infringement established in Section I of the order, in which it established the infringement of GDPR Article 33(1), (5) and Article 38(1), which was not disputed by the defendant. All this means that the petitioner failed to meet its obligation of notifying and registering a personal data breach and the obligation to involve the data protection officer in dealing with the data breach. This means that the defendant sanctioned the petitioner's behaviour after the personal data breach, which actually took place. Because of this, the petitioner's reference to the fact that it had no possibility to recall the decisions sent in relation to the data breach could not be right. Because of this, the subsequent data protection training of the petitioner was also irrelevant, and the petitioner's reference to the corona-virus situation was also weightless.

Judicial practice is also well established and the defendant referred to it on good grounds, that cooperation on the part of the petitioner cannot be regarded as a mitigating circumstance in itself, as against this, the absence of cooperation would have been an aggravating circumstance to be assessed against the petitioner.

The petitioner's excuse concerning the absence of the possibility of recalling enclosed documents in the Poszeidón system carries no significance in imposing the fine because all this is not related to the petitioner's behaviour in violation of the law as established by the defendant. The petitioner could have taken the steps (reporting, notification) even with this deficiency, which would have excluded the establishment of the infringement.

In relation to the infringement committed, the defendant appreciated that the petitioner did not commit it deliberately, but negligently (according to the order, through gross negligence), the petitioner's conscience was appropriately appreciated in the defendant's decision. It was also lawfully taken into account by the defendant that based on GDPR Article 83(4)(a) the infringement committed by the petitioner was among those to be sanctioned by a lower amount of fine, hence the petitioner's argument according to which GDPR does not distinguish between lower and higher amounts of fines is also wrong.

All in all, the court established that the defendant lawfully applied the sanction of the data protection fine against the petitioner that committed a data protection infringement for the first time and the circumstances of imposing the fine could be established from the order. The defendant appropriately evaluated the circumstances listed in GDPR Article 83(2) as aggravating, mitigating or other circumstances, and lawfully disregarded the provision not deemed relevant.

Because of this, the court established that the defendant's order does not violate the law as stated in the arguments of the petition and because of this, it rejected the petition as being unfounded based on Section 88(1)(a) of the Administrative Procedures Act *(Fővárosi Törvényszék 105.K.703.956/2021/8.)*

V.3. The DIGI case before the Court of Justice of the European Union

In the DIGI case[28], in which the Authority imposed a fine of HUF 100 million on the controller, the Municipal Court of Budapest referred two questions to the Court of Justice of the European Union. Firstly, whether the "purpose limitation" in GDPR Article 5(1)(b) should be interpreted as meaning that it is still satisfied if the controller stores personal data, which are otherwise lawfully collected and stored for a specific purpose, in parallel in another database, or the lawful pur-

28 NAIH/2020/1160

pose limitation of the collection of data no longer applies to the parallel database. On the other hand, the court wished to know whether, if the answer to Question 1 is that the parallel storage itself is not compatible with the principle of "purpose limitation", it is compatible with the principle of "limited storage" laid down in GDPR Article 5(1)(e), if the controller stores personal data, otherwise lawfully collected and stored for a specific purpose, in another database in parallel..

The Authority itself is represented in the preliminary ruling procedure. The hearing before the Court of Justice of the European Union was held on 17 January 2022 and the Opinion of the Advocate General is to be delivered on 31 March 2022.

V.4. The Budapest Electricity Works case before the Court of Justice of the European Union

In this case, although the Municipal Court of Budapest has essentially referred a procedural question to the Luxembourg Court, the answer may fundamentally determine the future relationship between administrative and civil jurisdiction and the relationship between the courts and the Authority, and it may have a fundamental impact on the unity of law in data protection law and its durability.

Questions referred to the Court of Justice of the European Union by the Municipal Court of Budapest:

Are Articles 77(1) and 79(1) of the General Data Protection Regulation to be interpreted as meaning that the administrative remedy in Article 77 is a means of public enforcement and the judicial remedy in Article 79 is a means of private enforcement?

If so, does it follow that the supervisory authority competent for administrative remedies has primary competence to determine the facts of the infringement?

If the data subject, who considers that the processing of personal data relating to him has infringed the General Data Protection Regulation, exercises both the right to lodge a complaint under Article 77(1) of the General Data Protection Regulation and the right to judicial remedy under Article 79(1) of the General Data Protection Regulation, which interpretation is in line with Article 47 of the Charter of Fundamental Rights:

a) the supervisory authority and the court are obliged to investigate the infringement independently of each other, and they might reach different conclusions; or
b) the decision of the supervisory authority takes precedence in assessing whether an infringement has been committed, having regard to the powers conferred on it by Article 51(1) and Article 58(2)(b) and (d) of the General Data Protection Regulation?

b) the decision of the supervisory authority takes precedence in assessing whether an infringement has been committed, having regard to the powers conferred on it by Article 51(1) and Article 58(2)(b) and (d) of the General Data Protection Regulation?

Furthermore, the court also asked whether the independent legal status granted to the supervisory authority by Articles 51(1) and 52(1) of the General Data Protection Regulation should be interpreted as meaning that the supervisory authority, in its procedure and decision on a complaint under Article 77, is independent of the final judgment of the competent court under Article 79 and it may thus reach a different decision on the same alleged infringement?

The Authority is also acting on its own behalf before the Court of Justice of the European Union in this case. A hearing has not been held yet.

VI. The Authority's activities related to legislation

VI.1. Statistical data on regulatory affairs

Number of the Authority's statements of opinion on regulatory affairs by the level of legal source

Legal source/ year	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Act of Parliament	85	49	86	33	79	85	82	72	61	73	77
Government decree	75	60	89	63	133	98	89	47	49	52	74
Ministerial decree	104	70	92	85	126	83	94	55	41	27	15
Government decision	26	12	28	21	61	29	33	40	34	22	14
Other (Decision by Parliament, Order, etc.)	10	16	15	7	27	20	23	17	29	10	16
Total	**300**	**207**	**310**	**209**	**426**	**315**	**321**	**231**	**214**	**184**	**196**

Statistical data on substantive observations in statements of opinion on legislation

Type of observation	Észrevételek száma							
	2014	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**	**2021**
Data protection	145	298	461	461	487	323	436	488
Freedom of information	21	53	28	28	22	39	80	89
Other	53	137	92	92	79	78	37	9
Total	**219**	**488**	**581**	**581**	**588**	**440**	**553**	**586**

Pursuant to Section 8(2) of Act CXXXI of 2010 on the Participation of Society in the Preparation of Legal Regulations, the minister in charge of drafting legal regulation has to publish and submit for consultation with citizens, the drafts and concepts of Acts of Parliament, government decrees, ministerial decrees, the summaries of preliminary impact assessments as well as the drafts not submitted for consultation with citizens on the website designated for this purpose (www.kormany.hu) and they may not be removed from there for a year from their disclosure. Anyone may express an opinion on the drafts and concepts published with a view to consultation with the citizens through the e-mail address provided on the website.

Unfortunately, for years now, the Authority has regularly observed that ministries preparing draft legislation do not comply with their legal obligation of disclosure. The Authority repeatedly draws the attention of the ministries preparing drafts to do this, yet the situation has remained unchanged for years.

VI.2. Bill T/16365 on stricter action against paedophile offenders and amending certain laws in order to protect children

The Authority continuously monitors the bills submitted to Parliament and uploaded to the parlament.hu website and reviews them from a data protection point of view. If an unclarified data protection issue or obviously flawed regulatory solution arises after submission, the Authority can turn primarily to the designated committee of Parliament, or to the legislative committee to remedy the problem.

In the course of the preparation of Bill T/16365 on stricter action against paedophile offenders and amending certain laws in order to protect children, the Authority was not given an opportunity to provide its opinion and was first confronted with the bill after it was submitted to Parliament.

First, the Authority contacted the Justice Committee directing the attention of the Chairman and the members of the committee to several issues in a letter, which were strongly objectionable from the viewpoint of protecting person data, then the Authority presented its objections in person at the meeting of the committee. The Authority considered the legal policy objective underlying the bill – the protection of the rights of children and the prevention of criminal acts committed against them – has to be supported and promoted also by legislative means, even in the manner intended by the bill, which entails restricting the right to the protection of personal data, but the safeguard rules incorporated in the bill were insufficient with regard to the protection of personal data. The bill did not sufficiently reduce the risk of using a large volume of criminal personal data and special category data for purposes other than that specified in the bill, i.e. unlawfully.

The Authority then conducted direct reconciliation with the entity submitting the bill involving the Ministry of the Interior and the Ministry of Justice, as a result of which an agreement was reached successfully, primarily in the regulation

concerning the criminal register and the text concerning the amendment of the Labour Code, so as to meet the expectations concerning the protection of personal data. According to the promulgated standard text of Act LXXIX of 2021, the person making the query has to make a statement on whether the processing was necessary and proportionate; the system logs queries, which enable subsequent checking whether a query was lawful. In case of multiple hits, the system does not display the relevant personal data of every hit, only the stored photo and the address, the name of the settlement, including the district in the case of Budapest, and then these data can be used to select the person to whom the query applies and only their personal data will be displayed on the screen.

When the Venice Commission studied the Act, the Commission pursued a dialogue also with the Authority about the Act, and as a result, it did not formulate an unfavourable opinion concerning the data processing issues of the Act.

VI.3. Biometric signature at the government office

The amendment to Act CXXVI of 2010 on the Budapest and County Government Offices and the amendment of acts related to the establishment of the Budapest and County Government Offices and regional integration introduced the legal possibility of using the signature pad enabling biometric signature at the Government Offices as of 1 September 2021. The signature pad is a device, which is capable of attesting electronic documents by the client through the electronic comparison of the data of the image, dynamics and writing strength of the signature. Provided that appropriate conditions set forth by law prevail, samples of minors with limited capacity to act and persons partially limited in their capacity to act may also be included in the register of specimen signatures by the Government Office..

VI.4. Act XXXI of 2021 amending certain Acts on law enforcement administration in order to strengthen public security

Act XXXI of 2021 amending certain acts on law enforcement administration in order to strengthen public security contains several data protection elements.

By amending Act CLXXXVIII of 2015 on the Facial Image Analysis Register and the Facial Image Analysis System, the Act included frontal facial images processed in the system of criminal records by the criminal records department in the facial image profile records, thus expanding the source register of facial image profiles. Consequently, a natural person whose data are already included in the facial image profile register will have new and presumably better-quality photos incorporated in the facial image profile register, taking into account that the human face may change as a result of ageing changes in lifestyles and life conditions, disease or accident. On the other hand, the facial image profile register is expanded with the facial images of foreign persons, who had not been included in the register before as they do not have their facial images in the records of organs with a mandatory data transfer obligation to the facial image profile register.

Due to the large amount of data to be handled and the order of magnitude of the increase in the number of images stored in the facial image analysis register (approximately 900,000-1,000,000 images were transferred upon the first upload and the facial image analysis register will grow by approximately the same amount in the long term), the Authority recommended that the submitter prepare a preliminary data protection impact assessment.

The other data protection aspect of the law package is that with a view to ensuring harmony with Regulation (EU) 2019/1157 of the European Parliament and of the Council on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement, the residence card to be issued to third country citizen family members of EEA citizens will have a new form as of 1 august 2021: a biometric document will be issued having the same format as the residence permit. In relation to this, it is necessary to record the facial image and fingerprint of the third country citizen family member.

VI.5. Data Change Management Service

When the Government decided to introduce the Data Change Management Service (AVSZ) in Government Decision 1795/2020. (XI.13.), the Authority had the opportunity to form an opinion of the law amendment package needed for the implementation of the first step of the AVSZ project in September 2021. The objective of AVSZ is to notify the public utilities and telecommunication service providers in a contractual relationship with the data subject about the changes in the name, address, document identification and contact data of natural persons processed in state registers with the consent of the data subject in an attested electronic format. The state also provides a free, one-stop-shop administration

service for the process of transferring public utilities, which can be used voluntarily by service providers and the data subject natural persons.

From 1 January 2022, electronic communication service providers, district heating providers, electricity traders, natural gas traders, water utility service providers may join the first phase of the project. Data storage related to secure delivery service (KÜNY storage) is required for joining as client. The two fundamental services available in this way include the service of data change reporting and the user change reporting service. The Government designated the Pest County Government Office as the data change management service provider in a decision.

VI.6. Registration of data of inland waterway passengers

Directive 2016/681/EU of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (the PNR Directive) requires Member States to keep a register of air passenger data to facilitate the prevention, detection, investigation and prosecution of specific criminal offences. The purpose of processing is the identification of persons who may be associated with terrorism and using that, the reduction of the risk of the threat posed by terrorist acts and severe criminal acts. In Hungary, the tasks of the passenger information unit have been carried out by the Terrorelhárítási Információs és Bűnügyi Elemző Központ (Terrorism Prevention Information and Criminal Analysis Centre) since September 2015. As of 30 December 2021, this task was supplemented with the registration of inland waterway passengers. The PNR directive neither requires, nor excludes that Member States record the data on border crossing passengers arriving and departing by routes other than air transport. The amendment necessary to allow carriers participating in inland waterway shipping to analyse the inland waterway passenger data for safety purposes did not create a new reporting obligation.

VI.7. Government decrees in a state of emergency

Since the introduction of the state of emergency proclaimed by the Government in Government Decree 478/2020. (XI. 3.) on 3 November 2020, the Authority has been continuously involved in stating an opinion on draft legislation in connection with the declaration of the state the emergency, as was the case during the period of emergency from 11 March to 18 June 2020.

Pursuant to Article 53(2) of the Fundamental Law, in a state of emergency the Government may adopt decrees by means of which it may, as provided by cardinal law, suspend the application of certain acts, derogate from the provisions of acts and take other extraordinary measures. One such item of legislation is Government Decree 521/2020. (XI. 25.) on the derogation from certain data request provisions in times of emergency, the provisions of which have already been described in the chapter on the Freedom of Information.

In 2021, the Authority provided its opinion on a number of draft government decrees prepared on the basis of the legislative powers granted by Article 53(2) of the Fundamental Law and addressed the processing of personal data. In many cases, these drafts provided for large quantities of transfers of special category (health-related) data, for instance to check the administration of vaccines. Epidemiological protection necessitates the processing of health-related data in a variety of life situations. Such data include whether somebody had already been infected, whether had been vaccinated, if so, how many times, what type of vaccine was administered and when. The processing of these personal data not only by person, but also by specific categories (such as employees of the same employer, students of the same school) is indispensable for the organisation of effective protection in as pandemic. When forming its opinion in such cases the Authority pays particular attention to having the Government Decree specify the purpose of the intended processing with the appropriate thoroughness and that the entire processing comply with the principles of necessity and proportionality, taking into account the benefits that may be achieved by processing. In the Authority's view, the purpose of the processing is not sufficiently described by the definition that the purpose is, for instance, to facilitate protection against the corona-virus or the discharge of the Government's epidemiological tasks. An appropriately specific definition of the purpose must apply to the given explicit processing and must at least make it clear in itself that the processing is necessary to achieve the purpose, for which no other means could provide a sufficient solution.

VI.8. Interoperability among EU information systems

Since 2016, it is the express objective of the European Commission to improve the EU framework for data processing in the area of border controls and security checks. Two new interoperability regulations were enacted with a view to setting up a framework of interoperability between EU information systems:

a) Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending regulation (EC) No. 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA; and

b) Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816.

The interoperability regulations created a framework, thereby ensuring interoperability between

a) the Entry/Exit System - European Union (EES),
b) the Visa Information System (VIS),
c) European Travel Information and Authorization System (ETIAS),
d) az Eurodac,
e) the Schengen Information System (SIS), and
f) the European Criminal Records Information System - third country nationals (ECRIS-TCN).

The new functions to be introduced by the interoperability regulations:

- European Search Portal (ESP).

- Shared Biometric Matching Service (BMS) This facilitates the comparison of biometric data stored in the information systems concerned with a view to detecting multiple personal identities.

- Common Identity Repository (CIR).

The interoperability regulations allow Member States to regulate access to CIR for the purpose of identifying a person so that the police agency be authorised to carry out queries in CIR for personal identification with biometric data (fingerprint data and facial image) taken from the person to be identified in the presence of the checked person. In addition, police agencies can be authorised to query CIR with the biometric data of unknown persons unable to verify their identity or unidentified human remains in the case of natural disasters, accidents or terrorist attacks.

- Multiple-Identity Detector (MID).

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

VII.1. Cooperation with partner authorities in the European Union – cooperation and consistency procedures

VII.1.1. Introduction

The application of the GDPR, the General Data Protection Regulation of the European Union, specifies tasks for the data protection authorities of the Member States. In discharging these duties, the authorities cooperate with one another, in some cases voluntarily, while in other cases cooperation is mandatory.

The EU legislator expects that GDPR is efficiently and uniformly enforced in every Member State. The expectation of a uniform application of the law is clear, its daily practice, however, is not at all self-evident: the supervisory authorities operating in every Member State of the European Economic Area have to take into account the positions and interpretations of the law by the other authorities, so as to genuinely act in a uniform way with regard to the interpretation of GDPR. This requires a great deal of work, attention and the meticulous discussion of issues of interpretation of the law in the various expert subgroups of the European Data Protection Board (EDPB). All this is a precondition to GDPR fulfilling the role intended for it by the EU legislator and to which it is designed: to provide uniform, high-level and effective data protection for every citizen of the European Economic Area.

Ever since its establishment, the Authority has paid particular attention to international cooperation in general and EU cooperation in particular. As reported in earlier years, the Hungarian authority is represented in every expert subgroup of the European Data Protection Board, furthermore, the cooperation expert subgroup, dealing with issues of cooperation, functions under Hungarian leadership. Unfortunately, there are no similar examples to this in our region. It can therefore be said that the Authority takes every possible opportunity for cooperation, for participating in the joint work and to incorporate all aspects into work at EU level which specifically arise in the Hungarian environment.

Below, we highlight the cases and events, which proved to be the most significant in 2021 and which deserve the greatest attention.

VII.1.2. Official opening of the Giovanni Buttarelli meeting room

In terms of international and EU cooperation, the Authority attaches importance to the evolution of a data protection culture in Hungary which guarantees a high, effective and efficient level of protection for personal data. The recognition of the right patterns, practices and outstanding authorities greatly contributes to this.

Giovanni Buttarelli, Italian lawyer, data protection expert and former European data protection commissioner, was such a person in all respects, whose work substantially contributed to the development of data protection in Europe. In the spirit of honouring his memory, the Deputy President's Cabinet responsible for EU cooperation named its meeting room after him in the new building of the Authority, which was personally inaugurated by Manuel Jacoangeli, Italy's ambassador to Hungary, in October 2021.

VII.1.3. Review of the cooperative procedures conducted pursuant to GDPR

Since the application of GDPR beginning in 2018, the Authority has taken an active part in Article 60 cooperation procedures with the Member States of the EEA. The one-stop access[29] is designed to investigate cases initiated on the basis of a complaint or ex officio in relation to cross-border processing.

The communication among the authorities related to the cooperation procedures is conducted via an interface specifically transformed for these procedures in the Internal Market Information System (hereinafter: IMI system).

Prior to the cooperation procedures, the Member State authority which received a complaint against a controller pursuing cross-border processing (hereinafter: initiating authority) launches an Article 56 procedure in the IMI system to identify the lead supervisory authority and the supervisory authorities concerned.

The initiating authority may presume the lead supervisory authority based on the centre of operation or a single place of activity of the controller/processor[30], which authority may accept or reject this role with appropriate justification.[31] In addition, the Member States in which the controller/processor does not have a centre of operation or place of activity may designate themselves as authorities concerned, if the processing under investigation is likely to affect a large number of data subjects who are residents in their countries.

In 2021, the Authority received 553 cases from the authorities of other Member States through the IMI system, in roughly a quarter of which the Authority found itself concerned. The Authority acted as the lead supervisory authority in four procedures and launched 18 Article 56 procedures of its own during the same period.

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

If an authority concerned submits a well-founded and relevant objection or amending motion to a draft decision, the lead supervisory authority may produce a revised draft decision based on the recommendations, which the authorities concerned may again comment on, similarly to the earlier version over a four-week period. The lead supervisory authority may modify its draft decision as long as all the authorities concerned accept it, after which it can be sent to all the Member State authorities in the form of a binding decision.

In 2021, the Authority received 76 draft decisions to be studied, 17 revised draft decisions and 337 binding decisions. In addition, the Authority received 101 informal consultations to assist in cooperation according to Article 60. During the same period, the Authority sent five draft decisions, one revised draft decision and three binding decisions to the other authorities under the cooperative procedures.

In the event that a lead supervisory authority disagrees with the relevant and well-founded objections of the authorities concerned, it may request the Board to resolve the conflict and decide on the disputed issues through a dispute settlement procedure according to Article 65.

In 2021, one such procedure was launched against a draft decision of the Irish authority concerning the controller WhatsApp Ireland Limited. The procedure was closed by a binding decision of the Board under Article 65 in July 2021. No draft decision of the Authority has been the subject of a dispute settlement procedure.

Also, cooperation procedures include mutual aid procedures according to Article 61 and voluntary mutual aid procedures. While the former is a procedure subject to stringent formal requirements and require performance within a given period, conducted generally between two Member States, the latter is a more permissive procedure both in terms of form and content, which the Member State authorities use, inter alia, for giving and obtaining information, making inquiries about inquiry procedures and conducting general consultation.

In 2021, the Authority participated in 1 mutual (mandatory) aid procedure and it received 140 requests for voluntary mutual aid procedures. During the same pe-

29 GDPR Article 60

30 Based on GDPR Article 27, in the case of controllers or processors not having a place of activity in the European Union.

31 GDPR Article 56(3)

riod, the Authority initiated 9 mutual aid procedures and 10 voluntary mutual aid procedures.

Although not closely related to the procedure according to Article 60, the opinions of the Board according to Article 64 should also be mentioned, of which the Authority received 33 in 2021, two of which were decisions by the Board according to Article 64.

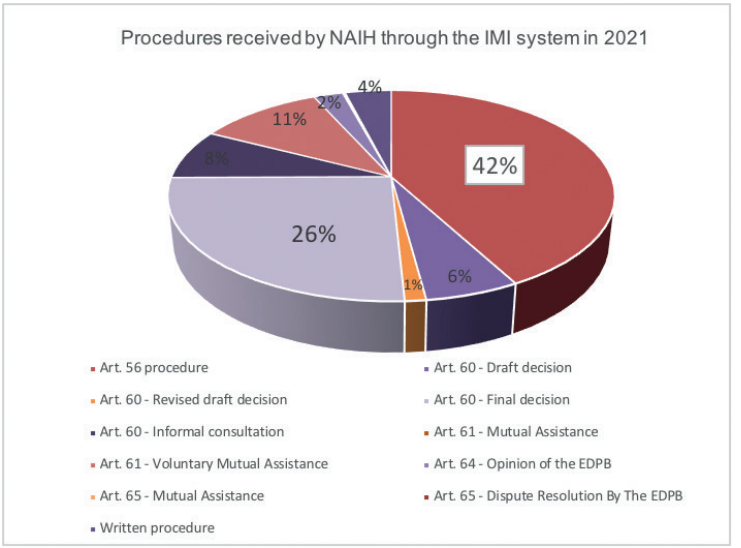
The first Article 66 emergency procedure was launched in 2021. The purpose of these procedures is to allow a Member State to take a provisional measure having legal effect for a period of three months within its own territory in order to protect the rights and freedoms of the persons concerned, bypassing the rules on cooperation procedures. The procedure was initiated by the German (Hamburg) data protection authority because the new terms of use of WhatsApp Ireland Ltd. would have allowed, inter alia, the transfer of users' personal data to Facebook, although they had no legal basis to do so. The Board closed the case with a final decision[32] on 12.07.2021 and took no action at EU level.

Also noteworthy are the 52 written procedures handled by the Authority in 2021 in relation to cooperation between Member State authorities, which are votes in the IMI system designed to simplify the Board's plenary agenda.

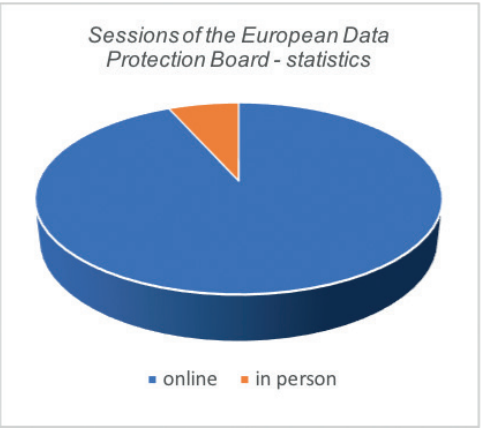
Statistics from May 2018, when the GDPR became applicable, show that the focus of procedures among national authorities has shifted from identifying the main supervisory authorities to cooperation and communication.

32 Urgent Binding Decision 01/2021 on the request under Article 66(2) GDPR from the Hamburg (German) Supervisory Authority for ordering the adoption of final measures regarding Facebook Ireland Limited

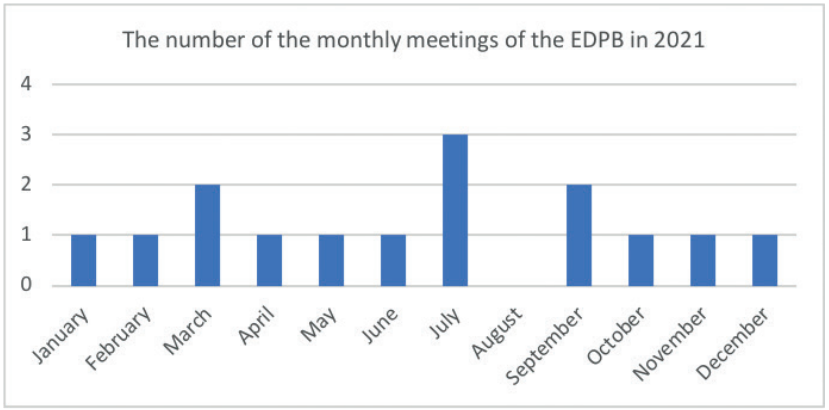
VII.1.4. Cases handled in 2021

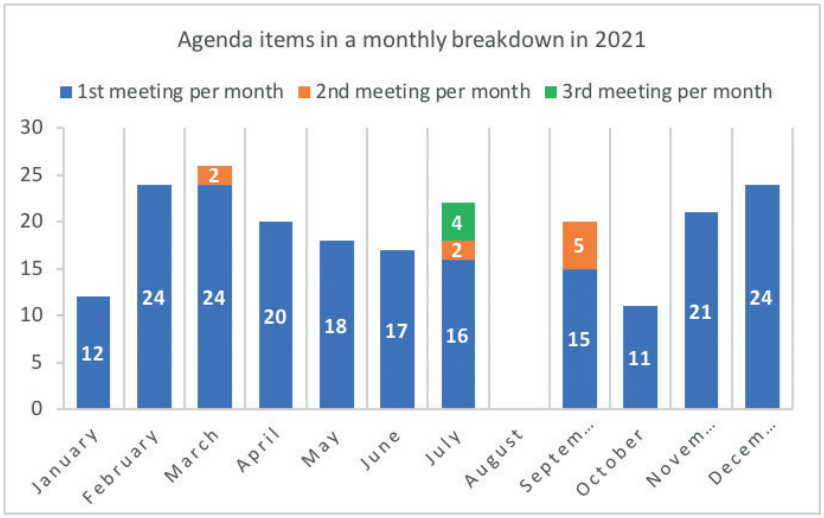


VII.1.5. Participation of the Authority in the activities of the European Data Protection Board – statistics



Even in 2021, the pandemic caused by the corona-virus had a direct impact on the functioning of the Board. In 2021, a total of 15 plenary meetings were held. Of the 15 meetings held, only one was conducted in person in Brussels and 14 were conducted by videoconference. The online meetings were still necessary to ensure that, in a pandemic context, DPAs in the EEA Member States could regularly coordinate their positions. In total, the 15 plenary meetings of the European Data Protection Board covered 215 agenda items, an average of 14.33 items per meeting, which is more than last year.





VII.1.6. Guidelines and opinions of the European Data Protection Board, the activities of the expert subgroups

1. EDPB opinion concerning Article 58(2)(g) – the powers of the authorities related to the erasure of unlawfully processed data

The Hungarian authority initiated that EDPB examine whether Article 58(2)(g) of the General Data Protection Regulation could be a legal basis for a supervisory authority to ex officio order the erasure of the unlawfully processed personal data in a case when the data subject did not request it.

The Enforcement expert subgroup designated for this purpose discuss the opinion first in September 2021; the members discussed it in detail and elaborated the draft. EDPB then adopted the document at its plenary session held on 14 December 2021.

The opinion clarifies only the issue of whether GDPR Article 58(2)(g) can be the legal basis for a supervisory authority to ex officio order the erasure of the unlawfully processed personal data in situations when the data subject did not request it, and it does not address other justification powers set forth in Article 58(2) or their interaction with one another. The opinion does not exclude reference to other legal basis set forth in Article 58(2) in the case of erasure ordered by a supervisory authority.

According to the opinion, the erasure of personal data is, on the one hand, the right of the data subject and the obligation of the controller, on the other hand, if a case set forth in Article 17 of the General Data Protection Regulation prevails. At the same time, the opinion underlines that GDPR Article 58(2)(g) may provide a valid legal basis for a supervisory authority to erase the personal data in order to guarantee the appropriate application of the General Data Protection Regulation, inter alia, in situations when the data subjects were not notified or they were not aware of the processing. According to the opinion, with a view to the effective application of the General Data Protection Regulation, it is important for supervisory authorities to have the appropriate means at their disposal to effectively combat infringements. An option requiring a prior erasure request of a data subject for a supervisory authority to be able to order the controller to erase the personal data would restrict the powers of the supervisory authorities. The opinion adopted by EDPB was only accessible in English on the EDPB website at the time of submitting this report.[33]

33 https://edpb.europa.eu/system/files/2022-01/edpb_opinion_202139_article_582g_gdpr_en.pdf

2. The second dispute settlement procedure before EDPB - the WhatsApp case

2021 saw the second dispute settlement procedure in the history of the application of the General Data Protection Regulation. The binding decision of EDPB was drafted by the Enforcement expert subgroup. The dispute settlement procedure became necessary because several supervisory authorities raised objections to the draft decision concerning Whatsapp Ireland Ltd. (hereinafter: Whatsapp IE) issued by the Irish lead supervisory authority. The subject matter of the case was the compliance of processing by Whatsapp IE with the provisions of Articles 12-14 of the General Data Protection Regulation based on the rules of processing and the general conditions of contract.

The authorities raising the objection, including the Hungarian authority, represented the position that with its processing practice Whatsapp IE infringed certain principles stipulated in the General Data Protection Regulation, furthermore, they contested the level of the fine as well as the period imposed for compliance with the data protection regulation. In addition, the majority of the supervisory authorities raising objections thought that the controller erroneously claimed that the phone numbers of “non-users” (i.e. persons who did not download the Whatsapp application, but whose phone numbers, as persons in the users’ contact list, are accessible to Whatsapp IE) lose their personal data character following the procedure applied by the controller.

EDPB evaluated the objections received in accordance with the provisions of Guidelines 09/2020 on relevant and reasoned objection. Based on the objections and the guidelines, EDPB established that Whatsapp IE violated the principle of transparency and the requirements set forth in GDPR Article 13(1)(d) by failing to appropriately notify users of legitimate interest and with respect to this, ordered the Irish authority to establish this infringement in its draft decision.

In relation to the procedure carried out with the phone numbers of non-users, EDPB established that following the procedure the data do not lose their personal data character; accordingly, it ordered the Irish lead supervisory authority to amend the draft decision.

In terms of the legal consequences, EDPB ordered the Irish authority to modify the period open for bringing the processing operations in line with the General Data Protection Regulation to three months in accordance with the transparency obligation. In addition, EDPB also evaluated the level of the fine and its calculation. In terms of the amount of the fine, EDPB established that the worldwide turnover of the undertaking can be taken into account not only in the cases set forth in GDPR Article 83(4)-(6), but also when determining the amount of the fine itself; furthermore, it declared in relation to GDPR Article 83(3) that with regard to the same, or related processing operations, in the event of infringing several provisions of the General Data Protection Regulation, all the infringements have to be taken into account when calculating the amount of the fine.

The Irish supervisory authority modified its draft decision in accordance with the EDPB decision. A significant aspect of this case was that this was the first dispute settlement procedure, whose subject matter was specifically compliance with the General Data Protection Regulation, in the course of which EDPB discussed the application and interpretation of certain provisions of the regulation in the given case in merit. The EDPB binding decision is accessible on its website in English. [34]

3. Guidelines on the management of personal data breaches

EDPB adopted Guidelines 01/2021 on Examples regarding Personal Data Breach Notification on 19 January 2021. EDPB had earlier adopted general guidelines concerning personal data breaches, but based on the experiences of the Member State authorities, there was a need for practice-oriented guidelines concerning data breaches. Accordingly, the expert subgroup dealing with technological cases drafted a document presenting the risk analysis of personal data breaches through empirical descriptions of legal cases over the past few years.

EDPB underlined that personal data breaches were, in general, symptoms of data security vulnerabilities, therefore, in addition to the management of the data breach and its risk analysis, controllers have always to lay major emphasis on the detection and termination of the reasons for the data breach. The guidelines present the process of risk analysis through several groups of cases (such as ransomware attacks, breaches caused by lost devices, hacker attacks, human omission, misposting, etc.). At the end of each chapter on a case group, there is a list of good practices about the technical and organisational measures, which would have prevented the data breach or could have mitigated its impact. Within each case group, the document illustrates through several fictitious legal cases, the special circumstances influencing risk analyses for the various types of data breach. The only rapporteur of the guidelines was the Hungarian authority.

34 https://edpb.europa.eu/system/files/2021-09/edpb_bindingdecision_202101_ie_sa_whatsapp_redacted_en.pdf

EDPB adopted the finalised text of the guidelines following social consultation at its session of 14 December 2021.[35]

4. Guidelines on the concepts of controller and processor

Following public consultation, EDPB adopted Guidelines 07/2020 on the concepts of controller and processor in the GDPR on 7 July 2021.[36]

The guidelines examine fundamental concepts; thus it is a foundational work for the uniform application of the law. According to the guidelines, controller is the entity that bears full and unlimited responsibility under data protection law for the processing it carries out. The organisation of the controller has to be treated as a single unit, from which no unit may be separated in terms of legal responsibility for data protection; furthermore, no organisational unit may become the processor of another unit. Practical examples provide the outstanding significance of this documents, clarifying the roles related to certain processing constructions.

The guidelines also addressed the concept of joint controllership in determining which joint complementary activities, the proximity of interest and the possibility of joint benefits are of key importance. Joint controllership requires the collaboration of both controllers, who carry out inseparable processing operations. It is, however, an important criterion that both parties need not have access to the data for having their activities qualified as joint controllership.

The guidelines distinguish the controller and processor in their functions, which has far-reaching legal consequences. It also declares that the selection of the processor is the task and responsibility of the controller. Only those processors may be selected that can verify operation in compliance with the legal regulations.

When using a processor, attention has to be paid to the availability of expertise, reliability and adequate resources. The agreement between the controller and processor must be made in writing, which serves the interests of both parties. The parties themselves specify the details of the binding agreement, but they may use general terms and conditions of contract based on GDPR Article 28.

35 https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012021-examples-regarding-personal-data-breach_en

36 https://edpb.europa.eu/system/files/2022-02/eppb_guidelines_202007_controllerprocessor_final_hu.pdf

5. European Data Protection Board guidelines on the interplay between Article 3 and Chapter V of the GDPR

In April 2019, the European Data Protection Board entrusted its expert group dealing with international data transfers to develop the draft of guidelines on the interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR. The guidelines address the relationship between GDPR's extraterritorial scope and its rules pertaining to data transfers abroad. The draft of the guidelines was compiled earlier (in 2019), but EDPB invited the expert group to revise it in 2021.

The revision of the text of the draft concerns in particular the definition of the concept of data transfer. The analysis of the concept of transfer was on the agenda of several meetings of the expert subgroup dealing with international data transfers in 2021. During these meetings, the subgroup identified the following three combined criteria for the concept:

1. The controller and the processor are subject to the GDPR for the given processing.

2. This controller or processor ("exporter") discloses by transmission or otherwise makes personal data, subject to the processing, available to another controller, joint controller or processor ("importer").

3. The importer is in a third country or is an international organisation, irrespective of whether or not this importer is subject to the GDPR in respect of the given processing in accordance with Article 3.

The new draft of the guidelines was presented at EDPB's plenary session in September 2021. According to the recommendations of the representatives of the delegations, two examples were omitted from the final draft to be adopted. The finalised guidelines adopted by EDPB were published on the EDPB website on 18 November 2021. For the time being, the guidelines are only accessible in English.[37]

Beyond this, it is an important addendum to the topic that the European Commission issued its Standard Contractual Clauses based on GDPR Article 46(2)(c) on 4 June 2021, which constitute adequate safeguards for data transfers

37 https://edpb.europa.eu/system/files/2021-11/edpb_guidelinesinterplaychapterv_article3_adopted_en.pdf

to a third country. The clauses do not apply to data transfers made by a controller or processor to an importer subject to the scope of GDPR based on Article 3(2) (extraterritorial scope).

Because of the above, EDPB attaches importance to the publication of standard contractual causes, which can apply to data transfers subject to the extraterritorial scope according to GDPR Article 3(2).

6. Draft regulation of the European Commission on Artificial Intelligence and the joint opinion of the European Data Protection Board and the European Data Protection Supervisor on it

The draft regulation, published by the European Commission in the spring of 2021, would regulate the development of artificial intelligence (AI) as a single piece of legislation to be implemented uniformly in all EU Member States. The draft aims to turn Europe into a global hub for trustworthy AI, according to a Commission press release.[38]

For classification as AI, the draft requires that three conditions are met at the same time. First, AI has to apply specific technologies; secondly, it has to be able to pursue goals designated by man independently and, finally, it has to produce outputs, which "influence" the environment. In addition to systems based on machine learning, the draft of the new regulation targets two additional technological groups to which its scope would extend. These are the systems based on knowledge representation and statistical systems.

The Code applies a risk-based approach for the classification of AIs in an attempt to divide the systems into four major categories. The first risk category contains the systems classified as having unacceptably high risk. These are AIs, which clearly endanger the safety, livelihood and rights of people. In the second, or high risk, category, the draft Code includes AI technologies that are used in areas and/or for purposes that pose a high risk to certain fundamental rights of individuals. Examples include, for example, critical infrastructure, education or vocational training, security devices for certain products (e.g. robotic surgery), law enforcement, asylum and border control, justice and democratic processes. AI systems that fall into the above categories must comply with strict obligations before they are placed on the market, and they must undergo rigorous risk assessment and mitigation processes during their development. The draft classifies systems, the users of which must be aware of communicating not with a human but with a machine (e.g. chatbots) as limited risk AIs. Finally, the draft classifies the systems constituting the vast majority of AIs, the use of which carries hardly any risk with respect to the rights and safety of users as low risk (for example computer games).

The European Data Protection Board (EDPS) and the European Data Protection Supervisor (EDPS) have also issued a joint opinion on the draft regulation, which generally welcomes the draft, but the Board would tighten the rules in some areas, such as remote biometric identification. As a main rule, the joint opinion would prohibit the use of remote biometric identification systems, which are capable of classifying data subjects into categories based on some characteristics, such as origin, sex and sexual orientation, as this could easily lead to discrimination.[39]

VII.2. Participation in the joint supervisory activity of data protection authorities

VII.2.1. Working group supervising the data protection of the Schengen Information System (SIS II Supervision Coordination Group)

As in previous years, the Coordination Monitoring Group, which operates under Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second-generation Schengen Information System (SIS II), had two meetings in 2021, which were held by video conference in view of the pandemic.

The working group has set the objective of monitoring the management of alerts[40] at Member State level in accordance with Article 36 of Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second-generation Schengen Information System (SIS II) for 2022, for which the European Union Agency for the Operational Management of Large-Scale IT Systems (eu-LISA) sends data to Member State authorities.

38 https://ec.europa.eu/commission/presscorner/detail/hu/IP_21_1682

39 https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf

40 Alerts on persons and objects issued for discreet checks or specific checks

The SIS II Working Group is expected to hold its last meeting in June 2022, after which it will carry out its tasks under the Coordinated Supervision Committee (CSC), which was established in 2019.

In 2021, the number of referrals received by the Authority in relation to data processed in SIS II increased significantly compared to previous years. In 2021, the Authority received 73 referrals from data subjects in relation to the processing of their personal data stored in SIS II. The majority of these requests were related to the exercise of data subject's rights (request for information, data correction, erasure), in which cases the Authority provided general information concerning the right and process of applying to the SIRENE Bureau and about the legal remedies available.

VII.2.2. Action plan for Hungary's Schengen data protection audit in 2019

In accordance with Article 15 of Regulation (EU) 1053/2013, the Authority had to draw up an action plan to implement the Commission's recommendations drafted on the basis of the report on the onsite evaluation visit of 6-11 October 2019 concerning Hungary's tasks related to data protection. When compiling the action plan, the Authority contacted the organs audited in 2019 concerned by the Schengen evaluation and monitoring mechanism, asking them to comment on each of the recommendations and state the activities (and deadlines) they could undertake to comply with the provisions of the European Commission's recommendations. Based on the responses of the SIRENE Bureau, the Ministry of Foreign Affairs and Trade, the National Alien Policing Directorate General and the Ministry of the Interior NYHÁT N. SIS Office, the Authority compiled its action plan for the recommendations made for the Schengen-related data protection audit, which was forwarded to the European Commission by the Department for European Cooperation of the Ministry of the Interior. With regard to the four recommendations concerning audit activities within the responsibilities of the Authority, it underlined the following envisaged activities in the action plan;

1. The Authority will incorporate the regular checking of alerts in SIS II in its procedures for monitoring the Schengen Information System.

2. In the interest of business continuity, the Authority will follow up on the findings and recommendations of previous audits, and it will incorporate the verification of their implementation into its next audit plan.

3. Under its monitoring activities concerning the Visa Information System (VIS), the Authority will monitor the practical implementation of the recommendations at the Ministry of Foreign Affairs and Trade and the National Alien Policing Directorate General.

4. In the course of its monitoring activities related to the Visa Information System, the Authority will also audit processing by external service providers.

The Authority has set a target date for the completion of the actions identified in the Action Plan for the end of 2022.

VII.2.3. The working group supervising the data protection of the Visa Information System (VIS Supervision Coordination Group)

The working group supervising the data protection of the Visa Information System (VIS Supervision Coordination Group) held two meetings by videoconference in 2021. The objective of the Visa Information System is to facilitate the implementation of the common visa policy, consular cooperation and consultations among the central visa authorities by way of the efficient identification of persons, who fail to meet the conditions of entry into, stay or establishment in the territory of the Member States.

In 2021, the working group worked on the development of a common audit plan, including a set of audit questions related to the Visa Information System Data Security Module, which each Member State can use in its own audit activities, similarly to the SIS II common audit plan. The working group will also develop an audit plan, building on the experience of previous years, to allow Member States' authorities to audit the data processing of so-called external service providers.

As regards VIS, NAIH's audit plan for 2021 did not include any onsite visit to a consulate in view of the virus situation. It is hoped that onsite inspections can be carried out again from 2022.

In 2021, the Authority received 6 requests in relation to the Visa Information System; in several cases, the data subjects wished to know more about the visa procedure. Typically, these requests were answered by way of providing general information, the submissions concerning specific cases were forwarded by the Authority to the competent bodies.

VII.2.4. The working group supervising the data protection of the Eurodac System (Eurodac Supervision Coordination Group)

The working group supervising the data protection of the Eurodac System (Eurodac Supervision Coordination Group) also had two meetings in 2021. The working group continued to address issues related to the modernisation of the Eurodac system in 2021.

The enhanced Eurodac database would be fully interoperable with border management databases as part of an integrated migration and border management system, thus helping to manage irregular migration, including the effective tracking of returned persons.

The European Commission informed the working group that the negotiations opened in connection with the Eurodac Regulation were not carried on during the Portuguese Presidency, but are expected to continue in 2022.

VII.2.5. Coordinated Supervision Committee – CSC

CSC carried out a survey concerning the Internal Market Information System (IMI) in 2021. The summary of the results of the survey stated that the number of those having access is very different in the individual Member States and proper information for the users is made more difficult by the fact that the number of users in the individual Member States may be of an order of magnitude of several hundreds or even thousands. There are differences between Member States as to where users can initiate the exercise of their data subjects' rights, with some Member States having one contact person designated, while others have one per body.

Member States also show considerable variation as to where users can initiate the exercise of data subject's rights as some Member States designate a single contact person, while elsewhere there is one each for each organ. There is no uniform practice concerning the information for the data subjects; in general, however, it can be stated that information on the IMI system is accessible in every Member State.

Over and above its survey concerning the IMI system CSC also consulted the data protection officers of Eurojust, as well as the European Public Prosecutors' Office (EPPO) to plan the future tasks of the working group.

In the future, CSC will become the single forum for the harmonised review of the large-scale EU information system. Through this, the authorities of the Member States will get a fuller view of the processing carried out by EU agencies in various systems; in addition, the planned IT cooperation (interoperability) between the various EU information systems may come into being and the supervisory activity of the authorities may become more effective. At the same time, this poses several new challenges to supervision and audits. The supervision of data protection for each large-scale IT system has its own legal framework requiring specific interpretation and the application of the law and communication between the systems has also to be supervised, hence efficient cooperation among the authorities of the Member States – ultimately coordinated by CSC – is going to be more important than ever before.

According to its procedural rules, CSC has to have at least two sessions a year, but taking into account the working groups within its powers (SIS II, EES, ETIAS, ECRIS-TCN, ECB – for the time being VIS, Eurodac and CIS are not included), presumably two sessions a year would not be sufficiently effective, so it is expected that more sessions will be held. Taking into account the three main areas (border control, police and judicial cooperation and IMI), the sessions can even be combined.

VII.2.6. Customs Information System Data Protection Working Group (Customs Information System – Supervision Coordination Group)

The task of the working group is the coordinated supervision of the Customs Information System (CIS) from the viewpoint of data protection with the participation of the data protection authorities of the Member States and the European Data Protection Supervisor. The purpose of the Customs Information System is to facilitate the prevention, detection and prosecution of the violation of the EU customs and agricultural rules. The heart of the system is a central database, to which Member State authorities can have access through a dedicated interface for uploading data and making queries.

In 2021, the working group had altogether one meeting in the form of a teleconference. OLAF's representative also participated in the meeting, who briefed the participants on the fact that the review of the CIS regulation continues to be a topical one. Also, a questionnaire was drafted whose purpose is to survey the targeted data protection training of the employees of Member State organisations having direct access to CIS.

VII.2.7. Europol Cooperation Board (ECB)

Europol supports the work of the law enforcement authorities of the Member States in combating international organised crime and terrorism by collecting, analysing and sharing data and coordination. ECB's task is to assist this work by providing advice. At the same time, it is expected that ECB will be terminated in this form in 2022 and its responsibilities will be transferred to the Coordinated Supervision Committee (CSC), such as, for instance, the SIS II Supervision Coordination Group and EES, as well as ETIAS. This means that CSC is going to fully cover the area of police and judicial cooperation and the new type of supervisory work will begin also in the field of border checks.

VII.2.8. Borders, Travel and Law Enforcement Expert Group (BTLE)

The expert group was actively involved in drafting the EDPB opinions 14/2021 and 15/2021 of 13 April 2021 concerning the adequacy decision affecting the United Kingdom. The former covers data transfers subject to GDPR, while the latter covers those subject to the Law Enforcement Directive (LED). In view of the fact that as of 31 January 2020, the United Kingdom officially left the European Union, it counts as a third country from the viewpoint of data transfers, hence data subjects must have safeguards, so that the level of protection ensured by the EU is not violated in the course of data transfers. These two opinions were borne of several rounds of lengthy discussions with the European Commission and also for this reason they can be regarded as significant milestones.

Another important activity of the working group related to adequacy decisions was to produce a professional statement on the EDPB opinion[41] drawn up in relation to the adequacy decision concerning South Korea. The opinion was adopted on 24 September 2021. In relation to this, the Chair of EDPB underlined the need for high-level data protection and support for EU relations with Korea. The opinion is of major significance also because South Korea is not an EU Member State, hence its legal order lacks EU traditions. The adequacy examination therefore required particular circumspection.

Beyond this, the BTLE expert subgroup also participated in drawing up joint opinion 5/2021 EDPS-EDPB adopted in relation to the draft Artificial intelligence (AI) regulation (18 June 2021). The opinion declares a general prohibition on using real time remote biometric identification systems with which a substantial part of

41 https://edpb.europa.eu/news/news/2021/edpb-adopts-opinion-draft-south-korea-adequacy-decision_hu

the Member States agreed. With the exceedingly rapid development of AI systems, the risk to fundamental rights affecting data subject rights increases so significantly that the operation of such system can be envisaged only if stringent safeguards of fundamental rights are imposed.

The first evaluation of the transposition of the Law Enforcement Data Protection Directive by the Member States to be carried out every four years became due in 2021 in relation to which the European Commission invited the data protection supervisory authorities of the Member States to answer a detailed questionnaire consisting of 47 points. Having summarised the answers, EDPB with the professional support of the working group adopted an evaluation document. In addition to providing a general overview of trends in each Member State, the document provides an opportunity to see the detailed responses of each Member State, thus meeting the requirement of transparency.

VII.3. International relations beyond EU cooperation – conferences

1. CEEDPA – Conference of Central and Eastern European Data Protection Authorities

The outstanding significance of the conference was given by the fact that the cooperation celebrated the 20th anniversary of its foundation in 2021.

In relation to the anniversary, Dr. Attila Péterfalvi, President of the Authority highlighted: "This cooperation was a highly useful forum for preparing for EU accession as the Member States had to face similar challenges. Since then, the number of participants expanded and today it has become a significant forum of cooperation for the Central and East European data protection authorities. Our members today include EU Member States and those awaiting accession. Because of the similarities in the political-legal establishments of these countries, the cooperation continues to be an excellent platform for solving the emerging data protection problems and for assisting one another's work through sharing the experiences and presenting the statements of the Member States."

Discussions at the conference were carried out in four major sections:

- Accountability mechanisms.
- How to protect our personal data following the Covid-19 pandemic?
- Implementation of the data protection standards of the European Union and the Council of Europe and the challenges of cross-border processingi.
- Key issues and challenges related to the protection of the personal data of children.

The celebratory meeting lasted two days and was organised as an online forum. The participants had an opportunity to share their experiences and practices in the course of the discussions concerning the key issues of the protection of personal data and they could present their plans for the coming years.

2. Meetings held on account of the 108+ Convention

This year also marked a significant anniversary for the Council of Europe's Convention 108. The 40th anniversary of the signing of the Convention took place on 28 January 2021. This Convention is the first legally binding international document in the field of data protection and it has served as a model for many other data protection regulations.

In 2021, three "bureau meetings" (24-26 March, 28-30 September, 20-22 December) and two plenary meetings (28-30 June, 17-19 November) were held online.

A number of important guidelines and recommendations were discussed and adopted during the meetings, two of which should be highlighted:

- Guidelines on the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns[42]
- Guidelines on facial recognition[43]

3. Global Privacy Assembly Konferencia

Since its creation in 1979, the GPA, with more than 130 members, has become one of the most important global organisations in the field of data protection.

The 43rd Global Privacy Assembly was held online in 2021, organised by Mexico.

The key documents adopted during the conference:

- Resolution on Children's Digital Rights[44]
- Resolution on Government Access to Data, Privacy and the Rule of Law: Principles for Governmental Access to Personal Data held by the Private Sector for National Security and Public Safety Purposes[45]

42 https://rm.coe.int/t-pd-bur-2021-3rev4-fin-draft-guidelines-political-campaigns/1680a4a36d

43 https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3

44 https://globalprivacyassembly.org/wp-content/uploads/2021/10/20211025-GPA-Resolution-Childrens-Digital-Rights-Final-Adopted.pdf

45 https://globalprivacyassembly.org/wp-content/uploads/2021/10/20211025-GPA-Resolution-Government-Access-Final-Adopted_.pdf

VIII. NAIH's projects

VIII.1. The Public Administration and Civil Service Development Operative Program (KÖFOP project)

The EU-funded priority project KÖFOP-2.2.6-VEKOP-18-2019-00001 "Mapping out the domestic practice of the freedom of information and enhancing its effectiveness in Hungary" is described in detail in the "Freedom of Information" section of the Report.

VIII.2. The Integrated Legislative System (IJR) Project

The Integrated Legislative System (IJR) project came into being among the projects designed to reduce the administrative burden on budgetary agencies financed on the basis of Government Decision 1004/2016. (I.18.) under the KÖFOP 1.0.0. – VEKOP-15 priority government project.

NAIH's procedural, administrative, IT and information security development adjusted to changes in legal regulations arising from its EU obligations was implemented under this project in 2017-2021. The Integrated Legislative System (IJR) Project was closed successfully on 31.08.2021.

Pursuant to Government Decision 1585/2016. (X. 25.), Amendment 1 to the grant contract of the IJR project was signed in April 2017, which named the Authority among the consortium partners, as well as the supported tasks arising from GDPR under the project.

Meeting the requirements of GDPR called for a full-scale optimisation, redesign and implementation of NAIH's legal professional fields in 2019, as well as the development and maintenance of an IT environment to support the redesigned processes, while ensuring flexibility in redesign. The implementation of these tasks continued also in 2021. The IRMA file management system was installed and its integration and introduction into the administrative module under the IJR project was carried out in 2021.

The 2017-2021 outputs of the IJR project include the administrative and the decision-editing modules, whose installation and the testing of organisational implementation was closed successfully.

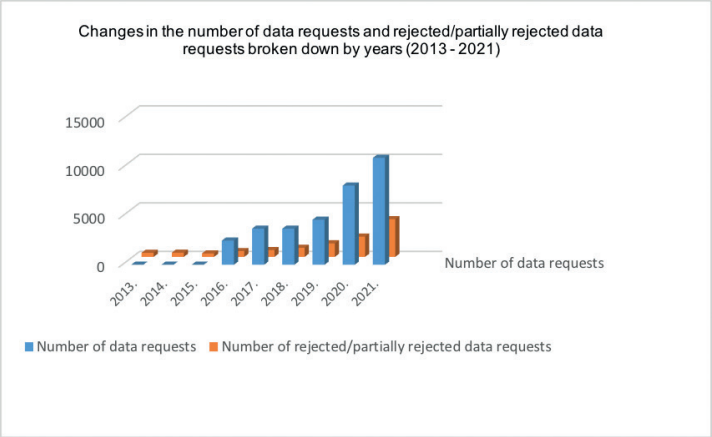
IX. Annexes

IX.1. Reports on rejected requests for data of public interest for the period 2013-2021 (frequency of application of each reason for rejection)

IX.1.1. Data series by year

Year	No. of data providers	No. of requests for public interest data (total)	Fulfilled	%	Rejected, partially rejectedt	%
2013.	114	no data	no data	-	424	-
2014.	156	no data	no data	-	431	-
2015.	162	no data	no data	-	984	-
2016.	228	2493	1900	76%	593	24%
2017.	223	3718	3016	81%	702	19%
2018.	256	3717	2882	78%	940	25%
2019.	443	4635	3306	71%	1393	30%
2020.	778	8162	5957	73%	2089	26%
2021.	997	11019	7127	65%	3881	35%

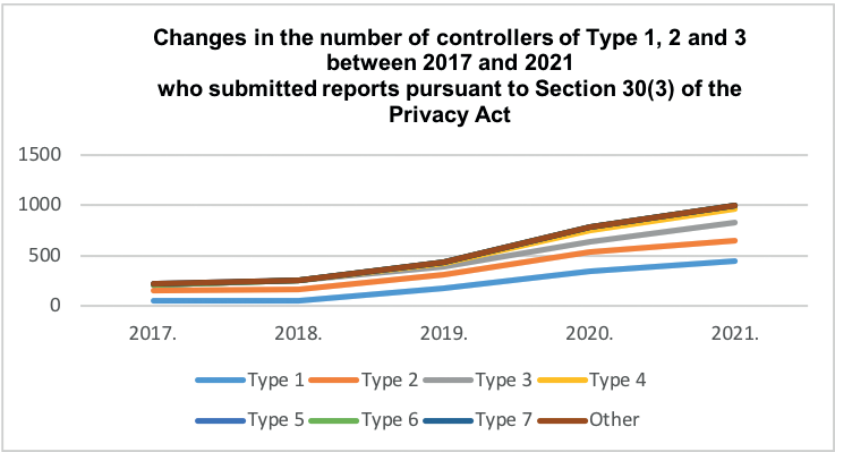
Table 1



IX.1.2. Breakdown of bodies providing data by type of body (2017-2021)

	Types 1[46]	Types 2[47]	Types 3[48]	Types 4[49]	Types 5[50]	Types 6[51]	Types 7[52]	Other[53]
2017.	46	101	56	3	1	0	11	1
2018.	50	109	92	5	2	0	0	0
2019.	177	130	77	37	12	2	0	0
2020.	338	192	109	114	26	1	0	0
2021.	447	200	176	144	30	2	0	0

Table 2

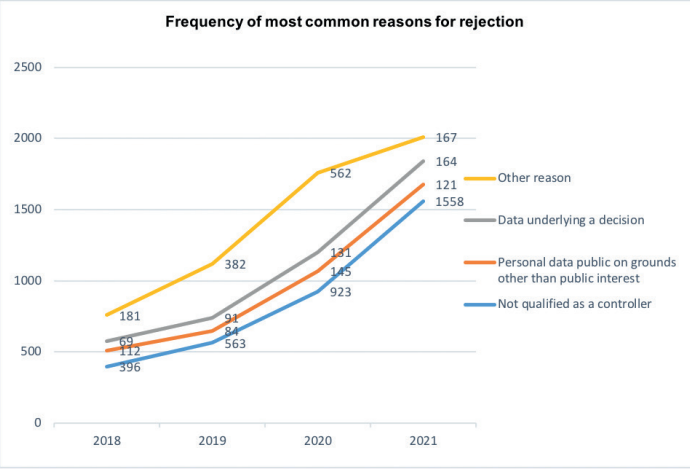


46 local, regional and national governments
47 bodies of central and regional public administration
48 bodies and public entities outside the public administration subject to publication requirements
49 educational, training and cultural institutions
50 health and social institutions
51 churches, religious organisations
52 financial institutions, banks
53 webshops

IX.1.3. Main reasons for rejection by year (2018-2021

Year	Reasons for rejecti-on (total	Does not qualify as controller	Personal data not in the pub-lic interest	Data for deci-sion-support (Article 27(5)-(6) of the Pri-vacy Act	Other reason
2018.	940	396	112	69	181
2019.	1393	563	84	91	382
2020.	2155	923	145	131	562
2021.	3881	1558	121	164	167

Table 3



IX.1.4. Characteristics of reports for rejected data requests in 2021

Under the project entitled *"Review of data sets subject to disclosure obligation under legal regulation"*, all the local governments and the national ethnic minority self-governments of the organs of the municipal subsystem were included in the test data requests. The project operators sent requests for data of public interest consisting of 6 questions compiled by the Authority to the Municipality of Budapest and 3,177 local governments, 19 regional government and 13 national ethnic minority self-governments in 2021. In addition to the municipal subsystem, the commitment for the freedom of information of central and regional organs of state administration (179 controllers) and 1,000 organs subject to disclosure obligation outside state administration in the other group (business organisations and foundations held by the state or municipalities) as well as public bodies were put to the test.

To assist with the fulfilment of the reporting obligation, the Authority put forward a proposal to use a datasheet, which contains data not only with regard to the reasons of data requests that were rejected or partially rejected, but also with regard to all the data requests submitted to the controller in the year of reporting and of these, those that were fulfilled. (The datasheet can be downloaded from the Authority's website in .pdf and .docx format.)

From the year of its introduction (2018), the number of organs, which fulfil their reporting obligation using the datasheet increased continuously and by 2022 close to 100% of the reporting controllers used the datasheet
Even though the number of controllers involved in the test data request was in the order of magnitude of several thousands, only 997 of them met their obligation according to Section 30(3) of the Privacy Act.

The analysis of the content of the reports drawn up by controllers on rejected requests for data of public interest in 2021 revealed that controllers frequently referred to the following reasons in addition to the reasons used often for refusing to disclose data (Table 3) in many cases:

- the data requested were not data of public interest - 390 cases;
- data requests were driven by personal interests, or the data request clashed with the principle of the proper exercise of rights - 436 cases;
- he person requesting the data failed to pay the cost reimbursement charged by the controller – 144 cases;
- in view of Constitutional Court Decision 13/2019. (IV. 8.) AB – 51 cases;
- with reference to Section 29(1)(a) of the Privacy Act – 90 cases;
- data not available – 268 cases.

IX.2. The financial management of the Authority in 2021

The Hungarian National Authority for Data Protection and Freedom of Information passed the 10th year of its operation and financial management as

of 31 December 2021. Below, we provide a brief presentation of the data related to its financial management.

IX.2.1. Revenue estimate and the data of its performance in 2021

The Authority received and accounted for other operating and non-operating grants to fund the priority project *"Mapping out the domestic practice of the freedom of information and enhancing its effectiveness in Hungary"*.

Of the revenue figures, the Authority's operating revenue does not show any significant change either in composition or in value compared to the 2020 budget year. However, the reimbursement of operating costs of almost HUF 6,500,000, paid by KEF, was outstanding, which was made ex post in the 2020 accounts.

The Authority's non-operational revenue was generated by the sale of 1 official vehicle, a filing container and some fixed assets written off to zero.

Rolling over the budget fund remaining from 2020 into a revenue estimate increases the original revenue estimate by HUF 329,314,000.

IX.2.2. Expenditure estimate and the data of its performance in 2021

By ensuring competitive salaries and creating new, decent working conditions, NAIH succeeded in reducing the extent of labour fluctuation and thus retaining highly qualified professionals.

The expenditure on payments to personnel and related employers' contributions was only 6% higher than last year. The increase was also influenced by a further small rise in staff numbers, a further reduction in the social contribution tax rate and, in some cases (e.g. cafeteria), tax exemptionst.

In 2021, two factors were of particular importance for the Authority's budget: the pandemic and the rise in expenditure for the Authority's operation in a new building. The former tended to result in cost savings, while the latter resulted in a substantial additional expenditure when looking at the Authority's figures for its operation. Expenditure on the upkeep of the new building was almost 82% higher than in the previous year.

Looking at capital expenditure, since most of the office furniture was already purchased by the Authority in 2020, this expenditure item is down to 1/3 compared to last year. However, the purchase of intangible assets of nearly HUF 100,000,000 gross, included in the KÖFOP project, brought the amount of the capital expenditure to almost the same level for the period under review.

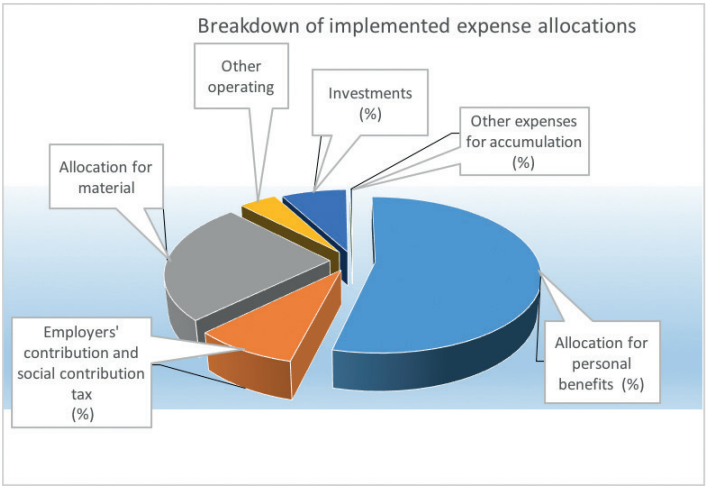
In the first days of January 2022, the Hungarian State Treasury introduced its new multi-currency account management system, which meant that the methodology of extraordinary salary advances (HUF 45,520,000) had to be used at the end of December 2021.

The residual amount from the Authority's core activities for 2021 is HUF 505,806,000, of which 98.2% is a committed residual amount.

MDescription	Original estimate	Modified estimate	Performance	Residue from core activities in 2021
Operational other support from chapterI		337 149	337 149	
Accumulation other support from chapterI		95 250	95 250	
Receipts acting as Authority		324	324	
Value of mediated services		97	97	
Invoiced VAT		459	459	
Exchange rate gain		144	144	
Other operational revenues		8 268	8 268	
Sale of tangible assets		4 204	4 204	
Recovery of loan for non-operational purposes		1 285	1 285	
Funds remaining from the 2020 budget		329 314	329 314	
Revenue from advance by General Government		45 520	45 520	
Grant from central budget from Managing Authority	1 604 200	1 616 549	1 616 549	
Revenue estimates total:	***1 604 200***	***2 438 563***	***2 438 563***	-
Estimates for payments to personnel	976 300	1 060 174	1 042 092	18 082
Employers' contribution and welfare contribu-tion tax	151 000	171 105	168 051	3 054
Estimate for material expenses	451 800	833 666	485 967	347 699
Other operational expenses		85 163	84 914	249
Investments	25 100	222 156	146 733	75 423
Renovations		15 779		15 779
Other non-operational expenditure		5 000	5 000	-
Financing expenses		45 520		45 520
Expenditure estimate tota:	***1 604 200***	***2 438 563***	***1 932 757***	***505 806***

The following table presents the figures for NAIH'S 2021 budget (in HUF '000)

The following graph shows the actual expenditures of the modified estimates in a percentage distribution:



IX.2.3. Changes in the headcount of the Authority

As of 31 December 2021, the Authority's headcount according to labour law was 108.

Headcount management is based on the Act on special statute bodies and the status of their staff (Küt.), namely, the Authority has five administrative (councillor, lead councillor, senior councillor I, senior councillor II, head senior councillor), and two managerial (one heading an independent organisational unit and one heading a non-independent organisational unit) job categories.

With competitive salaries since the introduction of Küt., staff fluctuation has been significantly reduced, with 8 staff leaving and 7 new staff joining during the year. In 2021, 4 staff became permanently absent due to child birth, while 3 returned from long-term leave

IX.2.4. Changes in revenues from fines

The amount of fines received in the Authority's account was HUF 74,364,000, which is in line with the average of previous years. It should also be noted that fines are not paid entirely to the Authority but to the central budget.

IX.3. Participation of the President of the Authority in Hungarian and international conferences and events of the profession in 2021

28 January 2021 – online conference organised by the Croatian Data Protection Authority: Digital transformation and data protection in a pandemic world - Attila Péterfalvi: *Developments in the field of data protection regarding SMEs – STAR II project*.

17 February 2021 – online conference – Meeting of the General Managers – *"The experience of the DPA in the light of the application of the GDPR"*

24 March 2021 – Budapest - The online inaugural conference of the project "*Mapping out the domestic practice of the freedom of information and enhancing its effectiveness in Hungary"*– Opening address

4 May 2021 – Budapest - OneTrust PrivacyConnect Budapest conference – *Roundtable discussion*

18 May 2021 – online international conference: *International Forum on Privacy and Data Protection – Attila Péterfalvi: National regulations and international challenges in the field of data protection in Hungary*

23 June 2021 – online conference – Public Administration Day Conference – *"Data protection and freedom of information in the context of the COVID-19 outbreak"*

24 September 2021 – Tata – The working session of the Working Committee on Public Administration of VEAB Economic, Legal and Social Sciences Committee on DATA PROCESSING AND INFORMATION SECURITY – *"Current issues on data protection and freedom of information"*

28 September 2021 – Budapest – Organised by the International Children's Safety Service *"The impact of the media on children and young people"* XIth Media Conference – *Data protection aspects of digital platforms*

12 October 2021 – Budapest – Organised by the Antall József Knowledge Center: thinkBDPSt Conference – Young Leader's Forum – *Data Breach Notification*

18-21 October 2021 – Organised by Mexico, online - *Global Privacy Assembly Conference*

19 October 2021 – Budapest – Organised by the József Attila Szabadegyetem: *"Spirit of the age"* an evening for professionals – *Current issues of data protection*

3 November 2021 – Budapest – Organised by the Home Affairs Science Council: Human-Centred Artificial Intelligence Conference – *Data protection requirements for the use of artificial intelligence*

30 November 2021 – Budapest – Organised by the Office of the National Police Headquarters: *A*nnual data protection conference– *Activities by NAIH – Experiences in 2021*

2 December 2021 – Budapest – End-of-year data protection conference by Adatvedelmi.hu – Activities by NAIH – Experiences in 2021

16-17 December 2021 – Organised by Poland online– *CEEDPA – Conference of Central and Eastern European Data Protection Authorities*

IX.4. Recipients of the NAIH Memorial Award

Based on NAIH's Rule 19/2012 on the Donation of the "Medallion of the National Data Protection and Freedom of information Authority", this medallion can be donated to whoever has reached high-level, exemplary achievements in the field of data protection, the right to informational self-determination and the freedom of information or has substantially contributed to the achievement of such results. The medallion, made of silver, is the work of goldsmith Tamás Szabó. It is donated annually on the occasion of the Day of Data Protection and Freedom of Informationr.

On 28 January 2021, the silver medallion was awarded to dr. Péter Báldy, Deputy Director of the Institute of Continuing Legal Education at the Eötvös Loránd University of Sciences for his outstanding work in organising the training of specialists and lawyers in data security and data protection law and for his outstanding work in promoting and disseminating legal knowledge on the protection of personal data.

IX.5. List of legislation and abbreviations referred to in the Annual Report

- Act CXI of 2011 on the Commissioner for Fundamental Rights (Ombudsman Act)
- Act CL of 2016 on General Administrative Procedures (Administrative Procedures Act)
- Fundamental Law, Hungary's Fundamental Law (25 April 2011)
- General Data Protection Regulation: see: GDPR
- AVSZ: Data Change Management Service
- Act XC of 2017 on Criminal Procedure (Criminal Procedures Act)
- Law Enforcement Directive, Directive on the protection of personal data processed for law enforcement purposes, Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and on the free movement of such data and repealing Counsel Framework Decision 2008/977/JHA
- CIS: Customs Information System
- CSC: Coordinated Supervision Committee (Committee for the joint supervision of large-scale information systems in the European Union)
- EEA: European Economic Area
- ECB: Europol Cooperation Board
- EDPB: European Data Protection Board
- EDPS: European Data Protection Supervisor
- EESZT: Egészségügyi Szolgáltatási Tér (Health Service Space)
- EET: Human Resources Support Management
- EMMI: Ministry of Human Resources
- EPPO: European Public Prosecutor's Office
- CJEU: Court of Justice of the European Union
- Health Data Act, Act XLVII of 1997 on the Processing and Protection of Health and Related Personal Data
- Health Care Act, Act CLIV of 1997 on Health Care
- GDPR, General Data Protection Regulation: Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC. To be applied from 25 May 2018.

- IMI system: Internal Market Information System
- Privacy Act, Act CXII of 2011 on the Right of Informational Self-Determination and the Freedom of Information
- IRMA: internal administrative system
- ITM: Ministry of Innovation and Technology
- KAÜ: Központi Azonosítási Ügynök (Central Identification Agent)
- Act IX of 2021 on public interest trusts performing public functions
- Act CXL of 2004 on the General Rules of Administrative Procedure and Services
- Act LXIII of 1999 on Public Space Surveillance
- Act CXXII of 2009 on the operation of publicly owned companies with increased efficiency
- KNBSZ: Military National Security Service
- Act CXCIX of 2011 on Public Service Officials
- LED: Law Enforcement Directive
- MÁK: Magyar Államkincstár (Hungarian State Treasury)
- Act CLV of 2009 on the Protection of Classified Data
- AI: artificial intelligence
- Labour Code, Act I of 2012 on the Labour Code
- Act CLXXXV of 2010 on Media Services and Mass Communications
- Act CXXV of 1995 on National Security Services
- NEAK: Nemzeti Egészségbiztosítási Alapkezelő (National Health Insurance Fund)
- Act CCIV of 2011 on National Higher Education
- NMHH: Nemzeti Média- és Hírközlési Hatóság (National Media and Infocommunications Authority)
- Act LXVI of 1992 on the registration of personal data and addresses of citizens
- PNR Directive, Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime
- Project Act, Act VII of 2015 on the investment related to the maintenance of the capacity of the Paks Nuclear Power Plant and amending certain related acts
- Civil Code, new; Act V of 2013 on the Civil Code
- Civil Code, old; Act IV of 1952 on the Civil Code
- SIS: Schengen Information System

- SIS II, Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second-generation Schengen Information System (SIS II)
- VIS: Visa Information System
- VIS regulation, Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas

Other legislation:

- Government Decree 350/2011. (XII. 30.) on certain issues of NGO management, fundraising and public benefit
- Act CXXVI of 2010 on the Government Offices of the Capital and the Counties and on the Amendments to Acts related to the Establishment of the Government Offices of the Capital and the Counties and to Territorial Integration
- Decision 29/2021. (XI. 19.) EMMI on protective measures in public education during the pandemic period
- Act CXXXI of 2010 on Social Participation in the Preparation of Legislation
- Act CXXVIII of 2011 on Disaster Management and Amending Certain Related Acts
- Act LIII of 1995 on the General Rules for the Protection of the Environment
- Act XXXI of 2021 Amending Certain Laws on Law Enforcement Administration in order to Strengthen Public Security
- Act XCIII of 1993 on Occupational Safety and Health
- Act LXVI of 1992 on the registration of personal data and addresses of citizens
- Government Decree 523/2020. (XI. 25.) on the partial compensation of revenue lost due to cancelled bookings by accommodation providers
- Government Decree 314/2012. (XI. 8.) on the settlement development concept, the integrated settlement development strategy and settlement planning instruments, as well as on certain specific legal instruments of settlement planning
- Act XIII of 2021 on the Allocation of Property
- Government Decree 484/2020. (XI. 10.) on the second phase of protection measures to be applied during an emergency
- Government Decree 521/2020 (XI.25.) on the derogation from certain provisions on data requests in times of emergency
- Government Decree 27/2021. (I. 29.) on the declaration of a state of emergency and the entry into force of emergency measures

- Act LXXXI of 2001 on the promulgation of the Aarhus Convention
- Act CLXXXVIII of 2015 on the Facial Image Analysis Register and the Facial Image Analysis System
- Government Decision 1413/2021. (VI.30.) on the provision of conditions and resources necessary for the operation of certain higher education institutions and certain public foundations performing public functions
- Act CVIII of 2001 on certain aspects of electronic commerce services and certain issues related to information society services
- Decree 2/2016. (IV. 29.) MvM on preliminary and ex-post impact assessment
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
- Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA
- Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816
- Regulation (EU) 2019/1157 of the European Parliament and of the Council of 20 June 2019 on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement
- Act LIV of 2018 on the Protection of Trade secrets
- Tromsø Convention, Council of Europe Convention on Access to Documents containing Data of Public Interest (CETS No.205., promulgated in Hungary by Act CXXXI of 2009)

Table of Contents

Nemzeti Adatvédelmi és
Információszabadság Hatóság

1055 Budapest, Falk Miksa utca 9-11.
Postal address: 1363 Budapest, Pf. 9.

Phone: +36 (1) 391-1400
Fax: +36 (1) 391-1410

Internet: http://www.naih.hu
e-mail: ugyfelszolgalat@naih.hu

Published by: Nemzeti Adatvédelmi és Információszabadság Hatóság -
Hungarian National Authority for Data Protection and Freedom of Information
Responsible publisher: Dr. Attila Péterfalvi president
ISSN 2063-403X (Printed)
ISSN 2063-4900 (Online)

Nemzeti Adatvédelmi és Információszabadság Hatóság

1055 Budapest, Falk Miksa utca 9-11.
Postal address: 1363 Budapest, Pf. 9.

Phone : +36 (1) 391-1400
Fax: +36 (1) 391-1410
Internet: http://www.naih.hu
E-mail: ugyfelszolgalat@naih.hu

**Published: a Nemzeti Adatvédelmi és Információszabadság Hatóság –
Hungarian National Authority for Data Protection and Freedom of Information
Responsible publisher: Dr. Attila Péterfalvi president
ISSN 2063-403X (Nyomtatott)
ISSN 2063-4900 (Online)**