Annual Report
of the
National Authority for Data Protection and Freedom of Information
(NAIH)
2018

National Authority for Data Protection and Freedom of Information
Budapest, 2019

Preface

To the Reader

As of 25 May 2018, the Member States of the European Union have been obliged to apply the rules of the EU Data Protection norm, the General Data Protection Regulation, the GDPR, adopted in 2016. 2018 also saw the transposition into Hungarian law of the other legislative act forming part of the Data Protection Reform package, the Police Directive, and also the amendment of Act CXII of 2011 on the Right to Informational Self-determination and on the Freedom of Information (even though somewhat later than expected), which established the appropriate legal basis for the operation, proceeding, and law interpretation of the Hungarian supervisory authority. We have thus come to an important milestone in a legal process. This process however has not yet been concluded, as the application of law faces many new and stimulating challenges day by day, while the 'adaptation' to the GDPR of several other (sectoral) laws with data protection provisions are either in progress or will require future legislative work.

If we look back in time, it took more than four years to adopt the EU Data Protection Reform package, including the preparation and negotiation of proposals, as a result of an unbelievably complex yet coordinated legislative procedure. The Treaty of Lisbon and the Charter of Fundamental Rights of the European Union, with the right to the protection of personal data as a fundamental right being enshrined in Article 8 of the latter, have created an unprecedented opportunity for the harmonizing and law unification of data protection regimes of the Member State. Gradually, the frameworks of the cooperation mechanisms, 'one-stop-shop' administration, have been put in place. The national supervisory authorities have started to operate their data-breach notification systems, the first investigations under the GDPR have been concluded, and, exercising their corrective powers, the data protection authorities have imposed data protection fines under the renewed provisions—in other words, the complicated mechanism, the first cogwheels of which were put in place by the GDPR, has started to operate. This has attracted a great deal of attention and interest from both the professional and lay public, which naturally implies added responsibility for us. It will only be possible and worthwhile to render a full assessment in the future, nevertheless National Authority for Data Protection and Freedom of Information; hereinafter: 'NAIH') has closed this preparation stage in 2018 fortunately without major failures.

The legal background of the other informational fundamental right, freedom of information, that NAIH supervises did not change, but the thirty-year history of introducing this right in Hungary may afford the formulation of certain basic principles and the drawing of some conclusions. On 22 November 2018, the Government published its decision specifying the flagship Project 'The Review of the Scope of Data to Published by Law' (KÖFOP [Public Service Development Operative Programme 2.2.6.–VEKOP [Competitive Central Hungary Operative Programme]–18). The several-year project aims to review and survey the scope of data to be published according to Hungarian law and, on this basis, to ensure further access

to data in order to increase transparency on the basis of scientific researches and surveys. This project would enable a comprehensive examination of the information providing practice of organs and organizations performing public duties in Hungary, the identification of the problems of efficiency, application of law, and law abidance, as well as factors obstructing transparency, and the preparation of proposals for intervention in their management. The NAIH pays special attention to the call to the tender, and looks forward to its possible participation in it, because this would be a remarkable opportunity to form a reliable and comprehensive view of the transparency of the operation of the public sphere in Hungary, the efficiency of the legal regulation system of the freedom of information, of the difficulties, obstructions, and 'good practices' encountered.

Budapest, 1 March 2019

Dr. Attila Péterfalvi
Honorary University Professor
President of the National Authority for Data Protection and Freedom of Information

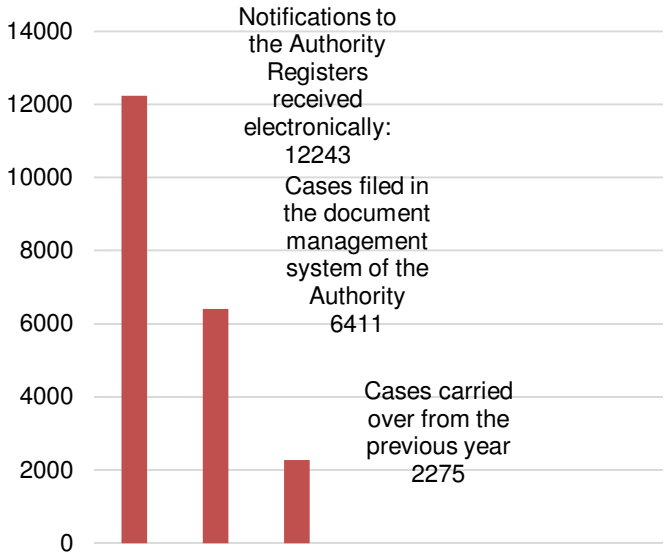
I. Statistical figures on the Activities of the Authority

I.1. The Statistical Features of Our Cases

Since the foundation of the NAIH on 1 January 2012, 2018 was the seventh year of its operation. As of 25 May 2018, 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 of such data, and repealing Directive 95/46/EC (General Data Protection Regulation; hereinafter: 'the GDPR') has been applicable.

Due to the changes in the legal environment, the statistics chapter of the 2018 report presents the data on the operation of the Authority in a way different from the accustomed. The Authority filed 18,654 new cases in 2018. 6,411 new cases went on to be administered in the

The number of cases with the Authority in 2018

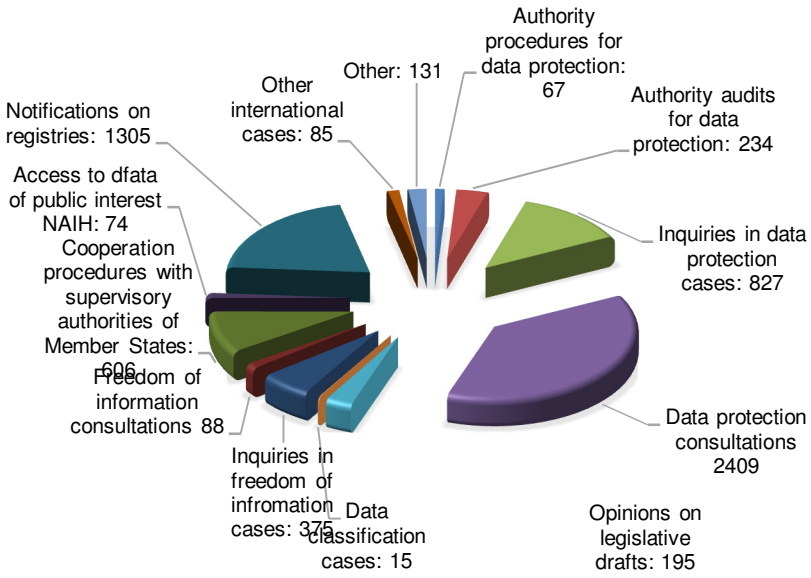


document management system of the Authority, while 12,243 notifications were received in the electronic registers (the Data Protection Register and the Data Protection Officer Register) of the Authority. The notifications received by the electronic registers of the Authority are filed electronically, separately from the document management system of the Authority.

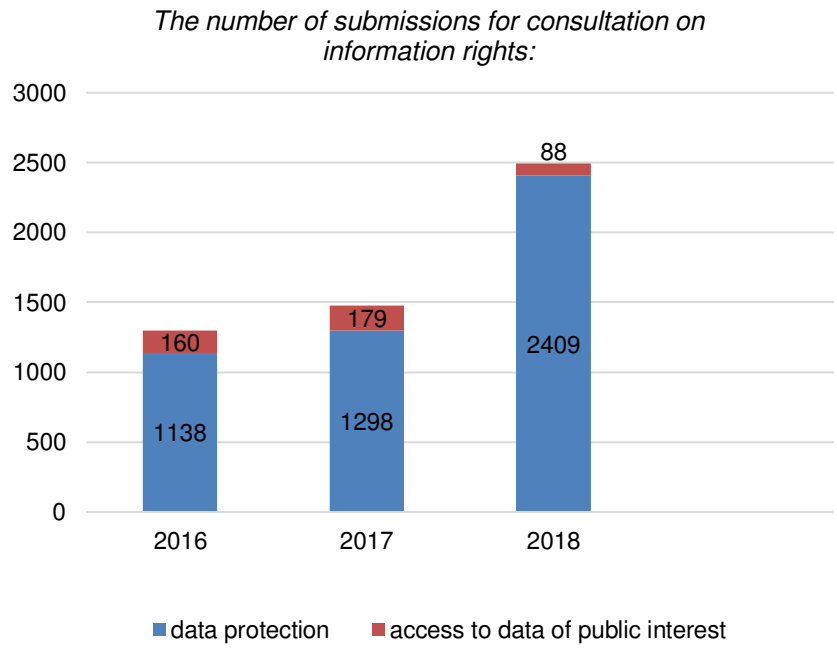
The number of cases increased in comparison with that of the previous year. The increase was perceivable in spite of the fact that the legal institution of the Data Protection Register

the Authority had kept terminated following 25 May 2018, as thus did the obligation of notification by data controllers, and the number of submissions for consultation on notification to the Data Protection Register also decreased significantly.

The Cases of the Authority Commenced in 2018

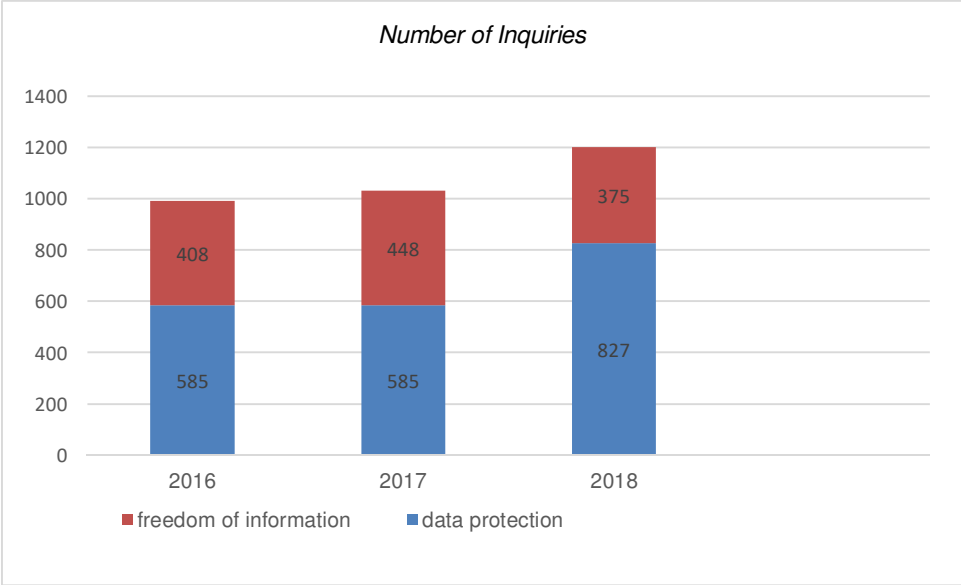


The number of submissions for consultation received by the Authority nearly doubled in comparison with former years' figures, implying significant workload for the Authority. 2,409 of them concerned data protection, and 88 access to data of public interest or data accessible on public interest grounds. The great number of submissions for consultation on data protection — where citizens, data controllers or organs performing public duties request counsel or information on the data processing issues they described — demonstrate that there was a great deal of uncertainty concerning the GDPR.



As a result of the moderate legislative activity due to the parliamentary elections of 2018, a lesser number of draft legislation was referred to the Authority for reporting. The Authority delivered its opinion on 195 pieces of draft legislation, but it ex officio monitors legislation activity concerning information rights, and, where necessary, ex officio delivers its opinion on draft legislation or amendment proposals submitted after setting the agenda.

Out of the 1205 inquiries, 827 were on data protection and 375 on freedom of information. The number of inquiries in data protection significantly increased in 2018.

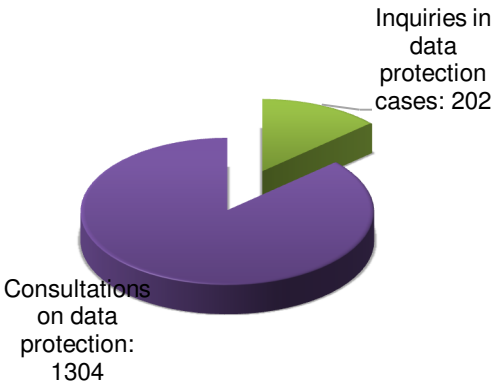


The Authority did not commence any authority procedures for data protection in the period between the GDPR becoming applicable, i.e. 25 May 2018, and the coming into effect of Act XXXVIII of 2018 on the amendment of Act CXII of 2011 on the right to informational self-determination and on the freedom of information (hereinafter: 'the Privacy Act') in

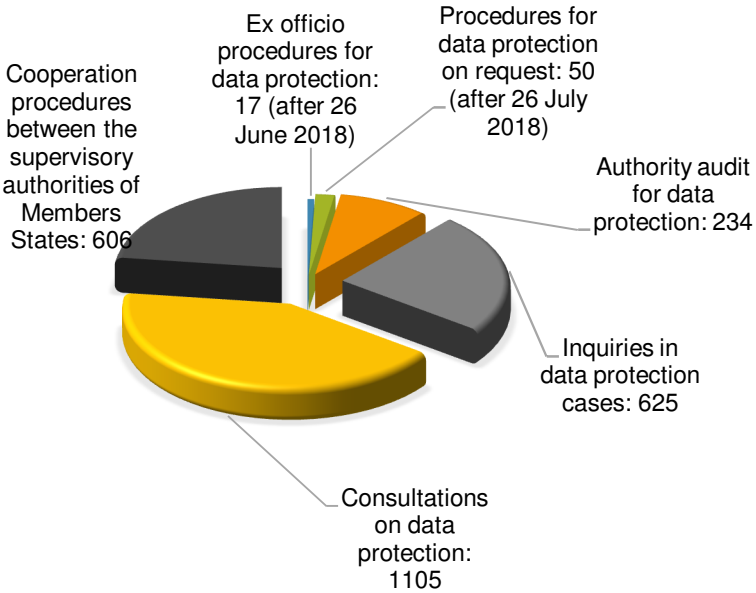
connection to the Data Protection Reform of the European Union and other related Acts (hereinafter: 'the Amendment Act'), i.e. 26 July 2018, due to the fact the prescription necessary for the Authority procedures to comply with the GDPR came into force following the adoption of the Amendment Act.

In this period the Authority used its ombudsman-type of means provided for by the Privacy Act, that is it examined the complaints it received by way of inquiry procedures.

Proecedures for data protection in the period before the GDPR becoming applicable



Procedures for data protection following the GDPR's becoming applicable



Following 26 July 2018, authority procedures did commence on complaints, out of which 50 were initiated on data subjects' request and 17 ex officio.

There is a continued opportunity to initiate inquiries in data protection cases.

The Amendment Act provided for the opportunity of initiating ex officio inquiries in data protection cases where other authorities signal, or the Authority itself detects, that there has been an infringement in respect of the processing of personal data, or there is an imminent danger thereof, and the initiation of an authority procedure for data protection is not obligatory under the Privacy Act.

After 26 July 2018, the Authority received 1,105 submissions for consultation, and initiated 625 inquiries.

The cooperation procedures of supervisory authorities of the Member States are the cooperation and consistency procedures under Articles 56 and 60–67 of the GDPR. In the course of cooperation procedures the supervisory authorities of Member States use the Internal Market Information System of the European Union.

In 233 cases the Authority examined, in the framework of audits for data protection, the fulfilment of obligations by data controllers in incidents, and examined the lawfulness of purpose in one further case.

The Authority had 15 cases in connection with classified data in 2018.

The Authority received 74 requests to access data of public interest, 59 of which it fulfilled, 3 it fulfilled in part, and 12 it rejected.

Prior to the application of the GDPR, the Authority received submissions concerning the data protection register (1,086) in significant numbers; prior to the start of the Data Protection Officer Notification System, there were 219 notifications of DPOs by postal or electronic mail, and 85 international cases. The number of cases filed as ‘other’ was 151, which includes, among others, cases not falling within the competence and scope of duties of the NAIH, as well as cases related to the operation and management of the Authority.

The Authority received over 2,800 telephone calls in 2018. The number of calls were exceptionally high in the month when the GDPR became applicable, and was higher in the month following it than in the beginning of the year.

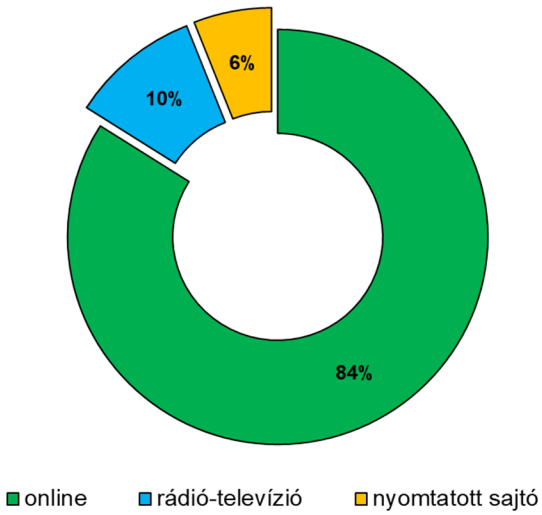
The Authority provided personal customer service in 27 cases as per appointment and in 24 cases without appointment, where data subjects submitted complaints with regard to processing of personal data or infringements of the right of access data of public interest or data accessible on public interest grounds, exercised their rights to access to documents on procedures.

The Authority provided a dedicated electronic surface for data controllers and processors for notifying data protection officers from 17 November 2018. 1,786 notifications were received in the DPO Notification System in 2018.

I.2 Media Coverage of the National Authority for Data Protection and Freedom of Information

By way of summary, there were 5,016 pieces of news in the media concerning the NAIH between 1 January and 31 December 2018. It was in the Online media that the activity of the Authority was most often reported, running 4,229 news items (84%). The printed press published 309 articles on the NAIH (%), while the electronic media 478 (10%).

Media Coverage of the NAIH in 2018



Online 84%
Radio and television 10%
Printed press 6%

II The Application of the General Data Protection Regulation

II.1 Data Protection Cases

II.1.1 NAIH Procedures

The GDPR's becoming applicable naturally brought about significant changes in the operation of the NAIH. The Hungarian data protection authority was also required to review and re-examine its activities, and thus modified them in terms of both material-law and procedural issues.

In order to ensure the concord of the procedures of the Authority with the rules of the GDPR, the Privacy Act had to be amended. Due to regulatory problems, no data protection procedure was initiated at the Authority in the period between 25 May 2018 and the coming into effect of the amendment of the Privacy Act.

In this period, the Authority deployed its ombudsman-type of means that had been provided for by the Privacy Act previously; that is it examined complaints filed with it in the framework of the inquiry procedure. In the event of an infringement found, it required the data controller to remedy the infringement, but this type of procedure does not enable the imposition of fines.

The Amendment Act came into effect as of 26 July 2018. To ensure concord with the GDPR, the Amendment Act introduced the authority procedure for data protection at the application of the data subject. This is based on the right of the data subject to lodge a complaint with a supervisory authority provided for by Article 77 of the GDPR, according which every data subject shall have the right to lodge a complaint with a supervisory authority if he or she considers that the processing of personal data relating to him or her infringes the Regulation.

From 26 July 2018, therefore, authority procedures for data protection on application of data subjects were initiated in accordance with the rules set forth by the GDPR, the amended Privacy Act, and the Code of General Administrative Procedure.

The most typical subjects with which applications for authority procedures were filed include the following:

- data processing at workplace;
- right of access;
- healthcare data processing;
- data processing related to claim assignment;
- camera surveillance;
- the rejection or omission of fulfilling data subject rights;
- data processing by banks.

If the data subject citizen wishes to have his or her application to be examined in the framework of an authority procedure, his or her submission has to meet formal and substantive requirements. (Applications by e-mail primarily result in inquiry procedures.)
In accordance with Section 60 (5) of the Privacy Act, applications shall contain the following:

- the identification of the alleged infringement;
- the description of the concrete conduct or state resulting in the alleged infringement;
- the data available to the applicant and necessary for the identification of the controller or processor committing the alleged infringement;
- the facts that support the statements related to the alleged infringement, as well as the evidences of such facts; and
- an explicit request to adopt a decision on remedying the indicated infringement.

The application shall also include data for the identification and the contact details of the data subject and his or her representative.
In the case of a deficient application, the Authority shall once, designating the deadline and the legal consequences of the omission, call upon the applicant to remedy the deficiency. If the applicant fails to remedy the deficiency, the Authority shall terminate the procedure. This occurred in numerous cases in the course of 2018.

If it so considers, the Authority may commence an authority procedure for data protection *ex officio.* Commencing an authority procedure is obligatory where

- it is preceded by an inquiry, and the infringement found was not remedied or its imminent threat was not eliminated in the course of the inquiry procedure, or
- the Authority finds on the basis of its inquiry that an infringement related to the processing of personal data has occurred or there is an imminent threat of such an infringement, and a fine may be imposed according to the provisions of the GDPR.

The time provided for completing an authority procedure for data protection is 120 days. If the Authority does not terminate the procedure, or does not come to a decision on the merits of the case, within 90 days of the submission of the application, it shall notify the data subject of the actions in the procedure it has taken.

Following 26 July 2018, authority procedures for data protection were commenced in 57 cases, out of which ex officio procedures were commenced in 8 cases, and the rest upon application. Until the compilation of this report, 27 decisions were made, most of which (17 cases) were termination of procedure due to the applicants failing to fulfil requests to remedy deficiencies of their submissions, the data processing objected to occurred pre-GDPR, or the Authority found on the basis of the documents submitted that the case did not fall within its competence. In three instances, the Authority dismissed applications due to lack of competence.

Decisions in favour, or partially in favour, of applications were made in 7 cases, in 3 of which the Authority imposed a fine on the data controller, and in 1 of which it imposed an administrative fine.

By way of notification, anyone can continue to initiate an inquiry procedure for data protection if he or she considers that the processing of personal data infringes rights or there is an imminent threat thereto.

With the Amendment Act coming effect, the Authority may commence an inquiry for data protection ex officio if other organs indicate, or the Authority itself detects, that the processing of personal data infringes rights or there is an imminent threat thereto, and the commencement of an authority procedure is not mandatory under the Privacy Act. An inquiry procedure does not constitute an administrative authority procedure, and is to be applied using the derogations defined by the GDPR alongside the provisions set forth by the Privacy Act.

II.1.1.1 Experience Gained in the Use of the Internal Market Information System

The appearance of a new procedural phase has brought about a significant change in the NAIH's order of procedure—the phase of formalized cooperation with other data protection authorities in the European Union as defined by the GDPR.

Before the data protection reform, Directive 95/46/EC (hereinafter: the 'Data Protection Directive') had provided for no detailed rules of cooperation between Member States. In

order to remedy this deficiency did the GDPR prescribe the cooperation procedure whereby Member States are to proceed jointly in cross-border cases (GDPR Article 60).

In the cooperation and consistency procedures under Article 56 and 60–67 of the GDPR, the supervisory authorities of the Member States are to use the Internal Market Information System of the European Union (hereinafter: 'the IMI'). Functionally, the IMI serves exclusively and only the purposes of communication between supervisory authorities (thus decision making e.g. takes place not within the IMI), which is assisted by modules designed to take into account the requirements of the individual procedures under the GDPR (e.g. there is a special module for running the joint operations of the supervisory authorities, which is indeed only part of the procedure under Article 60 of the GDPR).

The majority of the cases received by the Hungarian supervisory authority through the IMI was requests to identify the supervisory authority concerned under Article 56 of the GDPR. Until 12 December 2018, 500 such requests were received. The result of the procedures under Article 56 can essentially be regarded as the preliminary question of the procedure to be conducted by the lead and the concerned supervisory authorities under Article 60, because it is following the determination of the lead and concerned supervisory authorities that the procedure under Article 60, or, in its framework where necessary, the procedure under Article 61 and/or 62, takes place. An authority participates in procedures under Article 56 when the nature of data processing is cross-border, and the Hungarian authority qualifies as supervisory authority concerned within the meaning of Article 4 point 22 of the GDPR because the data controller is either established in Hungary or the data processing substantially affects, or is likely to substantially affect, data subjects residing in Hungary. To date, it has only been occasionally that the quality of supervisory authority concerned was established by reference to the fact that the data subject submitted the complaint to the Hungarian authority.

It was somewhat more than half of the some 500 cases under Article 56 received through the IMI in 2018 where the role of the Hungarian supervisory authority as an authority concerned arose, but it is important to note that the procedure in roughly 290 cases is still in progress, and it has not been decided yet whether the Hungarian authority is to be considered as an authority concerned or not.

A significant number of the cases under Article 56 received by the Hungarian authority concern data controllers operating popular social media surfaces and search engines; complaints frequently had to do with the full or partial lack of information due to data subjects on the circumstances of data processing by providers of services (GDPR Articles 12–14), with requests of erasure (GDPR Article 17), and with the fulfilment of declarations of objection (GDPR Article 21). In several cases, submitters protested that the data controllers of especially social media surfaces and sometimes smart phone software assistance services base, or wish to base, their data processing activities on the consent of the data subjects even when they had no opportunity to make a separate statement of consent as provided for by Article 4 point 11 of the GDPR in respect of the purpose of data processing and the scope of data to be processed (a typical turn of phrase by data controllers objected to is: 'by using this service you give consent to XY data controller accessing your search data'.

To deliver its opinion, the Authority received several submissions in cases under Article 56 that were related to the data required by service providers for personal identification as a precondition of exercising data subject rights, e.g. several service providers required scanned copies of personal identification certificates for this purpose, and, in one instance, the Authority itself commenced a procedure under Article 56 against a data controller pursuing such a practice.

Procedures under Article 56 are applicable in cases of personal data breach even when the supervisory authorities concerned in the personal data breach need to be identified.
Out of the cases commenced with the NAIH and requiring IMI communication, the Hungarian authority initiated a procedure under Article 56 in 7 cases until the end of December 2018. The NAIH has assumed a lead supervisory authority role in the examination of the data processing of a public transport firm where data subjects in Romania, Germany, and Great Britain objected to the data processing. The French data subject was unable to exercise his right of erasure under Article 17 of the GDPR by way of his compliant, and the Romanian data subject objected to the processing of his personal data for marketing purposes. As the effective and real exercise of data processing activity of the data controller through stable arrangements takes place in Hungary, the Hungarian authority proceeds as the lead supervisory authority when cross-border data processing occurs.

According to the experience of the Authority, the procedure under Article 61 (the so-called mutual assistance) can be applied so as, on the one hand, authorities can call the attention of one another to important pieces of information concerning concrete cases and data controllers, and so as, on the other hand, that experience concerning the legal issues of implementing the GDPR (e.g. do DPOs have to be designated in trade unions; the interpretation of 'neighbour camera' data processing and data processing for household purposes; the responsibility of joint controllers in applying the GDPR; and the experiences of authorities in applying Article 55 (3) of the GDPR in view of the fact that the data processing of the courts related to their judicial activities does not fall within the competence of supervisory authorities) can be exchanged. The Hungarian authority initiated procedures under Article 61 of the GDPR in several subjects matter—in, apart from notifications of 2 data-breach cases, the general issues partly mentioned above, such as whether the designation of DPOs are obligatory for trade unions or not; camera surveillance; and the publicity of court trial records, as well certain activities of private investigators.

The NAIH also participates in procedures where, as a supervisory authority concerned, it delivered its opinion on the measures taken or decisions made by other supervisory authorities (the lead supervisory authority submitting its draft decision in the case to other supervisory authorities concerned for obtaining their opinion on it).

Such a case was the procedure initiated against a data controller providing hotel services where the French data protection authority sent its draft decision to the Hungarian authority as authority concerned. The procedure had been commenced on the data processing related to a loyalty programme, where the data controller had required copies of personal identification documents as a condition of exercising data subject rights. Whereas, according the GDPR, the data controller does have to confirm the identity of the data subject when he or she is exercising data subject rights but only when reasonable doubt arises in this regard.

In such a case, it may request the data subject to provide information to confirm his or her identity under Article 12 (6) of the GDPR. However, in accordance with the principle of data minimisation, this may not lead to requiring more data than necessary from the data subject, and the requested documents must be relevant and proportionate to that purpose.

It was therefore disproportionate to require the personal identity certificate from a person who had submitted his or her request in a place where he or she had already been identified. It is reasonable however to require personal identification when the suspicion of identity theft or document forgery arises.

The Authority fundamentally agreed with the draft decision, but called attention to the fact that certain identifiers may only be processed by organs authorized to do so by national law, and thus, in the case of such regulation by a Member State, the data protection notice must provide for this too, and the Authority also made note of the fact that, with regard to documents with facial images, facial images may not always be regarded as necessary for data processing.

II.1.1.2 The Provision of Information and Consultation by the Authority

In the reporting period, especially in the weeks before and after the GDPR's coming into force, the number of submissions expressing interest or requesting information and opinion gradually increased, which demonstrates that there was significant uncertainty about the implementation of the provisions of the GDPR among law appliers.

Numerous requests were received by the Authority concerning the implementation and interpretation of the GDPR, but the scope of action of the Authority in this regard is limited, because the authentic abstract interpretation of the GDPR falls within the competence of primarily the European Data Protection Board. The Authority therefore continues to regard the remedy of infringements of data subjects and the appropriate application of data protection prescriptions as its primary duty. This does not however affect the prior consultations to be conducted depending on the results of data protection impact assessments, the possible meetings held in the framework certifications, and the fulfilment of obligations to provide information under law.

A significant part of the requests filed with the Authority was made up of submissions by data controllers aiming at the assessment of concrete activities and operations of data processing. It is the duty of the Authority neither under the GDPR nor section 38 of the Privacy Act to carry out the assessment of a given data processing and to deliver a prior opinion of its compliance with law or to conduct consultations on data protection matters. Such activity would even be significantly beyond its resources. All the criteria of data processing are available to the data controller, and it is the one primarily capable of assessing the measures required for compliance with law; as a consequence of the principle of accountability provided for by the GDPR, the Authority cannot take over the responsibility of the data controller in this regard. In view of the above, it is primarily the data controller that is capable of telling what technical and organizational measures are necessary for compliance with the requirements of the GDPR in concrete situations, as this requires the full knowledge of all the characteristics of the data processing, which are available to the

data controller. A full vetting of a given data processing can only be done through a full-scale examination of its legal and informatics measures. The Authority no longer carries out such audit procedures, because, the GDPR having come into effect, the possibility of providing data processing audit services ceased to exist for the Authority. The abstract interpretation of law, guidance, and delivery of opinion are the duties of the European Data Protection Board, and, due to this and the principle of consistency, the Authority deems itself entitled to deliver opinions only in exceptional cases, where domestic law is concerned.

As result of the changes in legal environment, the role of the European Data Protection Board in ensuring legal consistency, and the great number of requests received by the Authority to deliver its opinion on individual cases—also with a view to its resources necessary for its inquiries and authority procedures—the Authority, as a rule, does not issue individual opinions is response to requests for the interpretation and explanation of the prescriptions on the protection of personal data, especially not when the questions are not on the exercise of data subject rights and not from data subjects that are natural persons.

The GDPR prescribes the duties of promoting the awareness of controllers and processors of their obligations under the Regulation and of providing information, upon request, to any data subject concerning the exercise of their rights (Article 57 (2) d)–e)). In 2018, the Authority sought to comply with this of its obligations by way of notices published on its website and information provided in response to individual requests by data subjects, data controllers, professional and civic organizations, and law firms. As determined by the GDPR, the Authority fulfils this role by participating in the activity of the European Data Protection Board to ensure legal consistency.

In the reporting period, several requests were filed with the Authority about what kind of internal rules are to be adopted according to the GDPR, whether it is enough to amend existing rules for compliance with the GDPR, and several data controllers requested the Authority to deliver its opinion and approve their internal rules (NAIH/2018/3690/2/V and NAIH/2018/3193/2/V).

The GDPR does not explicitly provide for any obligation to adopt internal rules by data controllers. Under Article 24 (2), the data controller is obliged to apply internal data protection rules—as part of the technical and organizational measures taken for the protection of personal data—when it is proportionate to the data processing activity. The interpretation of this provision is assisted by recital (78). On this basis, the data controller has to consider whether the volume and scope of data processed are ‘proportionate’ to adopting data protection rules or any other system of rules (e.g. instruction, procedure description, security rules), or not.

In view of all this, if the data controller decides to adopt data protection rules, the GDPR provides for no special prescription on the substantive elements of such rules. The adoption of the data protection rules is the duty of the data controller, and there is no standard form or model to follow; it is up to each data controller to assemble the contents of such rules.

In accordance with the principle of accountability under Article 5 (2) of the GDPR, the data controller (or processor) has the duty of ensuring that the data protection rules and the

practice based on them concord with the Regulation. The Authority shall deliver no opinion or approval on them, but supervise them in the course of its procedures. Data protection rules need not be notified to the Authority (opinions number: NAIH-2018-942-2-K; NAIH-2018-1594-2-K; NAIH-2018-1868-2-K; NAIH-2018-2162-2-K; NAIH-2018-2471-2-K).

In order to assist lawful data processing practices, the Authority issued information on the application of the GDPR, and adopted opinions on data protection officers and data protection records and rules. Apart from those mentioned, the Authority also published information concerning the data protection reform to assist preparations for applying the regulation on the following subjects matter:

- data processing by small and medium enterprises;
- data processing at workplace;
- data processing by family doctors;
- data processing by individual entrepreneurs;
- data processing by accommodation services;
- activities of attorneys-at-law;
- data processing in the framework of newsletter services.

It is also a duty of the Authority to provide counsel in accordance with Member State law to the national parliament, the government, and other institutions and organs on the rights and freedoms of natural persons in respect of the processing of personal data. In connection with this duty, the Authority published information on the preparations for the GDPR by local governments (NAIH/2018/788/2/K, NAIH/2017/5364/2/V), on the quality data processor and the obligation to adopt rules, and the data processing of civic organizations and professional chambers (NAIH/2018/2919/2/V, NAIH/2018/3134/2/V, NAIH/2018/789/2/V). Apart from these, the Authority issued opinions on its website on the assessment of the handling of documents, certain obligations of mediator bodies under the GDPR, data processing by children's and elderly homes, and data processing carried out during legislation, and answered questions arising thereof.

Information issued by the Authority without the framework of a procedure, as consultation answer, shall qualify as neither law nor other legal instrument, and has no normative feature, legal force or binding content. An interpretation of law by the Authority on the basis of information it was provided in any concrete case shall not be binding for any other authority, court or the data controller; it serves the purpose of guidance only. The issue of information or an opinion shall exempt its addressee or the data controller from neither having to form its own legal position nor bearing liability for the lawfulness of its data processing.

II.1.2 Changes of the Data Protection Obligation System

II.1.2.1 The Material Scope of the GDPR

1. In all cases received by the Authority, each instance of data processing must be examined whether it belongs within the material scope of the GDPR. In this regard, the starting point is Articles 1 and 2 of the GDPR.

The GDPR applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

According to Article 2 (2) of the GDPR, its provisions do not apply to the processing of personal data:

- in the course of an activity which falls outside the scope of Union law;
- by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;
- by a natural person in the course of a purely personal or household activity;
- by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

The GDPR therefore applies to data processing

- concerning natural persons;
- is fully or partly automated data processing;
- is not automated data processing which forms part of a filing system or is intended to form part of a filing system; and
- concerning an activity falling within the scope of Union law.

The GDPR does not apply to data processing

- concerning activities in relation to the common foreign and security policy of the Union;
- concerning activities for the investigation or detection criminal offences, and public safety;
- carried out in the course of a purely personal or household activity.

The scope of the GDPR thus does not extend to the data processing falling within the scope of the other component of the Data Protection Reform, the Police Directive, and the scope of the acts of legislation in Data Protection Reform taken together do not extend to the regulation of all data processing legal relationships, thus naturally not to, on the one hand, legal relationships not subject EU law at (e.g. data processing for national security purposes) and, on the other, to those not excluded from the scope of EU law by the founding treaties and not intended to be regulated by the EU legislator (e.g. data processing based on paper and not organized into a filing system).

By adopting the Amendment Act, the Hungarian legislator continues to ensure the enforcement of the fundamental right to the protection of personal data under Article VI (2) of the Fundamental Law in the areas unregulated by EU law in legal relationships for data processing within the jurisdiction of Hungary, as the legal regulation containing the general rules of data protection has traditionally done in Hungarian law and in accordance with Hungarian declaration attached to Data Protection Convention of the Council of Europe promulgated by Act VI of 1998.

2. Special mention must be made of the fact that the GDPR, like the former provision of the Privacy Act, contains the so-called 'household exemption', that is, it does not extend the material scope of the regulation to certain types of data processing. In Article 2 (2) c), it states that it does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity.

According to Recital (18), the condition of applying the household exemption is that the data processing has no connection to a professional or commercial activity.

The household exemption includes, among others, correspondence, address storing, as well as maintaining contacts and online activity through community networks within the framework of personal or household activity.

The GDPR however applies to the data controllers and data processors that provide the means of such personal or household activity, that is the activity of the operator of the social media, electronic mailing system, and telephone application.

In the submissions received by the Authority, it was characteristically in cases related to social media and camera surveillance that the applicability of the household exemption arose.

Several requests were received by the Authority on groups created on the social media site Facebook, which were organized by kindergarten groups (NAIH/2018/3922/V) and school classes (NAIH/2018/5727/V) to facilitate communication between their members. In its opinions delivered in these cases, the Authority the composition of the groups are relevant in terms of delimitation; insofar as only parents and their children belong to these groups, the content shared in these groups does not fall within the material scope of the GDPR, but, should a teacher also belong in the group, it cannot be said to have no professional feature, and thus the household exemption does not apply.

The Authority did not include contents published on social media surfaces—e.g. sharing a dating-site profile with the likeness of a person on a Facebook-group site—within the exemption (NAIH/2018/6455/V), even though this had no professional relevance, because the exemption does not apply where the personal data is received by an unidentified number of people or is published.

In responding to submissions, the Authority included the photos taken at tourist trips and family or friendly gatherings (NAIH/2018/3389/V) and photos of children at school events by their parents even though other children appeared in the pictures (NAIH/ 2018/6083/V). It should be noted however that the Authority regarded the taking of these photos exclusively as data processing for household activity purposes; should the maker of the pictures have uploaded them on the internet, the data processing would have been subject to the GDPR.
A large number of complaints were received by the Authority where the complainants objected to the cameras placed on their neighbour's property, claiming these recorded happenings on their property also (NAIH/2018/3550/V.).

On the initiative of the Authority, discussions took place at EU level whether the supervisory authorities of the Member States include camera surveillance in the household exemption or not. Most of the supervisory authorities responded that the data processing in question is subject to the GDPR, only two supervisory authorities including it unequivocally within the scope of the regulation. In answering these types of submission, the Authority emphasized that, when the camera is set to record images on the property it is installed, the provisions of the GDPR do not apply to it; but as soon as the camera records happenings on a neighbour's property or in a public area, the exemption rule does not apply, and the data controller must meet the requirements under the GDPR.

3. The data processing of the courts is likewise subject to the GDPR with the proviso that, under Article 55 (3) of the GDPR, supervisory authorities shall not be competent to supervise processing operations of courts acting in their judicial capacity.

This is explained by Recital (20) of the GDPR in the following terms: the competence of the supervisory authorities should not cover the processing of personal data when courts are acting in their judicial capacity, in order to safeguard the independence of the judiciary in the performance of its judicial tasks, including decision-making.

The rules of supervising the data processing operations of the courts are provided for by Chapter VI/A of the Privacy Act as modified by the Amendment Act.

Under Section 71/A (1) of the GDPR, in contentious and non-contentious proceedings aimed at adopting a judicial decision, the supervision of the enforcement of the right to the protection of personal data in the context of data processing operations carried out by the courts in accordance with the relevant provisions shall take place through data protection complaints.

The complaint may be filed with the court proceeding in the basic case in writing, addressed to the court with material jurisdiction to decide on the complaint. Under Section 56 (5) of Act XCIII of 1990 on duties, a data protection complaint in order to supervise the data processing activity of a court shall be exempt from duties.

The complaint shall be examined by the court above the court proceeding and, in the case of the Curia, another council of the Curia. In accordance with Section 71/B (1) of the Privacy Act: 'The court shall examine, on the basis of the complaint, whether the judge, the lay judge or the judicial employee complied, in the course of his processing activity, with the provisions of the laws and of Union law on the protection of personal data.'

The Authority has therefore no competence to supervise the data processing subject to Article 55 (3) and Chapter VI/A of the Privacy Act, it does not carry out procedures on such data processing, and such examinations belong within the scope of the courts.

II.1.2.2 Principles of Data Processing

With regard to principles, the GDPR contains principles that, first, were provided for by the Privacy Act before the Data Protection Reform, second, renames principles, and introduces new principles, as per the following:

Name of principle	
Privacy Act	GDPR
purpose limitation (Section 4 (1)–(2))	purpose limitation (Article 5 (1) b))
fairness and lawfulness (Section 4 (1))	lawfulness, fairness, and transparency (Article 5 (1) a))
accuracy, completeness, and up-to-date status (Section 4 (4))	accuracy (Article 5 (1) e))
period of time necessary to achieve data processing purpose and identification (Section 4 (2) and (4))	storage limitation (Article 5 (1) e))
data minimisation (Section 4 (2))	data minimisation (Article 5 (1) c))
	integrity and confidentiality (Article 5 (1) f))
	accountability (Article 5 (2))

The principles of data processing accompany the entire process of data processing, including data collection, the choice of appropriate legal basis, and the provision of information to data subjects.

The principle of accountability defined by Article 5 (2) of the GDPR is given prominent emphasis, whereby the data controller shall be responsible for the enforcement of the principles under Article 5 (1) thereof, and shall also demonstrate compliance with those principles. The principle of accountability means that the data controller assumes responsibility for the data protection measures it took, including all the measures taken from designing the data processing through carrying it out and implementing the data processing purpose, access to personal data, their transfer, administration, and verification.

II.1.2.3 Case Law Regarding Principles in the Practice of the Authority

1. Purpose Limitation and Data Minimisation

Having examined the notice on unsubscribing from its newsletter accessible on the website of an insurance company, the Authority found that unsubscribing required submitting the given name and the surname, the name of the requester, and his or her contact details (e-mail address or telephone number), and thus the activity related to data processing did not raise any issue of the infringement of the principles of purpose limitation and data minimisation, and thus the Authority found no concern in the data processing practice of the insurance company in terms of the rights to the protection of personal data (NAIH/2018/3559/V).

The Authority found that a sports club processes personal data without lawful purpose, infringing the principle of purpose limitation as per Article 5 (1) b) of the GDPR, when it recorded the name and telephone number of individuals wanting use the running facility

open to the public. The purpose of data processing, that is the interest behind, could have been implemented without data processing.

The rejection of entry for people expelled or prohibited from entering and the related identification of persons prohibited from entry due to breach of law may be a lawful purpose, but recording the personal data of everyone wanting to do their sport exercise is not an appropriate means; it is enough to put down the names those breaching the law. This also follows from the principle of data minimisation under Article 5 (1) c) of the GDPR, according to which personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

With regard to recording the number of people using the sport facility, the opinion of the Authority is that this requires no processing of personal data. If the club wishes to record the number users of its track, it can do so in a number of ways without identifying data subjects.
The Authority required the club to review its data processing practice and to modify it accordance with the provisions of the GDPR, or terminate the data processing objected to, and, furthermore, should the club find the processing of personal data in respect of the running track necessary, it should carry out balancing of interests with regard to each purpose in accordance with the aforementioned, and compile an appropriate data protection notice detailing all the circumstances of the data processing (NAIH/2018/3750/V).
In one instance, the Authority received a request concerning requests to use parking benefit certificates for disabled persons. The data controller wanted to permit driving in to an area closed to the public by not only having the certificates placed in the car windows but also collecting and recording personal data.

In its response, the Authority noted that disability is to be regarded as sensitive personal data under Recital (53) and Article 9 of the GDPR. The personal data of disabled persons processed in the parking certificate for the purposes assisting their movement and parking may not be connected to data processing with other purposes. In accordance with the principles of data minimization and a purpose limitation under Article 5 (1) b) of the GDPR, the Authority held that it is unacceptable that the data controller should permit driving-in on condition of, beyond presenting the parking certificate, collecting and recording personal data for recording (NAIH/2018/1997/V).

2. Transparency

In one complaint the complainant requested guidance whether it is objectionable from a data protection perspective that filling in data protection form is not required when buying a guarantee offered by an insurance company in a technical department store.

Under Recital (58) and Article 12 (1), the principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, that clear and plain language, and, additionally, where appropriate, visualisation be used. Such information could be provided in electronic form, for example, when addressed to the public, through a website. This is of particular relevance in

situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising.

In its response, the Authority pointed out that it is the burden of the data controller to demonstrate compliance with the GDPR, e.g. that it met the requirements resulting from the principle of transparency (Article 5 (1) a) of the GDPR), especially from the obligation to provide information under Articles 13–14 of the GDPR, or, where the legal basis of data processing is consent, to prove that the data subject had given his or her consent. It is both in the interest and obligation of the data controller to document the fulfilment of these obligations; it lacking, the lawfulness of recording data or the existence of an appropriate legal basis can hardly be substantiated (NAIH/2018/5913/V).

In another case, where the complainant wanted to know whether it was lawful of the condominium representative to require the personal identifiers of the owners, the Authority held that the personal identifier is not necessary for fulfilling the tasks of a condominium representative.

The legal basis under Article 6 (1) c) of the GDPR is applicable exclusively to purpose-limited, minimally required personal data in accordance with Article 5 (1) b) and c) of the GDPR (the principles of purpose limitation and data minimisation).

In a given case, personal identifiers may be needed for amending the condominium's founding charter, but even there it is the countersigning attorney-at-law that is to process them. The condominium representative may only make records of personal identifiers if he or she is able to designate a special legal basis that cannot be reasonably carried out without processing the personal identifiers. The condominium representative is to set out this purpose and the interest in data processing needed for performing the condominium representative's contract in clear and plain language in the data protection notice in accordance with Article 5 referred to above (NAIH/2018/3464/V).

With regard to consent requested by way of filling in a document entitled 'Data and Confidentiality Protection Statement') in order to be able to access and process health data of the data subject in an accident a loss adjustment case, the Authority held that, following from Sections 135[1] and 136 of Act LXXXVIII of 2014 on the Business of Insurance, the insurance is entitled to process on the basis of the consent of the data subject the health data of the complainant if it is necessary for establishing the grounds of a claim, complying with the principles of purpose limitation and data minimisation.

In the opinion of the Authority, the request for data access and processing by the insurance company is lawful to the extent, insofar as, and within the scope of data collected, that the

[1] According Section 135 of the Insurance Act, an insurance company shall be allowed to process the data of clients which relate to the service provided on the basis of the relevant insurance contract.
According to *Act XLVII of 1997 on the Protection and Processing of Medical and Other Related Personal Data (hereinafter: 'the Health Data Act')*, insurance companies shall be authorized to process any data pertaining to the medical condition of clients only for the reasons set out in Section 135 (1) and only in possession of the written consent of the data subject.

collected data are indispensably necessary for a purpose under the insurance contract, e.g. establishing the grounds of a claim.

In its opinion, the Authority explicated that a request for access to data to information from the organs and persons given generally in the attached document[2], to access records and documents, and to make copies of documents including (health) data, seems to infringe Article 5 (1) b) and c) of the GDPR if data are accessed that are not required for assessing the claim. From a data protection law perspective, instead a general consent only a concrete one should be valid, and thus such a general authorization is expressly questionable. The lawfulness of the request to access to data cannot be assessed without the knowledge of all documents pertaining to the insurance relationship, especially the insurance contract. These documents may include contractual conditions that appropriately substantiate the data request of the insurance company, such as in respect of the conditions or reasons excluding the conclusion of contract (NAIH/2018/5815/V).

3. The Principle of Accuracy

In case number NAIH/2018/6408/H, the complainant, who is not the client of the financial institution, requested the institution no to use his telephone number to send him text messages on the debts of someone else.

Upon the request of the claimant, the financial institution sent letters to its client to rectify data, and also called the complainant to present his contract. In spite of his complaint, the complainant continued to receive text messages on the debts of another person from the data controller.

In the opinion of the Authority, the data processing of the data controller, sending text messages to the telephone number it stored, was lawful so long as it could be surmised that it recorded the telephone number of its client. When this was called into doubt by the claimant, the data controller should have taken measures to limit the data processing until the situation was clarified, the data was rectified. The data controller did not meet this of its obligations, because it sent text messages to the complainant even after it became clear that the accuracy and the up-to-date status of the data was questioned, and thereby infringed Article 5 (1) d) of the GDPR.

In the opinion of the Authority, that the data controller contacted the client in a letter asking for data rectification, was an appropriate but insufficient measure. The measures of the data controller upon the notification by the complainant should have both implemented the principle of accuracy and obstructed the use of inaccurate data. In such a case the data controller must limit the processing of inaccurate data for the time being.

4. Accountability

[2] 'The injured from his home doctor, the National Health Insurance Fund, National Rehabilitation and Social Office, Hungarian State Treasury, social security paying-offices, as well as al the medical institutions, doctors, natural healers and all other persons or organs treating injured'.

A complainant reported to the Authority that a website that he had previously browsed sent advertisements to his telephone and laptop without his consent.

Under Point 1 of Article 4 of the GDPR, the term personal data includes so-called pseudonymous or pseudonymized personal data as well, such as e-mail or IP addresses even when they do not contain the actual name of the person. According to the principle of accountability as provided for Article 5 (2) of the GDPR, the data controller is obliged to document and record data processing so that its lawfulness can be demonstrated afterwards. In the case of consent as a legal basis for example, the giving of consent should be provable at reasonable level (e-mail, logging the IP address), but the GDPR does not provide for any itemized mode of proving the lawfulness of data processing. The data controller is obliged to provide the data subject the information set out in the GDPR—among others, the ways of accessing, rectifying, and erasing data, and objection (NAIH/2018/4568/V).

In another case the complainant wrote of his concerns about the website of a tax consultant and accounting firm in his letter to the Authority, and objected to the lack of a data protection notice on the website.

If the personal data of the data subject is collected directly from her or him, the data controller is obliged to provide the data subject detailed information under Article 13 of the GDPR in order to ensure fair and transparent data processing. Pursuant to the principle of transparency under Article 5 (2) of the GDPR, the data controller must be able to demonstrate compliance with the principles of processing personal data.

The Authority stated that the provision of data protection information may be given either on the website of the data controller or in any other demonstrable way (e.g. form, contract, correspondence) depending on the particular mode of the given data processing.

II.1.2.4 Legal Bases

The legal bases of data processing are provided for by Article 6 (1) of the GDPR as follows:

- consent by the data subject;
- contract concluded or to be concluded with the data subject;
- a legal obligation to which the controller is subject;
- the vital interests of the data subject or of another natural person;
- performance of a task carried out in the public interest or in the exercise of official authority;
- legitimate interests pursued by the controller or by a third party.

The existence of any of these legal bases is not sufficient grounds for the processing of the special categories of personal data, as that requires the fulfilment of the further conditions laid down by Article 9 of the GDPR. The main rule is that the processing of special data is prohibited. The exemptions from this main rule are provided for by Article 9 (2) of the GDPR; given these exemptions, data processing may proceed under the condition that the data controller is capable of demonstrating the existence of a legal basis under Article 6 (1).

1. Consent as Legal Basis

The concept of consent is defined by the GDPR. Consent by a data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. As in the earlier regulation, the Privacy Act, the conceptual elements of consent are the prior provision of appropriate information, its being given freely, and the concrete and unambiguous indication of the will to consent. Should any of these elements not meet the requirements applicable, the data controller may not lawfully refer to consent as a legal basis.
From among these conceptual elements, it is by way of the information provided that the data subjects get to know about the processing of their personal data, monitor the fate of their personal data, and it is through the prior provision of information that informational self-determination can be enforced: data processing is lawful when it circumstances are fully known by the data subjects. The other component of valid consent is the free will of the data subject giving it, its being uninfluenced from without, which is realized by free or actual choice, and the choice of no consent, or its withdrawal, results in no harm to the data subject. A further requirement of the validity of consent is that it is a specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
Article 7 of the GDPR provides for further requirements of consent. One of these, that, if data processing is based on consent, the data controller must be able to demonstrate that the data subject has given his or her consent to the processing of his or her personal data, which follows from the principle of accountability, was set forth in this way in the Privacy Act.
A further requirement—a consequence of the principle of transparency—under the GDPR is that the request for consent in a written declaration shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.
Furthermore, the data controller must also ensure that it is just as easy for the data subject to withdraw his or her consent as to give it.
Beyond these main requirements, the guidelines on consent by the Working Party set up under Article 29 of Directive 95/46/EC (hereinafter ‘Working Party 29’) treats the further requirements of data processing making the reference to legal basis by data controllers lawful.
In case number NAIH/2018/3750/V, where the complainant objected to the data controller requiring all persons wanting enter to a running track to put down their names, addresses, and telephone numbers on a sheet of paper on the table of the porter, the Authority found that the legal basis referred to be the data controller was not applicable, because, first, no appropriate information was provided, and, second, consent was not given freely. Though the data controller did provide a data protection notice, it did not contain all the circumstances of and information on data processing prescribed by the GDPR, and the

freedom to consent was also not ensured, because if one did not subscribe the sheet, he or she could not use the running track.

2. Data Processing Based on Contract

New in comparison to the Privacy Act and separate from consent is the independent legal basis of data processing based on contract as per the GDPR, where data processing is necessary for the performance of a contract to which data subject is party or in order to take steps at the request of the data subject prior to entering into a contract. This legal basis has thus two types of cases. One type is when data processing is necessary for the performance of a contract where one of the parties is the data subject, while the other type is when data processing is necessary in order to take measures at the request of the data subject prior to entering into a contract.

Data processing necessary for the performance of a contract is conditional on a valid contract where one of the parties is the data subject. An example among others of such a contract is an employment contract, where the employer needs to process the data of the employees in order to perform the contract. It should be noted however that employment gives, or may give, rise to further data processing or different data processing purposes, where legal basis is not the contract but that e.g. a legal obligation or legitimate interest.

In a case when data processing is necessary in order to take measures at the request of the data subject prior to entering into a contract, where there is no contract, and its conclusion requires certain steps that include data processing. It is an important criterion here that the measures preceding the conclusion of the contract are initiated not in the interest or on the initiative of the data controller or a third party but that of the data subject. An example of such data processing is a request for a price offer. In order to be able to provide the offer, the service provider might need to temporarily process some of the personal data of the data subject (in the case of life or vehicle (third-party) insurance, this may span a large group of data).

3. Legal Obligation as Legal Basis

The processing of personal data may also be lawful if it is necessary for fulfilling a legal obligation by the data controller.

If data processing takes place in the framework of fulfilling a legal obligation by the data controller, it must have a legal basis in EU law or the national law of the Member States. The GDPR however does not require a specific law for each individual processing. A law as a basis for several processing operations based on a legal obligation to which the controller is subject may be sufficient. It should also be for Union or Member State law to determine the purpose of processing. Furthermore, such law could specify the general conditions of the GDPR governing the lawfulness of personal data processing, establish specifications for determining the controller, the type of personal data which are subject to the processing, the data subjects concerned, the entities to which the personal data may be disclosed, the purpose limitations, the storage period and other measures to ensure lawful and fair processing. The Authority supports and urges the determination of these conditions by the legislator for the purposes of legal security.

Laws may specify a legal obligation that may involve the processing of personal data without the given provision regulating the circumstances of data processing. Should such law prescribing data processing not fully meet Section 5 (3) of the Privacy Act, and not provide for the circumstances of data processing, the data controller shall enforce the principles and guarantees of the general rules of processing personal data, which the legislator failed to provide for.

It may so happen that the law provides for only a general authorization for the processing of a given activity involving the processing of personal data. This the case of the provision of the Labour Code enabling the employer to control the employee in respect of his or her conduct related to the employment. Here the law provides for the possibility (not the obligation) to control, does not prescribe data processing as an obligation, and thus the legal basis of data processing is likewise different (the legitimate interest of the employer).

4. Data Processing Based on the Vital Interests of the Data Subject — Force Majeure Data Processing

In accordance with the rules of the GDPR, data processing is also lawful when it is necessary for the protection of the vital interests of the data subject or another natural person.

With reference to the vital interests of other natural persons, the processing of personal data may take place if the data processing in question cannot be performed on another legal basis. With regard to this legal basis, it should be emphasized that some data processing may involve the use of several legal bases, of which the controller must select the basis on which it bases its data processing (e.g. some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters).

5. Data processing necessary for the performance of task carried out in the public interest and the exercise of public authority

Similarly to the legal basis examined in Point 3 above, it can be said about data processing necessary for the performance of a task carried out in the public interest and the exercise of public authority that, according to the Hungarian legal environment and the practice of the Constitutional Court, the State may restrict the fundamental rights of the data subject, such as the right to informational self-determination, to the degree necessary and proportionate for safeguarding a fundamental right or protecting a constitutional value, that is, in the public interest. The condition of the application of this legal basis is therefore that a law or EU norm regulate the data controlling activity with a purpose based on public interest of the data controller exercising its public authority tasks and powers or fulfilling other duties in the public interest. At the same time, however, such legal provisions often define only the data controller's public tasks, procedural scope and obligations but not the detailed rules for the related data processing operations.

The legal basis for data processing based on legal provisions defining the controller's public tasks is thus Article 6 (1) e) of the GDPR. It is also important to emphasize that a public authority or any other body performing public tasks—such as a budgetary organ—can be the

subject of a public-law and private-law relationship—and related data-processing legal relationships—only in the performance of its public tasks, all other qualities are conceptually excluded. As a result, this legal basis absorbs or assimilates, as it were, all other legal bases of data processing. This concept is also reflected by the Police Directive, which, in contrast to the GDPR, is not applicable to data processing in the private sphere due to its material and institutional scope, and where the legal basis for data processing can only be the activity as a public task covered by the Directive (Article 8 of the Police Directive).
If the legislator, without taking into account the provisions of Section 5 (3) of the Privacy Act, has failed to set forth the detailed rules of such data processing, the data controller is obliged to carry out its data processing activity in accordance with general data protection rules, particularly principles and the necessity measure of legal basis and to demonstrate its lawfulness in compliance with the principle of accountability.

6. Legitimate Interest and Legitimate Interest Test

Should the legal basis of data processing be legitimate interest, the data controller is obliged to carry out a legitimate interest test[3] and to inform the data subject specifically his or her right to object pursuant to its obligation to provide information.[4] As examples, the GDPR mentions two case where the application of this legal basis often occurs, namely where the data subject is a client or in the service of the data controller.[5]

Within a legitimate interest test, the data controller is obliged to clearly define the legitimate interest serving as the basis of data processing, its effects on the data subject, and whether the data processing is necessary and proportionate, and to assess whether the legitimate interest of the data controller or a third party has primacy over the rights of data subject or not. In order to ensure proportionality, the data controller is obliged to assess whether the given data processing has an alternative or not, whether the given alternative is likewise efficient and results in lesser intrusion, because, if the data processing with lesser intrusion is likewise efficient, it is the one the data controller is compelled to apply.

On the basis of considering the criteria mentioned above, it is to be established before starting the data processing whether the personal data may be processed or not. If the legitimate interest test concludes that the legitimate interest of the data controller or a third party has primacy, is proportionate, and the given data processing has no equally efficient and less intrusive alternative, the data processing referring to legitimate interest may be lawful.

In the experience of the Authority, data controllers usually do not properly carry out the balancing of competing interests. The most common failure is that data controllers do not,

[3] See Recital (47) of the GDPR.
[4] Articles 13 (2) b), 14 (2) c), and 21 (4) of the GDPR.
[5] Recital (4) of the GDPR.

apart from identifying their own interests, genuinely balance the interests, and deduce consistently why their interests identified in their legitimate interest test have primacy over those of the data subject.

Another objectionable data processing practice in connection to the balancing of interest is that data controllers compare the interests of protecting personal data not with legitimate and genuine interests, but they give primacy to criteria of convenience over the fundamental rights of the data subject, which cannot be accepted in terms of data protection, because these cannot be more accentuated than the interests of the data subject.
Without an appropriate legitimate interest test supporting the necessity of data processing, data controllers may not refer to legitimate interest as a legal basis, and so in such cases, it can be established that data processing is unlawful.

a) In case number NAIH/2018/6142/H, the Authority examined the case based originally on consent but later on legitimate interest. Here the telephone number of the data subject had been recorded on the basis of data subject consent. The data subject objected to the processing of the telephone number data after the GDPR came into effect, and requested its erasure.

The data controller did not erase the data upon request, because, in accordance with Article 17 (1) b) of the GDPR, if the data subject withdraws his or consent that was the basis of data processing, the data controller is not obliged to erase the data when it has another legal basis for data processing, and refers to a legitimate interest the existence of which a legitimate interest test demonstrates.

The Authority revealed many deficiencies in the legitimate interest test supporting legitimate interest of the data controller, and thus found that the data controller could not to have based its data processing on this legal bases in the absence of an appropriate and acceptable legitimate interest test. Examples of deficiencies in the legitimate interest test are as follows:

- the data controller named several purposes, but failed to carry out the balancing for each one;
- necessity in comparison with the purpose of data processing was unsubstantiated;
- the data controller gave primacy to business interest and comfort criteria over the interests and fundamental rights of the data subject without proving their primacy and analysing proportionality;
- the data controller made a deficient identification of the interest of the data subject;
- arguments were brought up in favour data processing without relevance for the balancing of interest.

b) In case number NAIH/2018/2041/, the findings were that a financial institution processed the personal data of someone it had no contractual relationship with. In

2007 the husband of the claimant had concluded a loan contract, which the bank later withdrew from. The claim was assigned, of which only the husband of the claimant was notified of. The financial institution named several legal bases for processing the personal data of the claimant, referred to oral consent, the Family Act, the Civil Code, and legitimate interest in their letter to the Authority. As of 25 May 2018, yet it would have been only acceptable to refer to legitimate interest among the legal bases invoked in the given case insofar as the data controller had completed an appropriate legitimate interest test to support the legitimate interest.

c)

The Authority found that the — undated — legitimate interest test was inappropriate, because, on the basis of what was included in it, the data controller had failed to complete any legitimate interest test, as the document requested by the Authority did not contain any examination whether the processing of the complainant's data was indispensably necessary.

7. Processing for a purpose other than that for which the personal data have been collected

The GDPR provides for data processing for purposes other than the original, so long as those purposes are compatible.

The GDPR provides a list of examples of criteria to be taken into account in order to establish whether a data processing with a different purpose is compatible with the purpose for which the data were originally collected.

Accordingly, any link between the purposes for which the personal data have been collected and the purposes of the intended further processing, the context in which the personal data have been collected (the link between the data subject and the data controller) must be taken into account, as must the nature of the data collected, existence of appropriate safeguards, as well as the possible consequences of the intended further processing for data subjects.

Pursuant to their obligation to provide information under the GDPR, the data controllers shall inform the data subjects of the change in the legal basis of data processing and their right to object in their exercising their data subject rights.

In case number NAIH/2018/6142/H, the Authority had to examine data processing concerning telephone numbers on the basis of Article 6 (4) of the GDPR, because the data controller had referred to a new purpose of data processing.

Under Article 6 (4) of the GDPR, the data controller may process personal data for a purpose other than that for which the personal data have been collected when processing for another purpose is compatible with the purpose for which the personal data are initially collected. In this case the data controller shall take several criteria into account, among which Article 6 (4) of the GDPR provides examples of those circumstances it regards the most important to be considered.

It was found in the case that the data controller processed the telephone number (development of customer service activity) for a purpose other than the original purpose of

data processing (performance of contract), and thus it should have applied Article 6 (4) of the GDPR, the Authority found that the data controller thus failed to carry out this assessment of compatibility, and therefore there was no legal basis for processing the telephone number for the new purpose.

II.1.2.5 Data Subject Rights

The rights of data subjects have broadened since the entry into effect of the GDPR. Data controllers are required to support the submission of all data subject requests, and, accordingly, all data protection notices have to outline the ways of proceeding with such requests.

1. The Right to Be Informed, and Transparency

1.1 It is important data controllers are obliged to provide prior information to data subjects in plain and clear language on all the significant circumstances and the path of the processing of their personal data.

The Authority encountered cases where the data controller failed to publish any information on data processing on its website. In several cases, the Authority found that, as the data subjects had not been given prior information on the circumstances of data processing before giving their personal data required for registering on the website, the provisions of Article 12 of GDPR were infringed (NAIH/2018/1549/V and NAIH/2018/5300/V).

The questions most often raised by data controllers were on the necessity of compiling such notices, their form, language, publication, and content, and whether the changes aligning notices with the GDPR on data processing already in progress have to be notified to the data subjects following 25 May 2018. The GDPR regards the obligation of the data controller to provide information as a base of accountability. In the course of compiling the notice for data subjects prescribed by the GDPR, the data controller shall take appropriate measures to provide such information about all data processing in concise, transparent, intelligible and easily accessible form, using clear and plain language. The provision of information meeting the requirements of law and appropriately detailed is not only an obligation to be fulfilled by the data controller but also one that serves the enforcement of the rights of the data subjects. The compilation of data processing notices is the duty of the data controllers, there is no standard form or model prepared by the Authority, and it is up to each data controller to assemble the contents of such notices (NAIH/2018/5909/V).

The form of providing information is usually in writing, but it is possible orally too. Oral provision of information may be based both on a living contact (e.g. telephone conversation) and pre-recorded oral message, in which case data controllers are obliged to ensure that data subjects can listen to the message repeatedly.

A data protection notice meeting the requirements of the GDPR depending on the given type of data processing may be published on the website of the data controller or in any other demonstrable way (e.g. in a form, a contract, and correspondence, etc.).

As the GDPR does not define the exact way of publishing/disclosing prior information, the Authority found in one case that it cannot be concluded from the mere fact that the website of a data controller has no data protection notice on its website that it processes personal data not according to the provisions of law, or fails to provide information on its data processing activity (NAIH/2018/5407/V).
The GDPR likewise does not define the language to be used in the data protection notice. Working Party 29 published guidelines on the transparency of data processing operations[6], where it provides information on the translation obligations of the data controllers. On the basis of the guidelines, it is reasonable to provide information in the native languages of the persons targeted by the services in order to comply with the requirement of transparent data processing (NAIH/2018/3847/V).

1.2 In contrast to the Hungarian rules applicable prior to the data protection reform, the GDPR distinguishes between the collection of data directly from the data subject and from elsewhere. If data are collected directly from the data subject, the data controller shall, at the time when personal data are obtained, provide the data subject with all of the following information: the identity and the contact details of the controller, the contact details of the data protection officer, the legal basis and the purpose of the data processing, and the recipients, or categories of recipients, of the personal data if data are transferred. Beyond those listed in Article 13 (1) of the GDPR, the data controller shall provide the data subject with the following so-called further information necessary to ensure fair and transparent processing as listed in Paragraph (2): the period for which the personal data will be stored, the right of access of data subject, the conditions of withdrawing consent, the right to lodge a complaint, whether the provision of personal data is a statutory or a contractual requirement, and of the possible consequences of failure to provide such data, and the existence of automated decision-making, including profiling.
Furthermore, Working Party 29 in its guidelines on transparency[7] expounded all those criteria it suggests data controllers should take into account when providing prior information.
The data controller is exempted from its obligation to provide information when the data subject already possesses all or part of the information. I practice it is difficult establish whether the data subject is genuinely in the possession of the information listed, or to what extent he is, the data controller therefore proceeds properly when he provides the data subject with, beyond all information mandatory under the GDPR, all relevant information on data processing in a demonstrable way (preferably in writing). In this way, it complies with another important principle of the GDPR, accountability.
The data controller shall provide the data subject with the information related to data processing even where personal data have been obtained not from the data subject (Article 14), because the data subject must not suffer any legal disadvantage due to his data being obtained from elsewhere. The GDPR provides for a flexible deadline for the data controller

[6] WP 260 rev. 01.
[7] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

to fulfil this obligation to inform by stating that it shall provide the information within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed. Apart from generally regulating this, the GDPR provides for two specific cases. The data controller shall provide the information, if the personal data are to be used for communication with the data subject, at the time of the first communication to that data subject at the latest, or if a disclosure to another recipient is envisaged, when the personal data are first disclosed at the latest.
No obligation to provide information burdens the data controller in this case either where and insofar as the data subject already has all or part of the information, or the provision of such information proves impossible or would involve a disproportionate effort. The GDPR prescribes no obligation to provide information where obtaining or disclosing the data is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests, or where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.
Following 25 May 2018, the duty of data controllers is to ensure that the information on existing data processing is made to comply with the GDPR, in respect of which the Authority holds that they need not inform the data subjects of changes thereto.
The Authority reviewed its own data protection notices, as well, from among which not only those about staff are accessible on the website of the Authority.

1.3 Under the GDPR and in the framework of the right of access, the data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and to access the personal data and, where the personal data are not collected from the data subject, any available information as to their source.
The information to be provided in respect of the right of access can be interpreted in terms of data processing already in progress. On these grounds, the data controller shall, in the framework of the right of access of the data subject, provide information as to the existence of data processing, its purpose, the categories of personal data, possible data transfers, the possibility and way of lodging complaints, the right to object, and the sources of collected data.
A large number of submissions were received by the Authority about being sent direct-marketing messages, according to which there is no possibility of unsubscribing, and when information is requested from the data controller, no answer is given.
During the examination of the dismissals of data subject requests for information, data controllers regularly referred to business secrets or the infringement of others' personal data. In this case, the right of access may be limited, but even so steps must be made to ensure that the data subject receives information in respect of his or her personal data, giving him or her the requested documents with the irrelevant data redacted.

1.4 In the framework of the right of access, the GDPR provides for a new partial right, the right to obtain a copy, to ensure its even more complete enforcement. The right to obtain a copy ensures that the data subject does obtain actual access to his or her personal data. The recognition of the right to obtain a copy as part of the right of access—the right to information in the earlier terminology of the Privacy Act—is not entirely new, and the Authority regarded it as part of the right to information, e.g. in the case of bank contracts, before the coming into effect of the GDPR.
A special case of the right to obtain a copy is the case of obtaining copies of camera recordings. In the practice shaped by the Authority before the GDPR coming into effect, the right to information with regard to camera recordings was most broadly enforceable by enabling the inspection of recordings. One reason for this was that the Privacy Act did not provide for data subjects to be able to choose the form of receiving information in the framework of the right to information, having only prescribed that the provision of information be in clear and plain language. Article 15 (3) of the GDPR expressly provides for the right of data subjects to obtain copies.
In case number NAIH/2018/5559/H, the data controller rejected the request of the data subject to receive a copy of the camera recording on grounds that the data subject had failed to justify his right, or legitimate interest, to obtain a copy of the recording, and that providing a copy of the recording is not appropriate to the purpose defined in the request of the data subject.
In this respect, the Authority found that, the GDPR not stipulating any additional requirement for the exercise of the right to obtain a copy, it can be exercised unconditionally, and thus the data subject is not obliged to justify his or her legitimate interest in obtaining the copy, and does not have to provide his or her grounds for wanting to exercise this right. The right of access, including the right to obtain a copy, may only be rejected in the cases provided for by Article 12 (5) of the GDPR, Article 15 lays down no other limitation, and thus the data controller shall fulfil such requests without stipulating any further condition.
It should be noted that, in accordance with Recital (63) of the GDPR, the exercise of the right to obtain a copy should not adversely affect the rights or freedoms of others; as a consequence, the data subject continues no to be entitled to receive the copy of a camera recording where other data subjects appear with being redacted, but the data controller may be obligated to carry out the redaction under Article 15 (3) in order to enforce data subject rights.

2 The Right to Erasure (‘the right to be forgotten’)

The right to erasure had already been included in Directive 95/46/EC, but it was Article 17 of the GDPR that expressly named the right to be forgotten as a mode of exercising this right, whereby the data subject shall have the right to obtain, upon request and under certain

conditions, from the controller the erasure of personal data concerning him or her without undue delay.
It is characteristic of the right to be forgotten that the request is directed at either the erasure of data appearing on the website operated by the data controller and the removal of information processed and stored by the processor or the removal of a result or link appearing while using a search engine.
It is laid down as a principle by the GDPR that personal data may only be processed for specified purposes and for a defined period of time. As a result, e.g. the termination of the purpose of or the lack of appropriate legal basis for processing, or, as a matter of fact, the fulfilment of a legal obligation prescribed by Union or Member State law the data controller is subject to, may induce erasure, especially if the data subject withdraws his or her former consent.
Apart from those mentioned above, the data controller must also erase personal data upon request by data subjects addressed to it. It shall provide information on action taken (erasure) on such a request to the data subject without undue delay and in any event within one month of receipt of the request.[8]
The data controller is under a further obligation when has made the personal data public. Taking account of available technology and the cost of implementation, the data controller shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.
The GDPR regulates several cases when the data subject may not exercise his or her right to erasure or to be forgotten. Such is the case when the processing of personal data is prescribed for the data controller by Union or Member State law, or when processing is for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. A request for erasure may be rejected on grounds that the processing of the data is necessary for the establishment, exercise or defence of legal claims. In such a case, the data controller shall prove that the further processing of the data is necessary.
In authority procedure number NAIH/2018/6093/H, the applicant wanted to exercise his right to erasure against a winding-up institution. In 2011 the obligor had been assigned old debts, but the applicant disputed the claim and the processing of data, and contacted the obligator. In the course of making the contact, the obligor required the applicant to identify himself with a natural person's identifier, because this was the only way it could handle the request. The applicant however refused to do so, because, in his opinion, the case number and his name were enough for identification. The obligor held that the identification was unsuccessful, and therefore closed the procedure for examining the complaint. The applicant then requested the erasure of his personal data in postal mail. The obligor provided the information that the claim had been withdrawn, and measures were to be taken towards the erasure of the applicant's personal data, but those would continue to be stored in the backup copies of the computer system of the company. The Authority ruled partly for the

[8] GDPR Article 13 (3).

applicant, and required the obligor to, among others, provide information to the applicant as to the date of the erasure of the backup files containing the personal data of the applicant. The Authority however rejected the part of the application on the erasure of the personal data related to the assignment contract and the contract for repurchasing the claim against the applicant, because these qualify as accounting documents to be stored by obligor for eight years under the provisions of the Act C of 2000 on Accounting (hereinafter: 'the Accounting Act'). The legal basis for processing personal data in accounting documents is Article 6 (1) c) of the GDPR, and they may not be erased even on request by the data subject pursuant to Article 17 (3) b).

3 The Identification of Data Subjects

Under Article 12 (6) of the GDPR, if the controller has reasonable doubts concerning the identity of the natural person making a request to exercise his or her data subject rights, the controller may request the provision of additional information necessary to confirm the identity of the data subject. When the data subject submits his or her request to exercise data subject rights personally, identification is relatively straightforward, as he or she can provide his or her identification document if necessary.

Identification is more complicated when parties are separated by distance, when a request to exercise data subject rights is submitted to the data controller via postal or electronic mail. In such a case, when the data controller has reasonable doubts concerning the identity of the requester—it had not known or processed his or her e-mail, it must carry out the identification.

The certification of personal identity and identification are not identical concepts, and thus all the four natural personal identification data are necessary for identification only in exceptional cases; in most cases, the name and one of the three other identifiers are enough on account of the principle of data minimisation. This naturally does not exclude identification through name and client number or name, client number and address in combination. The data controller must assess on a case-by-case basis whether it has reasonable doubts concerning the sender of the e-mail, and what piece—or, exceptionally, pieces—of personal data would dispel such doubts. In doing this assessment, the data controller must be particularly attentive as to require only such personal data that it already processes, that it can compare with; otherwise, the data requested will not be suited for identifying the data subject, and processing it might infringe the principle of purpose limitation (NAIH/2019/1841).

It should be noted that the obligation to identify does not always apply. If the request or other submission by the data subject contains information whereby he or she can be identified, no further personal data may be requested from the data subject.

II. 1.3 Certain Frequent Groups of Cases

II. 1.3.1 The Cost Exemption of the First Copy of Healthcare Documentation

With regard to healthcare, the right of access brought about major changes. In this framework, the data controller's obligation to provide information under the Privacy Act was

replaced by the obligation to provide a copy of the personal data undergoing processing pursuant to Article 15 (3) of the GDPR, which brought about changes particularly in the access to healthcare documents.

Act XLVII of 1997 on the Protection and Processing of Medical and Other Related Personal Data (hereinafter: 'the Health Data Act') and Act CLIV of 1997 on Health (hereinafter: 'the Health Act') provide for the right of the data subject to inspect and request a copy of his or her healthcare documentation. As of the entry into force of the GDPR, the data subject has this right directly on the basis of the GDPR, which details access to data and copy requests in Article 15.

While under the currently effective regulation of the Health Data and the Health Acts, the data subject may receive a copy of healthcare documentation at his or her own cost, the GDPR provides for the cost exemption of a copy requested in the framework of the right of access of the data subject (Article 15 (3)), and thus this applies to the documentation processed by healthcare service providers.

In recent years the Authority conducted several inquiries where the healthcare provider charged an unrealistically high fee (HUF 50–100 thousand) for providing a copy to the data subject. As no law regulated the fees institutions could charge, healthcare providers charged a wide variety of fees for copies. Earlier on the Authority had detailed the criteria of determining fees recommendation, and recommended a measure for determining fees.

In 2018 a hospital charged over HUF 50 thousand for the copy of the documentation of the pregnancy and delivery of a mother. This sum was well over the fees determined in the recommendations applicable, and was multiply more than the market price, which, in the opinion of the Authority, significantly curbed the right of informational self-determination of the data subject, and effectually rendered it impossible for financial reasons.

Since the applicability of the GDPR, healthcare providers are obliged to provide a cost-exempt first copy of documentation in the framework of the right of access.

Consequently, the Authority ordered the provider in the case examined to provide a cost-exempt first copy of the documentation to the data subject on grounds of the direct effect of Union law, and called the attention of the head of the State Healthcare Provision Centre to ensure that the institutions it maintains follow the practice detailed. In its response, the data controller reported that it had refunded the fee to the data subject (2018//262/V).

II.1.3.2 The Copy of Data Provided by Data Subjects During the Examination by a Forensic Expert

In the course of judicial or authority proceedings, forensic experts record various personal data from data subjects, have them fill in tests, take down answers to questions, have the examinees make drawings, etc. for expert opinions. These qualify as the personal data of the data subject, which he or she provides during the examination.

These data are distinct from the data and conclusions the expert establishes from the data recorded during examination. As per court rulings as well, these qualify as expert data, and it is up to the expert to decide how he or she presents these conclusions in the expert opinion.
Prior to the entry into force of the GDPR, there were several inquiries where data subjects did not receive their personal data (e.g. tests filled in) when requesting them from experts, who referred to the Privacy Act not stipulating an obligation to provide copies thereof.
It was a regular question in the procedures of the Authority requiring interpretation of law that the information provided under Section 15 (1) of the Privacy Act in effect until July 2018 did not prescribe the obligation to provide the data subject with the copy of the data carrier containing his or her personal data. As a consequence, data controllers regularly referred to the fact that they provide the information on the processing of personal data, but, the Privacy Act not prescribing any such obligation, they did not ensure the provision of a copy of the document containing the given personal data — or data qualifying as such — or an inspection thereof. Decision number 20.971/2013/5 of the Curia supported this argument as well.
The Authority held that the data subject, in view of the essence of the right of informational self-determination, must not be prevented from accessing data on — and, moreover, given — by him or her unless exceptions are provided for by law, and urged data controllers to take a broad view of information and to provide copies thereof on request, but, undoubtedly, law did not require data provision in this case, and a contrary judicial practice also came into being.
The GDPR regulates the legal institution of the right of access of the data subject in essentially, on its merit and function, the same way as the provision of information under Section 15 of the Privacy Act as applicable prior to the Data Protection Reform. In Article 15, it prescribes not only the right to information but also the obligation of providing a copy (Article 15 (3)).
According to Article 23 (1) i) of the GDPR, Member States may restrict by way of a legislative measure the scope of the obligations and rights under its provisions for the protection of the data subject or the rights and freedoms of others.[9]
This restrictions means Section 42 (5) of Act XXIX of 2016 on Forensic Experts, according to which 'the expert shall refuse to provide information due to the data subject under the Act on Informational Self-Determination and Freedom of Information and processed by the expert upon instruction by the appointer or commissioner for purposes of crime prevention and investigation, as well as the protection of the rights of the data subject or others'. The restriction on the provision of information (effectively, access) may be ordered by the appointer or commissioner court or authority.

[9] GDPR Article 23 (1): Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:
(i) the protection of the data subject or the rights and freedoms of others.

The data that the data subject provided in the course of the examination (tests and questionnaires filled in, the data of examination records, etc.) are therefore not data generated by professional conclusions derived by the expert but clearly the personal data of the data subject,[10] and, typically, these are the data the data subject seek to access in their requests thereto.

In the opinion of the Authority, the changed regulatory system under the GDPR coming into effect concerns experts' data processing insofar as, when the data subject requests a copy of the data he or she provided during the examination and is processed by the expert, the expert has to provide a copy, and may only refuse to do so only when justified, when ordered by the appointer court or authority pursuant to Section 42 (5) of the Act on Experts. It is a further important circumstance that the right of access of the data subject does not automatically apply to accessing the examination material of third persons, typically that of the child by the parent.

The provision of data recorded during a psychological examination would imply that the psychologist provides data concerning the safety and psychic integrity of the child to a person who has neither the competence nor the experience to assess the resulting circumstances, which would have a negative and harmful effect on the child. When using the examination data for formulating the expert opinion, the expert must be careful not disclose e.g. the elements of the exploration of the child important for the appointment that might elicit retorsion against the child by the adverse-party parent.

The Authority shares the expert's justification that it falls within the competence of the expert to decide whether to initiate the refusal to provide information on the child to the statutory representative of the child as provided for by Section 42 (5) of the Act on Experts under Article 15 (4) of the GDPR.[11]

Experts must therefore change their practice insofar as, instead of providing information on data processing, data subjects have the right to access their own personal data and also the right to request a copy of their data within its framework, and are thus obliged to provide the data subjects with a copy of their data. The Authority called the attention of the president of the expert chamber that experts are to change their practice accordingly (NAIH/2018/426/V).

II.1.3.3 Parents' Rights, Parental Custody Rights

Recently the Authority received an increasing number of complaints where complainants requested information about their minor children's data from schools, pedagogical expert services, nurseries, healthcare institutions, and the institutions rejected to fulfil their

[10] Point 1 of Article 4 of the GDPR: ' (1) | 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'.

[11] GDPR Article 15 (4): 'The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.'

requests. It turned out that in all cases the complainants were parents not exercising their custody rights.

Under the Civil Code, parents living separately shall exercise their custody rights jointly as a main rule. If one of the parents exercises custody rights — including their partial right of statutory representation — due to an agreement between the parents or a court ruling, the other parent has a right of decision only in the so-called substantial matters provided for by the Civil Code.

Though the Civil Code (4:24) obligates parents living separately to inform each other, this however is often not realized due to the parties' acrimonious relationship. The other parent therefore seeks information directly from the institution, because the parent living separately has not enough information about the child in the lack of cooperation with the parent exercising custody rights.

The protection of personal data as a personality right may be exercised by the data subject, and thus, under the GDPR, it is the data subject — when of majority age, he himself, and, when a minor, his or her statutory representative (Civil Code 2:14) — who may exercise the right of access. It is thus the parent exercising custody rights that may, as the statutory representative, submit data/information access requests.

Certain Hungarian laws (Act CXC of 2011 on National Public Education; hereinafter: 'the Public Education Act') and Act XXXI of 1996 on the Protection of Children and Guardianship Administration; hereinafter: 'the Guardianship Act') designate the parents as recipients of information without specifying whether this implies the parent exercising custody rights or not, or whether it is to be taken as independent, *sui generis* parental information.

Under the Civil Code, even if parental custody is exercised by one of the parents, separated parents shall exercise their rights concerning substantial matters, e.g. schooling and choice of career, which right includes statutory representation, including the right of access to data as discussed above. In the lack of information, the parent living separately cannot take a well-grounded position on the school and career of the child requiring joint decision. In the opinion of the Authority, the right to information processed of the parent otherwise not exercising custody rights covers information relevant to choosing a school/career, and may exercise it proceeding as the statutory representative under the Civil Code.

Besides all these, the Public Education Act provides for the obligation to provide information on 'the development, conduct, and progress at school of the child' as a parental right. The Guardianship Act provides for the parent's right to inspect documents (at e.g. the nursery) and to request a copy thereof (Section 136/A).

In sum, the concepts of parent and statutory representative in the case of parents living separately and exercising custody rights do not overlap, and, while under the GDPR and the Civil Code, the statutory representative has the sight of access to/information on data, it is the 'parent' — i.e. also the one not exercising custody rights and thereby not proceeding as the statutory representative — that has the right to access the same data content or request a copy thereof under the Guardianship Act. The Public Education Act does not define the recipient or the scope of the information to be provided.

As a result of the not unambiguous formulations of these laws, the practice of data controllers is not unified in respect of whether the parent not exercising parental custody is entitled to access data under these laws or not, and if he or she is, what the scope of the data is, and if the data subjects — separated parents not exercising parental custody — refer to their right of access or inspect documents provided for by law.

Pursuant to data protection rules, the data controller that provides data upon request not to the data subject — the statutory representative of the minor — commits unlawful transfer of data and can therefore be held accountable thereof. The data controller may not consider that, the parent exercising custody rights not providing the information to the separately living parent in accordance with the Civil Code, it should disclose the data. Data controllers, 'just to be on the safe side', avoid unlawful transfer of data, and disclose as little information as possible. However, not complying with the obligation to provide information under specific laws is likewise unlawful.

Under law, the parent not exercising custody rights may not request healthcare data on the child. Section 24 of the Healthcare Act provides for the right to request information on healthcare data, but, as the health condition of the child does not appear among the substantial matters defining the affecting the future of the child, the parent not exercising custody rights is not entitled to request access to data/information in this regard.

Such parent may not request information from the family doctor on what illnesses and medication the child had, and, if the other parent does not designate the family doctor, he or she may not obtain the information on the identity of the family doctor from the healthcare administration organ, nor may he or she, for that matter, receive information about what health reason the child is absent from kindergarten/school. Not even does the Public Education Act provide for the disclosure of such data content.

The parent who does not exercise custody rights is therefore not entitled to receive information on his or her child in cases where he or she has no right to make decisions or juridical acts. Though his or her right to make decisions is limited to substantial matters, it is to be examined, in the opinion of the Authority, whether the parent living separately and not exercising custody rights is entitled or not to request information directly from the institutions purely for the sake of obtaining information. In other words, he or she is not entitled to receive information about the child pursuant to the GDPR, because, lacking the quality of statutory representative, he or she is often not entitled to, but as parent in his or her own right may be.

On the basis of the above, the Authority requested the Commissioner for Fundamental Rights to examine whether the legal background and practice of providing information to parents living separately and not exercising custody rights is appropriate or not, or whether it would be justified and possible to provide for the right of parents to the provision of information in law irrespective of the right of access to the data of the child under Article 15 of the GDPR.

II.1.3.4 Data Processing by Websites

The issue of the data processing by websites featured several times in the 2018 practice of the NAIH. Under Article 2 of the GDPR, the material scope of the regulation extends to, aside from those listed there, all processing of personal data irrespective of whether the operator of the website is a big corporation, an SME or a private person. Insofar as a website processes personal data, it shall apply the rules of the GDPR, including those on the obligation to provide information under Articles 13 and 14 and to maintain records under Article 30 (1) thereof.

As per point 1 of Article 4 of the GDPR, personal data means any information directly or indirectly relating to a natural person. These include pseudonymized personal data as well, such as nicknames or e-mail addresses when they do not include the actual names of the natural persons. Unrecoverable hashes may, in certain cases, not be personal dada, but that they cannot be related by anyone to a natural person can only be established on the basis of all the circumstances of the technical realization of the data processing. As per Article 5 of the GDPR, data processing may not extend to personal data inappropriate, unnecessary or disproportionately numerous for the specific purpose of the data processing, and may only last for the period necessary for the specific purpose.

Under the GDPR, the processing of personal data here also requires one or more lawful purposes and legal bases. The taxonomic list of possible legal bases is given in Article 6 (1) of the GDPR, and only one of these may be associated with a given purpose — it being the responsibility of the data controller to choose one in a given case — which may not be changed afterwards one-sidedly.

It is expedient to be base the processing of cookies, server logbooks (e.g. the logging of IP addresses) or other personal data necessary for the fundamental operation of the given website and the security of the information system on legitimate interest under Article 6 (1) f) of the GDPR, because, if data processing is necessary for the fundamental operation of the given website and the security of information system, the website would be objectively inaccessible otherwise, and thus could not be subject to valid consent.

When referring to Article 6 (1) f) of the GDPR, it is important to document in advance that the enforcing of the given legitimate interest(s) has priority over the right of disposal of the data subjects using the website and what technical, organizational, and procedural measures are put in place to ensure the safety of the personal data of the data subjects (legitimate interest test).

In the case of the processing of cookies, server logbooks or other personal data which are not necessary for the fundamental operation of the given website and the security of the information system (serving e.g. statistical, convenience, marketing, etc. purposes), consent under Article 6 (1) a) of the GDPR is generally applied as a legal basis.

In its guidelines WP259, Working Party 29 specifies the conditions of consent under the GDPR. According to this, it is a minimum requirement that consent be informed, freely given (it can be refused or withdrawn without negative consequences), unambiguously indicated,

and specific, as well as the data controller is able, under Article 5 (2) of the GDPR, to demonstrate at any time that the given data subject has actually given consent. The condition of unambiguous indication is not met when consent is collected by way of pre-ticked boxes, passive conduct not qualifying as appropriate. The condition of specificity is not met when different, independent data processing purposes or data processing by different data controllers cannot be consented to separately, only in a 'package'.
Intended by the legislator to review the currently effective Directive 2002/58/EC ('ePrivacy Directive'), the Regulation on Privacy and Electronic Communication (ePrivacy Regulation), which is still under consultation with the Member States, will contain the special rules of online data processing and direct marketing.

II.1.4 Certain Important Cases

II.1.4.1 The Data Processing of the Church of Scientology in Hungary and Church of Scientology Mission XVIII

1. Precedents

Both the Data Protection Commissioner and the Authority have examined the data processing of the Church of Scientology in Hungary on several occasions. The last inquiry of the Authority was concluded in October 2017, and examined the data processing practice of not only the Church of Scientology but also its highest-level organization, Central Organization of the Church of Scientology in Hungary. In this procedure, the Authority assessed the processing of the personal data of employees, the forms used upon joining the Church and the compliance with law of the scope of data these collect and the data processing carried out in the course of the services provided by the Central Organization of the Church of Scientology. In its decision, the Authority established several infringements of law, prohibited the unlawful data processing practice, and imposed the maximum data protection fine possible, HUF 20 million on each of the organizations. The judicial review of the decision is currently in progress.
In order to become acquainted with and assess the data processing practice of the local organizations, the so-called missions, of the Church of Scientology in Hungary, the Authority ex officio initiated a data protection procedure against Church of Scientology Mission XVIII, the Mission of Nyíregyháza (hereinafter: 'the Mission'), parallel to the procedure mentioned. The decision in case of the Mission was adopted in 2018.
In respect of these data processing activities prior to the coming into force of the GDPR, the Authority examined their compliance with the former provisions of the Privacy Act.

2. The Procedure

In order to clarify the facts of the case, the Authority conducted an on-site inspection without prior notification thereof. In the course of the on-site inspection, the Authority seized all documents and data carriers that had personal and sensitive data in them. The

Authority included the Church of Scientology as a party in the procedure too (the two examined data controllers together hereinafter: 'the Church').
On account of the fact that the Authority had to become acquainted with the records of the Mission processed electronically, it appointed a forensic IT expert. It also found it necessary to examine the effects of the special data processing activities of the data controllers on the decisions of the data subjects, on e.g. freely given consent as the legal basis of data processing, and therefore, to examine this, it appointed a clinical psychologist forensic expert.

3. The Types of Folder

Since the Church of Scientology fully operates on the basis of the strictly controlled, unified principles and practices of the International Church of Scientology, the data processing under examination is embodied in various paper-based folders already known from the previous procedure.
The purpose of the various services offered by the Church is to assist the believer, the Preclear, on the road to spiritual freedom. In the course of providing these services an extremely huge amount of personal and sensitive data is processed, as various folders are kept for believers. The Authority found that these folders process the data of not only the believers but also, and typically so, those of third persons.
In accordance with the rules laid down by the Church of Scientology, the folders systematically contain various forms, reports, and notes. Among them are the so-called PC Folders, which contain the notes, records, and reports made during the most important services, auditing and detoxification, of the Church; Ethics Folders, which collect reports of actions considered ethically inappropriate by the Church and documents generated by the internal justice system; CF Folders, or mailing files, which include correspondence with copies of letters to believers; Staff Member Folders, which include collected together agreements, forms for qualifications, interviews, and tests.

4. The Identification of Data Processing Activities

The data processing activity of the Nyíregyháza Mission is related to three purposes:

I. The data processing purpose related to the services provided to believers and monitoring their spiritual development, primarily in the PC and Ethics Folders;
II. The data processing purpose related to the application and aptitude testing of staffers and employees, primarily in Staff Member Folders;
III. Direct marketing purpose, CF Folders.

5. Auditing and Detoxification

PC Folders include the notes, records, and reports made during the most important services, auditing and detoxification, of the Church, which contain great numbers of personal data of both believers and third parties.
Auditing is a procedure based on a predefined schedule; an auditor (a minister of the Church of Scientology), and a believer ('preclear') participate in, and the auditor asks questions, and acknowledges and records the answers; auditing is supported by a 'religious artefact', the E-meter.
During auditing, the believers share an extremely high number of personal and sensitive data with the auditor, in the course of which much data related to third persons, personal and sensitive data of third persons are recorded in the worksheets.
The PC Folders include also several documents with highly sensitive data on PCs, their former diseases, operations, mental and physical conditions, family relations, the personal data of family members, etc.
'Detoxification' is also a characteristic service of the Church. The Detoxification Programme is preceded by medical examination for fitness and the related filling in of a fitness form—stored by the Church—with the personal and sensitive data of the believer (e.g. blood pressure, symptoms of anaemia, heart, liver disease, diabetes, use of drugs and medicaments, former operations, etc.).
As in its 2017 decision, the Authority found, in the case of the PC Folders, that the Church had failed to provide appropriate information in the declarations required to be signed before the beginning of services, because the data controller was not identified clearly, and the purpose of data processing was outlined far too briefly. In the opinion of the Authority, in the case of a complex data processing that treats a great many personal data, such as the data processing under consideration, the purpose of the data processing, the range of data processed in relation to that, as well as the way those are used to achieve the purpose specified must be stated clearly and far more understandably. It is only in this way that the data subject can decide whether to give his or her consent to the data processing. The notices do not indicate precisely which Church persons, officials or staff members are entitled to access the data; do not provide complete information on data subject rights, remedies, and do not obtain consent to data transfers.
On account of the fact that all services, including detoxification, are carried out under the strict guidance of the Church of Scientology, it could be established in the case of the detoxification programme of the Mission that, as in the first decision, the healthcare data, data on the medical check-up and medical reports should have been processed on the basis of consent only by the examining physician or the medical service provider, who should have handed over to the Church only the information that the data subject fulfilled the conditions of participation in the programme or not.
As a result, the Authority found that the Church infringed Section 20 (2) of the Privacy Act and, because of the insufficient provision of prior information, the requirements of consent under Section 3 (7) of the Privacy Act.

The Authority also found, as in the first Decision, that the Church processed sensitive data in the course of auditing and detoxification, the legal basis of which may not be Section 5 (2) a) of the Privacy Act, and the legal basis under Section 5 (2) c) of the Privacy Act cannot be established in the data processing of the Church; and, in view of the fact that the Church had designated religious services as the purpose of data processing, this purpose cannot be reconciled with provisions on data processing with healthcare network under Section 4 (1) of Health Data Act nor the provisions on other purposes under Section 4 (2) of Health Data Act. The consent as legal basis under Section 4 (3) of the Health Data Act can likewise not established.

The Authority regarded the processing of personal data of third parties without appropriate legal basis a particularly grave infringement of law is. According to the definition of the Privacy Act, all data in the documents held in the Folders concerning persons other than the PC is to be deemed a third party and personal data relating to a third party. This includes, for example, data on the applicant's relatives, friends, acquaintances, and love partners. In several cases, the Authority identified sensitive data of third persons in the documents seized from the Nyíregyháza Mission in spite of the fact that the data controllers had not obtained any consent form the data subjects.

The Church breached the principle of purpose limitation under Section 4 (1) of the Privacy Act by processing the personal data of third parties. In the opinion of the Authority, the Church processed the personal data of third persons in the course of processing the documents held in the PC Folders without a defined purpose and without the provision of appropriate prior information.

If data processing has no lawful purpose, it is then, on the basis of the above, unlawful. It must however not be forgotten that the Church not only failed to provide these third parties information on the circumstances of the data processing, but processes the personal and sensitive data of these persons without their slightest notion of the Church doing so at all. By this data processing without the provision of information, the Church acquires a 'dominant informational position', which is extremely damaging to the rights of these third parties to the protection of personal data and to privacy, they cannot enforce their right to informational self-determination; moreover, the data processing qualifies also as unfair. Due to the absence of prior information, the requirements of being specific and freely given are also not met. Concerning consent, it should also be noted that the given data subject's—the PC's—consent cannot bear the interpretation that it applies to another person, that it is made instead of another person, the PC's consent cannot be construed as the consent of a third party.

Collecting and recording the data of data subjects who qualify as third parties not being in any legal relation with, not being members of, the Church is also objectionable, because there is no lawful or acceptable purpose that unconditionally necessitates or at least renders acceptable the processing of their personal, often sensitive data. Recording certain persons' data for a purpose they have nothing to do with or because of a legal relationship or a

consent that does not apply to them cannot be justified and is wholly unnecessary, moreover it means an unwarranted infringement of their privacy.
Respecting the right to privacy of the data subject in no legal relationship with, not being a member of, the Church has priority over the interests of the Church or the PC sharing the data in the course of a procedure. The Church may record and process data in relation to providing religious services where it has a valid legal basis.
With regard to the Nyíregyháza Mission, the Authority therefore also found that it may not connect the personal and special data of the PC to the personal and special data the PC gives of persons living in his or her environment, because processing the personal data of persons with no legal, membership, relationship with the Church of Scientology violates the principles of purpose limitation and necessity.
In addition, the Authority also found that it is also without appropriate legal basis that the Data Controllers processed the personal and special data of third parties, because none of the conceptual elements of the legal basis they indicated, consent, is met: third parties had received no prior information; it was not freely, themselves personally, that they gave consent to the processing of their personal data, and consequently a further conceptual element, consent being specific, could not be effected. Since no other legal basis can be established—such as a law requiring the processing of these data on the basis of public interest—the Church violated Sections 3 (7) and 5 (1)–(2) of the Privacy Act.
On account of the aforementioned, the Authority, in the operative clause of its Decision, prohibited the processing of health data, ordered the provision of appropriate information to believers, the re-obtaining of their consent, the erasure of the personal data of those persons who did not confirm their consent and third persons, and prohibited the practice of collecting data relating to third parties.
As an infringement related to the PC Folders, the Authority established in this procedure as well that the right of the data subjects to access their personal and sensitive data processed is not ensured, the believers not being allowed access to their PC Folder. It is part of the right to informational self-determination of the data subject that he or she be able to track and control the entire path of data processing, that is, he or she has the right to know who uses his or her data, and when, where, and why so, and thus the Authority found that the Church violated the data subjects' right under Section 14 a) of the Privacy Act.

6. Ethics Folders

An Ethics Folder includes reports on a believer or a staff member, records and results of ethics and judicial procedures taken in respect of a person, as well as various praises of him or her. Knowledge Reports make up the bulk of the Ethics Reports. Believers write various reports on each other in these, calling attention to the irregularities of others' lifestyle, work, duties done in the Mission, and love relationships. The reported irregularities range from insignificant 'sins' to others' health, financial or sex life, even crimes a believer committed.
The documents of the Church's internal judicial procedures are also kept in Ethics Folders. As it appears from several Church forms, statements to be completed by believers, believers essentially forgo taking the disputes between each other and the Church itself to court,

disputes can only be resolved by the religious authorities of Scientology. Various procedures were therefore developed to investigate and penalize ethics and other vices.
In respect of this type of folder, the Authority also found the infringement presented above; that is, processing of the personal and sensitive data of both believers and third parties without appropriate legal basis.

7. Staff Member Folders

Before being employed, applicants are required to fill in various application form, aptitude tests, and questionnaires, which provide an extreme amount of personal and sensitive data for the Church.

Having reviewed the information provided in the forms related to employment, the Authority found, just as in the case of PC Folders, the Data Controllers violated the requirement of providing prior information and, as a consequence, because prior information is one of the conditions of consent, also the requirement of consent under Section 3 (7) of the Privacy Act, and it could therefore be established that the Church processed the personal data of job applicants without legal basis, infringing Section 5 (1) a) of the Privacy Act.

8. Correspondence Folders and Direct Marketing

In this regard, the Authority examined the lawfulness of the processing of personal data carried out in the correspondence folders, a database which can be regarded as an electronic register of members, the various online surfaces — websites such as the ones for filling in the Oxford Capacity Analysis, the most important personality assessment test of the Church, and online book selling.

The Authority found the marketing activity of the Church to be in breach of the law in two respects:

- The Data Controllers failed to obtain the consent of the data subjects within the meaning of Section 6 (1)–(2) of Act XLVIII of 2008 on the Fundamental Conditions of and Certain Constraints Commercial Advertising (as well as Section 3 (7) of the Privacy Act), because obtaining consent in respect of the processing all data collected in the ways mentioned above is necessary for the lawfulness of data processing for marketing purposes; and
- On account of the fact that the sources of the data subjects' consent cannot be established from electronic records kept by the Data Controllers, it can be concluded that the Data Controllers failed to comply with their obligation to maintain records of the sources of consent under Section 6 (5) of the Commercial Advertising Act.

9. Operative Clause and Imposition of Fine

In view of the above, the Authority prohibited the Data Controllers from further unlawful data processing, and required them both to modify their practice of providing prior information to comply with effective provisions of law, to provide their data subjects with appropriate prior information, and request all their data subjects' consent or reaffirmation of consent. In the lack of reaffirmed consent, the Authority ordered the data controllers to document the erasure of the data subject's data. The authority prohibited the collection of personal data without appropriate purpose and legal basis from third parties not qualifying as staff members, employment applicants and believers, and ordered the erasure of data processed in such a way. The Authority also ordered the Data Controllers to terminate the transfer of certain personal data of data subjects without an appropriate basis, and to comply with data security requirements in respect of the transfer of personal data to other countries.

Beyond these, the Authority imposed a data protection fine of HUF 12 million on each of data controllers. In determining the sum of the fine, the Authority took into account all the circumstances of the case, in particular the number of data subjects, the gravity and repeated nature of the violation of law.

II.1.4.2. Google Cases

1. On 29 October 2018 the NAIH ex officio initiated an administrative audit in view of the fact that the data available were not sufficient to assess whether Google LLC is the sole data controller in the provision of services according to the notice on the website https://policies.google.com/privacy?hl=hu&gl=ZZ , and to assess whether Google Kft. is related to the data processing mentioned above, and if yes, in what quality.
In the course of audit, the Authority requested data and declarations from both Google LLC and Google Kft., and they both declared that Google LLC carries out cross-border data processing, in respect of which its main establishment is in Ireland under Point 16 of Section 4 of the GDPR, and, as Google Ireland Ltd is a branch of its central administration in the Union, the Irish supervisory authority qualifies as the lead supervisory authority. They also stated that Google LLC is the data controller in respect of the processing of personal data related to the notice being audited, the services of Google LLC, and Google Kft. performs no data processing in this respect. Google LLC also reported that preparations were under way to transfer some of the data processing activity to Google Ireland Ltd, but this was not completed when the answer was made.

In negotiations towards clarifying the competent lead supervisory authority under Article 56 of the GDPR in respect of complaints from Member States to the data protection authorities of other Member States and personal data breaches, the Irish data protection authority stated that it could not currently be regarded as the lead supervisory authority under Article 56 of the GDPR in respect of data processing of Google LLC.

As result of the above, the NAIH requested — in order to clarify the authority competent to act in a procedure under Article 61 (1) of the GDPR — the Irish data protection authority to provide more detailed information on the circumstances and facts corroborating its position. In its response the Irish data protection authority explained that, in its interpretation, Google LLC, in the lack of data processing within the Union, has no main establishment in the Union, and the one-stop-shop mechanism therefore does not apply. If Google LLC changes its operation and data processing processes appropriately, the Irish data protection authority may become the lead supervisory authority under Article 56 (1) of the GDPR as of 22 January 2019.

2. In a request submitted to the NAIH, a Hungarian data subject reported that he contacted electronically the operator of Google AdWords, Google Ireland Ltd, under Article 15 of the GDPR, and requested information as to the processing of a name being a personal data as a keyword associated with advertisements in the Google search engine, but Google Ireland Ltd failed to fulfil this request exercising data subject rights.

Pursuant to the rules of the GDPR, the data processing in the request qualifies as cross-border data processing in respect of which the NAIH is an authority concerned, and thus the Irish data protection authority, the supervisory authority of the main establishment of Google Ireland Ltd as the lead supervisory authority under Article 56 of the GDPR, needs to be requested in order to clarify whether the case should be handled as a local case under Article 56 (2), or whether it intends to act as the lead authority of the main establishment. The request of the data subject was received by NAIH before 22 January 2019, but the decision is to be made in the case after 22 January 2019, and thus, other detailed rules in the GDPR lacking, the Irish data protection authority may decide on the request of the NAIH which data protection authority of the Member States will act in the case.

3. In another case, a complainant, a well-respected public person, objected to URLs appearing in the list of Google search results that contain offensive and irreverent information of the person's deceased spouse and family life. Google had previously rejected the request on grounds of public interest, but, complying with the order of the NAIH, the irreverent links were finally removed from the list of results.

It should be noted here that delisting means merely the cancelling of the link, that the search engine does not list the URLs removed, but the websites concerned will have the information available. If the data subject wishes to have the data deleted, he or she needs to turn to the data controller or the operator of the website requesting the erasure of the data.

4. Beyond those mentioned, the Authority directly contacted Google in several cases. A part of these was meant to map general practice, but there were cases when the Authority, referring to the modified legal environment (GDPR, Section 25 of the Privacy Act), required the data controller to review its former position. We asked Google on what basis it ranked search results, how the search algorithm worked, what were the criteria of ranking, and what measures it took to comply with the requirements of the GDPR in respect of the search engine.

The following links may assist orientation:

- https://transparencyreport.google.com/eu-privacy/overview
- https://policies.google.com/privacy?hl=hu
- https://privacy.google.com/your-data.html.
- https://support.google.com/transparencyreport/answer/7347822/?hl=hu

II.1.4.3. The ISZT Case

In case number NAIH/2018/3474/H, the NAIH found in its decision published on website ((https://www.naih.hu/files/NAIH-2018-3474-H-hatarozat.pdf) that the data processing practice related to .hu highest domain registration of ISZT Non-profit Company Limited [Council of Hungarian Internet Providers Non-profit Company Limited] did not comply with the effective laws in the period examined, 2012–2017. As a result, the Authority issued a warning, and prohibited the data controller from further infringement of law. ISZT undertook to change its data processing activity concerning '.hu' domain registration and to provide appropriate information to data subjects taking into account the GDPR coming into force in the meantime. The undertaking is being monitored and controlled by the NAIH.

II.2 Personal data breach Notification and Prior Impact Assessment

II.2.1 Consultation with the Authority on Data Protection Impact Assessment

Under Article 35 (1) of the GDPR, a data protection impact assessment shall be carried out when data processing is 'likely to result in a high risk to the rights and freedoms of natural persons'. The aim of an impact assessment is to reveal the nature of the data processing, examination of its necessity and proportionality, and, the assistance of managing the risks to the rights and freedoms of natural persons resulting from the processing of personal data by way of assessing those risks and defining the measures envisaged to address the risks.
According to the Working Party 29 Guidelines on Data Protection Impact Assessment (hereinafter: 'the DPIA Guidelines')[12], if a data protection impact assessment indicates that the processing would, in the absence of safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of natural persons and the controller is of the opinion that the risk cannot be mitigated by reasonable means in terms of available technologies and costs of implementation, the supervisory authority should be consulted prior to the start of processing activities (see Article 36 (1) and Recital (94) of the GDPR).

[12] Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 [WP249 rev.01]

On the basis of the above, the supervisory authority is required to be consulted on the results of a DPIA when the data controller, having assessed the risks to the rights and freedoms of data subjects, cannot find sufficient measures to reduce the risks to an acceptable level, i.e. the residual risks are still high.

An example of an unacceptable high residual risk includes instances where the data subjects may encounter significant, or even irreversible, consequences, which they may not overcome (e.g.: an illegitimate access to data leading to a threat on the life of the data subjects, a layoff, a financial jeopardy). Under Article VI (4) of the Fundamental Law and Section 38 (2a) of the Privacy Act, the Authority is the supervisory authority as per the GDPR, and consequently it shall be the Authority to conduct the prior consultation on a DPIA.
In the framework of a prior consultation, the Authority assesses, on the basis of the documentation of the DPIA already carried out by the organization, whether the DPIA met the provisions of the GDPR and the DPIA Guidelines, and whether it can assist in the mitigation of the residual risks.

Article 36 (3) of the GDPR specifies the information the data controller is to provide to the Authority during consultation. In the course of the consultation, the Authority examines the actual process of the DPIA, and thus, on the basis of the data processing processes it was informed of, it focuses on whether the data controller identified the data processing activities and the risks of data processing precisely, and whether the data controller is successful at bringing measures to address the risks. Furthermore, the Authority examines whether the assessment of the scope of data to processed clearly separates personal and sensitive data in the processing, whether data processing is always lawful, and whether the data controller conducted the legitimate interest test. A DPIA can be conducted with the help of several different methods, but it must take into account the same criteria, because its basic features are determined by the GDPR. With regard to determining the basic criteria of a DPIA, the Authority emphasizes Annex 2 of the DPIA Guidelines, which lists the common criteria developed by data protection authorities to assist data controllers to choose between DPIA methodologies and to comply with GDPR provisions. In the course of consultation, the Authority always emphasizes that risk assessment concerns processes related to the processing of personal data and data processing operations, which, as a result of the DPIA, imply risks to the rights and freedoms of the data subjects. The essence of a DPIA is the prior control of data processing through the exploration of risks and the assessment of measures to be made to address them. A risk must be clear and specific, and thus the data controller must conduct a risk assessment to be able to identify a risk.
Essentially, a DPIA consists in two major parts. On the one hand, the data controller assesses compliance with the principles of data protection, performing a sort of legal compliance analysis. On the other hand, the data controller has to assess the data security measures, that is it must conduct an IT security analysis as well. Under a DPIA, it is particularly data security measures that provide scope for action for risk reduction. Accordingly, the Authority recommends the choice of a method that the given data protection authority has already brought into line with the provisions of the GDPR. Such is the methodology published by the French data protection authority (CNIL) on its website, the use of which is further assisted by the fact that CNIL has published an open-source software whereby data controllers can easily prepare a DPIA appropriate to the method. The CNIL software was developed for data

controllers that are somewhat adept in conducting a DPIA. They can easily download it, and start an independent version. It can be downloaded onto a server, and an organization can use it integrated with other devices and systems within itself. The software is available in Hungarian from the website of the Authority.

If the Authority finds during consultation that the planned data processing would infringe the GDPR, especially when the data controller failed to identify and address the risk, it may exercise its powers pursuant to Article 58 of the GDPR, and may, among others, issue a ban on the processing (GDPR Article 36 (2)).

II.2.2 Prior Consultations with the Authority on Draft Legislation DPIA

Under Article 36 (4) of the GDPR, the supervisory authority shall be consulted during the preparation of a proposal for a legislative measure to be adopted by a national parliament, or of a regulatory measure based on such a legislative measure which relates to processing.

In Hungary the DPIA of draft legislation is provided for by the Privacy Act following the coming into effect of the Amendment Act. Section 25/a (6) thereof states with regard to mandatory processing that the DPIA shall be carried out by the party preparing the legislation that requires processing. By mandatory processing the Act means data processing based on provisions of law (thus data processing under Article 6 (1) c) and e) of the GDPR).

Accordingly, the preparer of legislation must conduct a DPIA when drafting legislation concerning or prescribing the processing of personal data.
According to the DPIA Guidelines, the supervisory authority is required to be consulted on the results of a DPIA when the data controller, having assessed the risks to the rights and freedoms of data subjects, cannot find sufficient measures to reduce the risks to an acceptable level (i.e. the residual risks are still high).

In view of the recommendation, the Authority holds that prior consultation is necessary only when the DPIA finds that risks continue to be significant and the data controller cannot reduce them to an acceptable level. The Authority regards this prescription as governing with regard to a DPIA to be conducted during legislation where the GDPR is applicable to the planned data processing. Insofar as the DPIA conducted in the course of drafting legislation indicates that the planned data processing involves high risks, and the data controller cannot reduce them, the party preparing the legislation shall initiate consultation with the Authority. This prescription governs data processing subject to the GDPR. Thus, in the case of drafting legislation for data processing subject to the GDPR, consultation is required for data processing where residual risks are high, and the data controller cannot reduce them.

The situation is different with regard to data processing subject no to the GDPR but exclusively to Hungarian jurisdiction. In respect to them, it is the provisions set forth in Section 25/H (1) and (2) of the Privacy Act that define the conditions of prior consultation.

Under the Act, high risk and thus the necessity of prior consultation shall be presumed in the case of data processing for criminal investigation, national security and national defence from among those exempted. Accordingly, a DPIA must be conducted and the Authority must also be consulted by the party preparing legislation to regulate data processing for criminal investigation, national security, and national defence purposes.

In the case of preparing legislation related to data processing subject to either the GDPR or exclusively Hungarian jurisdiction, it is important to note that, in the event of prior consultation, the Authority shall conduct it with the party preparing the legislation (usually the ministry concerned). If drafting has been concluded, the legislative proposal submitted to parliament for adoption, and the Act perhaps even promulgated, the consultation procedure shall also be concluded, and cannot be continued after adoption.

II.2.3 The Substantive Criteria of DPIAs Conducted During the Preparation of Legislation

With regard to the DPIA documentation annexed to the draft legislation, the Act prescribes only that it shall contain the general description of the planned data processing operation, the description and features of the risks to enforcement of fundamental rights of the data subjects the data controller identified, and the measures designed and implemented to address those risks and to ensure the enforcement of rights related to personal data. The documentation of a DPIA made during the preparation of legislation must therefore include the same elements as in the case of DPIA conducted by a data controller.

The DPIA documentation must describe the specific data processing defined and envisaged by the draft legislation (e.g. the operation and use of processing systems) and how the data controller intends to mitigate the related specific and identified risks. It is thus not enough for the DPIA to state in general ‘there is a risk of identity theft’, it must describe precisely how this might take place with regard to the given data processing (e.g. an unauthorized hacker might access the password of the system administrator). The measures to address the risks identified (e.g. monthly software-enforced password changes) must also be specifically described in the DPIA documentation.

Naturally, the party preparing legislation is usually unable to identify specific risks within its competence, because it does not have all information available pertaining to the data processing. Resolving this might require consultation with the future data controller, who might be requested to comment on the DPIA documentation.

It may also naturally occur that the risks arising from the data processing cannot be identified during preparing the legislation (e.g. the text of the law provides a general authorization for data processing). If this is the case, the legislator must clearly say so in the DPIA documentation and decide on the future amendment of the DPIA (e.g. by

commissioning the data controller to conduct a full-scale DPIA before putting the system into operation and developing its technical parameters).

II.2.4 The Impact Assessment List

Under Article 35 (4) of the GDPR, supervisory authorities shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment. Upon compiling the draft list, the Authority sent it to the European Data Protection Board. With regard to the list sent, the Board prosed amendments and additions in its Opinion number 10/2018 in accordance with the vote held at its meeting on 25–26 September 2018. The Authority accepted the proposals in the Opinion, and the accordingly modified list was uploaded in the IMI system on 11 October 2018, and the Authority also published it on its website in both Hungarian and English. The published list was amended again pursuant to the decision of the meeting of the Technology Subgroup on 19 December 2018; the concept of biometric data under Article 4 of the GDPR in the list shall be applied with the addition under Article 9 of the GDPR. The addition ensures concord with Article 9 (1) of the GDPR, and also provides greater assurance for data controllers as which data processing is subject to the list.

The list includes the following data processing operations:

1) Where the processing of biometric data for the purpose of uniquely identifying a natural person refers to systematic monitoring.

2) Where the processing of biometric data for the purpose of uniquely identifying a natural person concerns vulnerable data subject, in particular, concerning children, employees, and mentally ill people.

3) Where the processing of genetic data is carried out in connection with sensitive data or data of a highly personal nature.

4) The purpose of the processing of genetic data is to evaluate or score of a natural person.

5) Scoring. The purpose of data processing is to assess certain characteristics of the data subject, and its result has an effect on the quality or the provision of the service provided and to be provided to the data subject.

6) Credit rating. The purpose of data processing is to assess the creditability of the data subject by way of evaluating personal data in large scale or systematically.

7) Solvency rating. The purpose of data processing is to assess the solvency of the data subject by way of evaluating personal data in large scale or systematically.

8) Further use of data collected from third persons. The purpose of data processing is the use of personal data collected from third persons in the decision to refuse or cancel a service to the data subject.

9) The use of the personal data of pupils and students for assessment. The purpose of data processing — regardless of whether tuition is at primary, secondary or advanced level — is to record and examine the preparedness, achievement, aptitude, and mental state of pupils and students, and the data processing is not statutory.

10) Profiling. The purpose of data processing is profiling by way of evaluating personal data in large scale and systematically, especially when it is based on the characteristics of the workplace performance, financial status, health condition, personal preferences or interests, trustworthiness or conduct, residence or movement of the data subject.

11) Anti-fraud activity. The purpose of data processing is to use credit reference, anti-money-laundering or anti-terrorism financing, and anti-fraud databases for screening clients.

12) Smart meters. The purpose of data processing is the application of 'smart meters' set up by public utilities providers (the monitoring of consumption customs).

13) Automated decision making producing legal effects or similarly significant effects. The purpose of data processing is to make decisions with legal effects or other significant effects on natural persons, which decisions might result in the exclusion of or discrimination against individuals in certain cases.

14) Systematic surveillance. Systematic and large scale surveillance of data subjects in public areas or spaces by camera systems, drones or any other new technology (wifi tracking, Bluetooth tracking or body cameras).

15) Location data. Where the processing of location data refers to systematic monitoring or profiling.

16) Monitoring employee work. Where the purpose of data processing is the systematic and extensive processing and assessment of employee's personal data in course of the monitoring of employee work, including, e.g. placing GPS trackers in vehicles, and camera surveillance against theft or fraud.

17) Processing of considerable amounts of special categories of personal data. Under Recital (91) of the GDPR, processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer.

18) The processing of considerable amounts of personal data for law enforcement purposes.

19) Processing of large amounts of data related to vulnerable data subjects for purposes different from the original purpose, in the case of, e.g., the elderly, children, and mentally ill persons.

20) The processing of the personal data of children for profiling, automated decision making, marketing purposes or providing them information society related services directly.

21) The use of new technologies for data processing. This includes the processing of large amounts of data obtained via sensor-equipped devices (e.g. smart televisions, smart household appliances, smart toys, etc.) and transferred through the Internet or other channels, and such devices providing data on the characteristics of the financial status, health condition, personal interests, trustworthiness or conduct, residence or movement of the natural person, and such data form the basis of profiling.

22) The processing of health data. In respect of large amounts of special data processed by hospitals, healthcare providers, and private medical services or non-medical practitioners with a large clientele. This also includes the processing of health data collected from members of major sports establishments or workout rooms.

23) When the data controller is planning to set up an application, tool, or platform for use by an entire sector to process also special categories of personal data.

24) The purpose of data processing is to combine data from various sources for matching and comparison purposes.

The fact that a data processing appears in the list does not mean that data controllers have to carry out a DPIA in these cases. If the data processing meets the conditions set forth in Article 35 (1) and (3) of the GDPR, the data controller shall conduct a DPIA.

II.2.5 Personal Data Breaches

Under Point 12 of Article 4 of the GDPR, personal data breach means a breach of security leading to the accidental or unlawful destruction, loss (damage to availability), alteration (damage to integrity), unauthorized disclosure of, or access to (damage to confidentiality), personal data transmitted, stored or otherwise processed.
In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay. If the personal data breach occurs within the scope of action of the data processor, the data processor shall notify the data controller without undue delay after becoming aware of a personal data breach.
If the data controller is reasonably certain about the occurrence of a personal data breach, but does not possess all the relevant information, it is worth applying the opportunity of recurring notification in order to comply with the 72-hour deadline. Such notifications may be supplemented, corrected, and modified later with the information not available at first.

Personal data breach notifications can be sent to the Authority by post or electronic mail (ugyfelszolgalat@naih.hu), for which the form can be downloaded from the website of the Authority (http://naih.hu/adatvedelmi-incidensbejelent--rendszer.html); or on the notification surface specially dedicated to this purpose by the Authority (https://dbn-online.naih.hu/public/login). The personal data breach notification portal is exclusively meant to facilitate the process of personal data breach notification for data controllers, and not for submitting complaints.

When examining a notification, the Authority particularly focuses on whether it contains at least the following provided for by Article 33 (3) of the GDPR:

a) the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
b) the name and contact details of the data protection officer or other contact point;
c) the likely consequences of the personal data breach;
d) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

The copy of the section of the personal data breach record the data controller maintains is an important part of the notification (and, in a given case, the response to a procedural decision to clarify the facts of the case).

From the GPPR's coming into effect until 31 December 2018, the Authority received 244 personal data breach notifications. The Authority examines the fulfilment of personal data breach notification obligations by the data controller in accordance in the framework of administrative audits provided for by Act CL of 2016 on the Code of General Administrative Procedure (hereinafter: 'the Administrative Procedure Act'). If the notification and its supplements do not contain the necessary information, the Authority shall contact the data controller to clarify the facts of the case.

If the Authority finds an infringement of the obligations under Articles 33 and 34 of the GDPR in the course of the administrative audit, it shall initiate an authority procedure; in a contrary case, it shall conclude the administrative audit. On the basis of circumstances revealed by way of administrative audits related to personal data breach notifications, authority procedures were initiated in 7 cases in 2018; however, there were no fines imposed in concluded cases.

The following is a list of typical personal data breaches in practice alongside the measures to mitigate the risks as expected by the Authority:

The most significant part the notifications is about wrong deliveries due to misaddressing or e-mails sent to wrong addressees. In such cases, the data controller must do all it can to have the wrong addressee destroy/delete the document or message containing personal data in his or her possession. Where a postal letter is concerned, the data controller may send the wrong addressee a self-addressed envelope requesting him or her to send the letter back. The data controller must also ensure that the right addressee receives the message, and, if it deems the risk likely to be high due to the nature of the personal data concerned, it must inform the data subject of the data breach. It is convenient to send of copy of this information to the Authority. Similar conduct is expected of the data controller

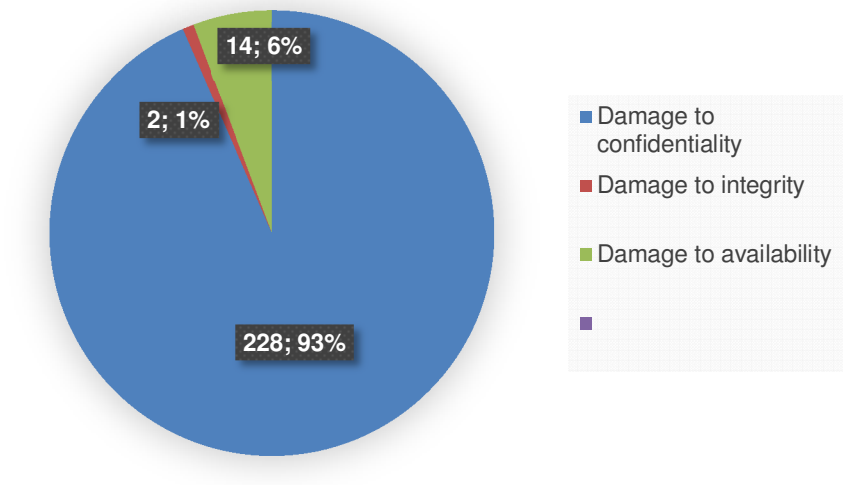
when an addressee mistakenly receives, apart from the message he or she is meant to receive, an annex containing personal data by postal or electronic mail.
E-mails sent to several addressees, where the addressees are listed not in the 'Blind copy' but the 'Copy' field, and thus the addressees see, have unauthorized access to, each other's e-mail addresses. In order to mitigate the risk to the personal data, the data controller is expected to contact the addressees requesting them to erase the message.
Data leakage due to hacking the data controller. In such as case it is important to identify as soon as possible the scope of data concerned and to review the security of the IT system. If, in the lack of expertise, the data controller does not manage to identify the process of the hacking and the details leading to the breach, it is worth seeking an external expert. If the hacking occurred due to taking advantage of human factors (e.g. phishing), the process of prevention must include the training of employees. If the vulnerability was a result of IT defects, a review of the entire system is justified. In all cases, a review of the IT security rules of the data controller is justified.
IT devices, telephones stolen/lost. In such cases, it is a priority to see whether the data controller took appropriate measures to protect its equipment (passwords, encryption), whereby unauthorized persons can be prevented from accessing the data on the devices. In the case of remote access availability, data might be erased afterwards. It is important that, having become aware of the data breach, the data controller should immediately identify what data and servers the client accessed and what entitlements were assigned to him, which should be immediately revoked, the servers and services withdrawn, and their accessibility changed.
It can be generally stated that, after a personal data breach and the assessment of deficiencies revealed, the data controller should review internal procedures, include further filters and controls into the work process, and raise the data protection awareness of employees.

II.2.6 Personal Data Breaches Related to Cross-border Data Processing

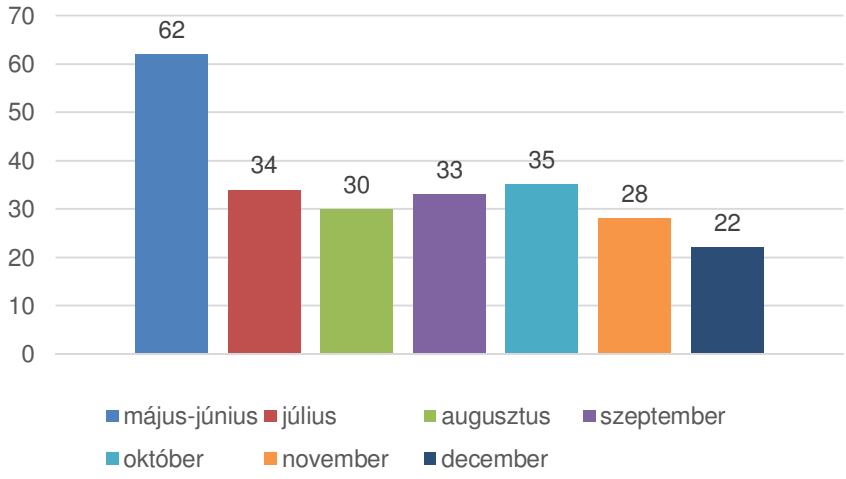
Pursuant to Article 56 of the GDPR, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure ('the one-stop-shop mechanism') provided in Article 60.
The procedure of the Authority data breaches related to cross-border data processing therefore depends on whether the data controller or processor has a main establishment in Hungary or not.
An example of cross-border data processing is the personal data breach at Marriott Hotels Limited, where unauthorized persons had access to the database of one of its subsidiaries, Starwood Hotels, since 2014. As the breach concerned a cross-border data processing and the main establishment of the company was in the United Kingdom, London, the data protection authority of the UK, the Information Commissioner's Office (ICO) initiated a procedure under Article 56 of the GDPR to determine the lead supervisory authority and the supervisory authority concerned on 30 November 2018.
The ICO regards itself as the lead supervisory authority in the case, with which the Authority (along with the other supervisory authorities concerned) agreed, and indicated to the ICO that it regards itself concerned in view of the fact that the data processing affects or is likely to substantially affect data subjects residing in Hungary.

In practice this means that ICO is the single contact point of the data controller in the cross-border data processing it carries out, and conducts the inquiry into the data breach, but the authorities concerned—including the Hungarian National Authority for Data Protection and Freedom of Information—may deliver their opinion on, comment on, and express objections to on the draft decision in the case.
In contrast, the main establishment of the data controller in a data breach case concerning cross-border data processing has its main establishment in Hungary, and, in such cases, it is the Authority that acts as the lead supervisory authority; in a procedure under Article 56 of the GDPR, it identifies the supervisory authorities which may deliver their opinion on the draft decision the Authority prepares.

Nature of data breaches

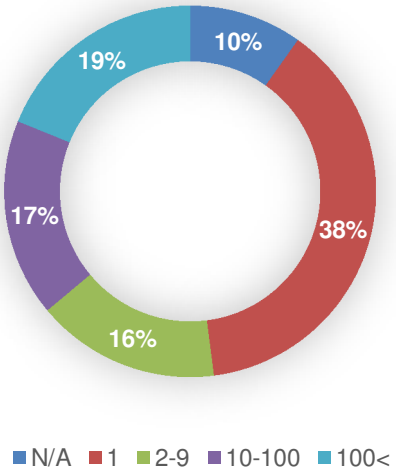


Monthly distribution of data breaches



May-June, July, August, September, October, November, December

Distribution of data breaches as per data subjects



II.2.7 Personal Data Breaches before GDPR's Coming into Force

The Authority received several notifications about the online ticketing system operated by the Budapesti Közlekedési Központ (Centre for Budapest Transport; hereinafter: 'the BKK'). Notifiers objected that BKK's online ticketing system did not meet the data security requirements under Section 7 of the Privacy Act, and, moreover, several complainants objected also that it was likely according to press reports[13] that the personal data submitted during registration was accessed by unauthorized third parties.

On the basis of the complaints, the Authority commenced an inquiry, and, substantiating the infringements of law considered likely by the complaints, initiated an authority procedure for data protection on 31 July 2017. The subject of the authority procedure for data protection was the data processing related to online ticketing, particularly data security requirements and the provision of prior information to the data subjects.

With regard to the provision of prior information, the Authority found that the data processing notice provided to the data subjects by the BKK did not contain all the facts and circumstances of data processing, and that, in certain points, included information that did not correspond to reality. The notice had abstract formulations which could not be understood and grasped by the general user. The BKK therefore failed to provide the data subjects with appropriate information infringing Section 20 (1)–(2) of the Privacy Act. The Authority thus required the BKK to modify its data provision practice so as to meet the requirements of the Privacy Act, and to provide appropriate information to the data subjects in the future.

The news website 24.hu sent to the Authority the documents (simultaneously deleting the copy it processed) it deemed to prove that the personal data of registered users collected

[13] http://index.hu/tech/2017/07/14/ez_nektek_e-jegy_kedves_bkk/;
http://index.hu/tech/2017/07/14/meghekkelheto_a_bkk_rendszere_barmennyiert_lehet_jegyet_venni/;
http://index.hu/tech/2017/07/14/meghekkelheto_a_bkk_rendszere_barmennyiert_lehet_jegyet_venni/;
http://index.hu/tech/2017/07/15/barki_feltorheti_a_bkk_elektromos_jegyvasarlo_rendszeret/;
http://index.hu/tech/helpdeszka/2017/07/17/bkk_e-jegyet_vett_azonnal_valtoztasson_jelszot/;
http://index.hu/belfold/budapest/2017/07/18/bkk_digitalis_berlet/;
http://index.hu/tech/2017/07/21/a_bkk_webshopja_biztonsagos/;
http://index.hu/tech/2017/07/21/barki_torolheti_a_bkk_rendszerebol_a_nevrokonainak_fiokjat/;
http://24.hu/tech/2017/07/25/regisztralt-a-bkk-e-jegy-rendszereben-hozzaferhettek-az-adataihoz/.

from the database of the online ticketing system operated by the BKK might have accessed by unauthorized persons. In the course of clarifying the facts of the case, the Authority found that the database it received was identical with the database processed in connection with the online ticketing system of the BKK, data security was thus damaged, as a result of which unauthorized access to the data processed by the BKK and thereby a personal data breach under Section 3 (26) of the Privacy Act did occur.

In the course of the procedure, the Authority also examined whether the BKK complied with the data security requirements provided for by Section 7 of the Privacy Act, and, in this respect, found the following:

- While designing the data processing, the BKK had failed to take the technical and organizational measures and to set out the procedural rules that serve the security of the data, particularly the prevention of unauthorized access to, modification, transfer, publication, destruction or erasure, as well as unintentional destruction or erasure, of the personal data. The absence of such measures is also proven by the fact that the BKK was unable to establish that personal data breaches had occurred in relation to the data processing it carried out, and the circumstances thereof, particularly its effects on the data subjects. With regard to the data security measures, the BKK should have ensured that it could establish the procedure applicable in the event of a personal data breach, which, according to the declarations it made and the documents it submitted, it failed to do.
- In the contract with the data processor, the BKK had failed to specify data processing issues, including data security prescriptions and requirements. After the conclusion of the contract, it had failed to give instructions to the data processor on data security measures.
- The BKK had generally failed to establish an internal procedure, rules, for personal data breaches, whereby an eventual breach could be explored and handled. In addition, the BKK had failed to do everything in its power in order to investigate the circumstances and the severity of the particular personal data breach and its impact on the data subjects and to take the necessary data security measures. It reduced risks by terminating the online ticketing system, but failed to inform the data subjects about the personal data breach, and especially about its possible consequences, thereby infringing their right of informational self-determination.

Based on the above, the Authority imposed a data protection fine of HUF 10 million on the BKK, and ordered it to take the necessary measures with regard to the violation of the data security requirements in order to reveal the circumstances and probable risks of the personal data breach, and to inform users registered before 24 July 2017 thereof. It also required that the company ensure the proper fulfilment of the data security requirements and, an in the framework of this, to establish the internal procedure for personal data breaches and to give appropriate instructions thereof to the data processor commissioned including them in writing the contract concluded for the technical processing of the data.

On 4 July 2018, the Budapest-Capital Regional Court of Appeal dismissed the action brought by the BKK for the judicial review of the decision of the Authority. The BKK appealed this ruling at the Curia, the proceedings of which were still underway while writing this report.

II.2.8 Authorization Procedures

Under the GDPR, the scope of duties of the Authority were broadened by the powers of authorization set forth in Article 58 (3), the detailed rules of which are provided for by national laws. In this regard, the Privacy Act as amended by the Amendment Act is applicable, Sections 64/A–64/C of which provides that the authorization procedure for data processing shall be conducted within the exercise of such powers.

A procedure for the authorization of data processing shall be conducted in the following groups of cases:

Approval of a code of conduct and the activity of a body monitoring compliance with a code of conduct;

Approval of the criteria of certification;

Authorization procedures for transfer of personal data to third countries.

II.2.8.1 Approval of a code of conduct and the activity of a body monitoring compliance with a code of conduct

1. *Codes of Conduct*

Under Section 64/A (1) a) of the Privacy Act, the Authority shall conduct a procedure for the authorisation of data processing if application for the approval of the draft, extension or amendment of the codes of conduct pursuant to the GDPR is submitted.

Associations or other bodies representing categories of controllers or processors may draw up codes of conduct so as to facilitate the effective application of the GDPR. A code of conduct as designated by the GDPR is a means the free application which assists the data controller in ensuring compliance with the GDPR. The GDPR provides a list examples of the issues where a code of conduct may specify the application of the GDPR. Beyond those defined by the Administrative Procedure Act, the application shall include the draft code, or its draft amendment or extension.

The following substantive elements must be included in the code or the application:

- A code should focus on the questions of the data processing of a specific sector or group of activities, and offer data controllers and processors solutions to these questions. In the procedure for approval, the applicant must demonstrate that the code of conduct represents sufficient added value.
- The applicant must present the characteristic questions and problems of the sector it represents that justify the drawing up of a code of conduct.
- As a preliminary question, the applicant must assure the supervisory authority that it is ‘mandated’ to draw up a code; that it, is an organization appropriate for setting out distinct rules concerning the given sector, and to establish effective means to ensure enforcement.
- It should be clear from the code what material and territorial scope it has; that is, the code should define the data processing activities and data controllers subject to the code, and what Member States it is to be applicable in.
- The application and the draft code appended should demonstrate the mechanism the code establishes to enable the body monitoring compliance with the code to monitor whether the data controllers and processors that agreed to apply the code comply with the code, and to enforce it.
- If the code is to apply to data processing activity concerning several Member States, the applicant must justify the competence of the Authority. In this, it may consider the following: the place of the most frequent occurrence of the sector or data processing activity, and the seat of the applicant association or the suggested monitoring body.

In drawing up the draft, the guidelines to be adopted by the European Data Protection Body should be taken into account, which, following its finalization, the Authority shall publish on its website.
Pursuant to Article 40 (5) of the GDPR, the Authority shall provide an opinion on whether the draft code complies with the GDPR, and shall approve that draft code by way of an authorization procedure for data processing.
It may happen that the code relates to processing activities in several Member States; in this event, the supervisory authority shall submit it to the European Data Protection Board pursuant to the consistency mechanism. In such cases, the Board shall also provide an opinion on whether the draft code complies with the GDPR. If the Board finds that the draft is appropriate, it shall submit it to the Commission, which may, by way of implementing acts, decide that the approved code of conduct submitted to it has general validity within the Union.
It is among the duties of the supervisory authority to maintain a record of and publish the approved codes of conduct if the code does not relate to processing activities in several Member States. If a code has general application by a decision of the Commission, its publication shall be the duty of the Commission, too. Furthermore, the European Data Protection Board shall collate all approved codes of conduct in a register and shall make them publicly available by way of appropriate means.

2. *Approval of a body monitoring compliance with a code of conduct*

Codes of conduct must establish mechanisms enabling the bodies accredited to monitor compliance with the provisions of the code by the data controller and processors that have undertaken to apply it. Under Article 41 (1) and (6) of the GDPR, 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. This provision shall not apply to processing carried out by public authorities and bodies.
Under Section 64/A (1) b) of the Privacy Act, the Authority shall conduct a procedure for the authorisation of data processing if an application for the authorisation of the activity monitoring compliance with a code of conduct.
In accordance with Article 41 (2) of the GDPR, a body may be accredited to monitor compliance with a code of conduct where that body has:

- demonstrated its independence and expertise in relation to the subject-matter of the code to the satisfaction of the competent supervisory authority;
- established procedures which allow it to assess the eligibility of controllers and processors concerned to apply the code, to monitor their compliance with its provisions and to periodically review its operation;
- established procedures and structures to handle complaints about infringements of the code or the manner in which the code has been, or is being, implemented by a controller or processor, and to make those procedures and structures transparent to data subjects and the public; and
- demonstrated to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interests.

Under the GDPR, the Authority shall publish the criteria of accrediting monitoring bodies, which will take place after the European Data Protection Body has provided its opinion pursuant to the consistency mechanism.

Applications for the authorization of such activities shall include proof of how the body fulfils the conditions set forth in Article 41 (2) of the GDPR and the authorization criteria published by the NAIH.

II.2.8.2 *Approval of the criteria of certification*

Certification is a means established by the GDPR and voluntarily applied by data controllers and processors, which can be used for certifying that the data controller fulfils its obligations under the GDPR.

Certification is a compliance assessment under set requirements, the criteria of certification, carried out and verified by a third person. The requirements arise from standards and laws; in the case of data protection certification, the GDPR is the normative system of rules on which the assessment of the requirements is based. In order that the certification meets its purposes, the requirements of the GDPR need to be specified in the criteria of certification and the mechanism of certification and for the object of the certification. The result of a successful certification is the certificate, a seal or mark, which verifies that the given organization met substantive and procedural requirements of the certification mechanism. Further information on certification can be found in Guidelines 1/2018 on certification and identifying certification adopted by the European Data Protection Board (https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying-certification_en).

In the opinion of the European Data Protection Board, the object of certification under the GDPR may be a processing operation or processing operations as a whole. This may mean processes of direction, which may be regarded as organizational measures, and thereby form an organic part of a data processing operation.

A certificate can only be issued by an accredited certification body or competent supervisory authority. If a certification body wishes to issue a certificate, it can do so under the certification criteria or certification mechanism approved of by the competent supervisory authority. It is therefore a precondition of the approval of a certification body that the criteria and mechanism of certification has been approved of by the Authority in the framework of an authorization procedures for data processing.

Under Section 64/A (1) c) of the Privacy Act, the Authority shall conduct a procedure for the authorisation of data processing if an application for the authorisation of the criteria of certification is submitted. Beyond those defined by the Administrative Procedure Act, the application shall include the general description of certification mechanism and a draft of the criteria of certification. The Authority shall publish the minimum requirements of the criteria and mechanism of certification following the finalization of the guidelines of the European Data Protection Board.

II.2.8.3 Authorization Procedures for Transfer of Personal Data to Third Countries

Pursuant to the provisions of the GDPR, there are means that provide for appropriate safeguards in the transfer of personal data to third countries when they authorized by the competent supervisory authority.

A data transfer does not require special authorization by the competent supervisory authority, but the means it is based on shall be authorized by the competent supervisory authority:

1. binding corporate rules (BCR);
2. code of conduct;
3. certification.

Subject to the authorization from the competent supervisory authority, the appropriate safeguards may be the following:

1. contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country; or
2. provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

1. Approval of Binding Corporate Rules

Should a group of undertakings, or a group of enterprises engaged in a joint economic activity (hereinafter: 'Group' or 'Applicant') wish to draw up Binding Corporate Rules, it must take into account the mandatory substantive elements provided for by Article 47 of the GDPR, as well as the guidelines and working documents by the European Data Protection Board.[14] It is the existence of these substantive elements that the competent supervisory authority, the supervisory authorities concerned, and the Board assess.

The GDPR provides that the competent supervisory authority shall approve binding corporate rules in accordance with the consistency mechanism, thus providing consistency throughout the Union. If a competent supervisory authority thus conducts an authorization procedure for the approval of BCR, it shall submit its draft decision and all relevant information—including the opinions of the supervisory authorities concerned—to the European Data Protection Board, which shall issue its opinion thereof subsequently.

The GDPR does not provide for a detailed procedure of drawing up the draft decision to be submitted to the Board, that is coordination between the supervisory authorities concerned on the appropriateness of BCR. Nor does the GDPR set down how to determine the authority 'competent' with regard to BCR under Article 47 thereof, that is, which supervisory authority the approval of specific BCR should be initiated with.

To redress the above, the European Data Protection Board adopted Working Document WP 263 rev. 01,[15] setting forth the basis of a reviewed cooperation procedure for the approval of BCR. It defines, on the one hand, how to identify the supervisory authority that can be regarded as 'competent' with regard to the specific BCR, that is act as Lead Authority, and, on the other, how cooperation is to proceed between the supervisory authorities of the Member States prior to the approval of BCR in order to analyse and asses their content.

2. *Approval of Contractual Clauses between the Controller or Processor and the Controller, Processor or the Recipient of the Personal Data in the Third Country*

Data transfer to third countries may also be carried out when the data controller or processor has notified the competent supervisory authority about the appropriate safeguards, and ensures them by way of contractual clauses concluded with the controller, processor or the recipient of the personal data in the third country. The supervisory authority of the Member State from where the data are transferred shall be 'competent' to approve of such contractual clauses.

The European Data Protection Board has not yet issued any guidelines with respect to such contractual clauses; further information shall be available subsequently.

3. *The Approval of Provisions to be Inserted into Administrative Arrangements Between Public Authorities or Bodies Which Include Enforceable and Effective Data Subject Rights*

[14] See WP 256 rev.01, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules (https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614109)
[15] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623056

Data transfer to third countries may also be carried out when the appropriate safeguards are ensured by provisions to be inserted into administrative arrangements between public authorities or bodies which are approved of by the competent supervisory authority. Such provisions must include enforceable and effective data subject rights. The supervisory authority of the Member State from where the data are transferred shall be 'competent' to approve of such provisions.
This is therefore a means public authorities or bodies may apply for transferring personal data to the public authorities or bodies of third countries when any of them lack the opportunity or powers to ensure safeguards in any other way (e.g. it cannot enter into a legally binding agreement). This shall not be a means for establishing appropriate safeguards for data transfer between public authorities or bodies and private-law organs.

II.3 Data Protection Certification

Following the entry into force of the GDPR, the Authority no longer has the opportunity of providing data-protection audit services. The Amendment Act however, taking into account Article 42 (5) of the GDPR, set down the fundamental provisions for conducting a certification procedure on the initiative of the data controller or processor, which provisions—due to the similarity of the two legal institutions—the Hungarian legislator laid down in the place of the former rules pertaining to the data-protection audit in the Privacy Act, with a similar content.
For all the similarities, the data-protection certification however is closer to the activity of assessing and certifying compliance with standards, and, in this respect, differs from the data-protection audit, which can be interpreted as a means of general supervision. The data-protection audit sought to survey compliance with legal requirements by way of assessing the data processing activities carried out or planned by the data controller on the basis of criteria defined and published by the Authority and to shape the expectations and safeguards effective during the examination, while the data controller had the opportunity of defining the aim and scope of the audit. During data-protection certification however, the data controller's duty is to demonstrate in a documented way compliance with the system of criteria defined and published by the Authority, which can be attained in a much narrower circle of data-protection operations.
In data-protection certification, the Authority examines only the data processing practice that the data controller designates in its application and that falls within the certification scope of the Authority; it is in this framework that the Authority assesses compliance with the principles of data protection, the fulfilment of the obligations of the data controller concerning data subject rights, its documented internal and external procedures, rules, notices, risk assessment and risk management activities, and its fulfilment of obligations concerning its possible technical data processing and data transfer activities. In publishing a seal for individual data processing, the Authority may certify compliance only with pre-set requirements; the new legal institution lacks consultation activity assisting compliance, preparation in a broad sense. Besides this, Article 42 (4) of the GDPR states that certification does not reduce the responsibility of the controller or the processor for compliance with data protection requirements and is without prejudice to the tasks and powers of the competent supervisory authorities; that is, certification may affect neither the assessment of a data subject complaint regarding the data processing operation that is its object, or already has a seal, nor the commencement of the procedure.

Certification and the issuing of a seal by the Authority must be distinguished from both the authorization procedure for data processing (see above) under Section 64/A c) of the Privacy Act and the procedure for the accreditation of certification bodies by the National Accreditation Authority, in which the NAIH participates as a specialist authority.
Furthermore, the certification activity of the Authority under Section 69 of the Privacy Act, in contrast to the authorization procedure, is subject neither to Hungarian accreditation provisions nor the requirements of the standard ISO/IEC 17065/2012 in view of the fact that its authorization for preparing certification mechanisms rests directly on the GDPR. Such certification activity was carried out by several data protection authorities in the Member States of the Union previously (see e.g. the certification mechanism for digital safe boxes, data-protection training and data-protection audits published by the French data protection authority (CNIL) on 13 January 2015).
Within the organization of the Authority, duties related to certification are fulfilled by Data Protection Certification Department of the President's Cabinet established for this purpose, the staff members of which have competencies both in information-security and data-protection law.
The detailed rules of the certification mechanism, criteria system and the resulting data-protection seal issued to the initiator of the Authority are currently being drafted in order that a flexible and high-standard certification mechanism meeting the requirements of Articles 42 and 43 of the GDPR and the related Guidelines nos. 1/2018[16] and 4/2018[17] of the European Data Protection Board will be available for data controllers and processors.
The definition of the circle of certification products by the Authority will take place subsequently, following the publication of the finalized version of the Guidelines of the European Data Protection Board and taking into account the certification practices of the supervisory authorities of other Member States.

III. Procedures Related to Data Processing for Criminal Investigation, National Defence, and National Security Purposes

The discussion of the three data processing purposes mentioned in the subtitle and the related data processing activities in separate chapter is justified by the fact these are not subject to the rules of the GDPR, and continue to remain within the scope of national legislation; that is, the fundamental rules of the protection of personal data shall continue to be defined by the Privacy Act even after the coming into force of the Amendment Act. Both the GDPR and the Privacy Act aim to achieve a high standard of the protection of personal data, and the principles and legal institutions they provide for have many similarities, but the themes falling within the scope of the Privacy Act are connected to fundamental state interests that cannot be regulated fully in parallel with the GDPR (focussing as it does on the data-protection regulation needs of market, company, and transnational data processing). Accordingly, e.g. mandatory data processing has a greater role among possible legal bases of data processing in the themes regulated by the Privacy Act, but it can also be mentioned that different conditions apply to the limitation of data subject rights than in data processing the data-protection framework of which is defined by the GDPR.

[16] Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679 - version for public consultation.
[17] Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679).

Date-protection experience worth reporting on arose in all three subjects as well as in the data-protection control of international and European data transfers for criminal investigation purposes; these are what are outlined in what follows.

III.1 Procedures Related to Data Processing for Criminal Investigation Purposed

III.1.1 The Control of Social Media Profiles and Cloud Services in Criminal Proceedings

A citizen turned to the Authority because, following the police seizing IT and telecommunications equipment from him and his close relatives, they found that someone had entered their own Facebook and Gmail accounts and other applications, and requested new passwords for them. When the equipment was returned to them following the forensic expert's inquiry, they found that SMS messages and other data had been downloaded from them, and a Gmail account had also been installed on it, which could be attributed to the forensic expert. In the course of the inquiry, the Authority contacted the expert and the appointer, the police. In the inquiry, no data arose that could lead to the conclusion that the forensic expert had exceeded the framework of his appointment and had processed the personal data of the complainants beyond what was necessary for his expert activity.

III.1.2 Camera Recordings of Police Action

The Commissioner for Fundamental Rights requested the opinion of the Authority on a matter he was examining, because the facts of the case he had established concerned several fundamental rights, including fundamental information rights. Essentially, the question was whether the likeness, the personal data, of a policeman may be processed or not as he apprehends a wanted person, who makes camera recordings with his mobile phone of the action against him and the police acting.

Having examined the known circumstances of the case, the Authority found that two sets of interest conflict in such a case: first, the interest in the effectiveness of lawful action, itself serving the preservation of democratic control, and, second, the interest of controlling the operation of public authorities, the precondition of which is that information is available for citizens, on the basis of which well-grounded opinions can be reached as to whether a public authority, in this case, the police, fulfilled its duties pursuant to the rule of law and effective laws.

A policeman acting qualifies as a person exercising public authority tasks and powers, and thus the personal data related to his performing duties within the scope of data defined by the Privacy Act shall be regarded as data accessible on public interest grounds. Data accessible on public interest grounds may be disseminated respecting the principle of purpose limitation in data processing. The constitutional framework of exercising the right to disseminate data was discussed by the Constitutional Court in several of its rulings. It should be noted however that the likenesses of police shall not be data accessible on public interest grounds under the Privacy Act.

The precondition of exercising the right disseminate data is access to, or coming into possession of, the data (the copy of the data) publishable or disseminatable. Typically, access to data of public interest and data accessible on public interest grounds takes place through a data access request and provision of information or document copy by the organ or person requested, though this is not the only way of exercising the right of access to data. Usually, no image recordings are made of police actions by the police; that is, there is no way of accessing data by subsequent request, and thus other ways of exercising citizens' rights that are not expressly prohibited by law should be regarded as acceptable. In the opinion of the Authority, if a person acted against makes image recordings of the action, this belongs in this category. However, this mode of exercising may not obstruct the execution of lawful

action. At the same time, the police shall refrain from obstructing the documentation of the action through camera recording by referring to specious arguments. As the likenesses of police are not data accessible on public interest grounds, the camera recording may not be published, but may be used in a procedure reviewing the lawfulness of the police action.

III.1.3 The Recording of the Personal Identification Data of the Accused and the Injured in Requests by Investigation Authorities

The notifier turning to the Authority, the head of a firm, objected to the fact that his firm had received several data access requests form the police, the public prosecutor, and occasionally the courts, that contained several personal data of persons involved in criminal proceedings (the accused and injured parties) among the identifiers of proceedings. The personal data provided in the requests was not necessary for fulfilling the requests.

The Authority is aware of similar practices from other sources as well, such as e.g. an investigative authority needlessly recorded in a request the personal data of minors who were victims of sexual crime among the identifiers of the criminal case. In the opinion of the Authority, the data processing practice described is not in accordance with the principle of purpose limitation in the processing of personal data. Furthermore, the needless disclosure of data might add to the grievance and suffering of the victims of criminal acts. But the needless transfer of data is unacceptable not only in the case of the injured but also the accused, as the presumption of innocence is the due of the accused, and the protection of data extends to the personal data of the accused.

On the basis of the notification, the Authority, requesting the Ministries of the Interior and Justice, initiated the termination of the practice.

III.1.4 Possible Leaks of Data Processed by the Police

A notifier turned to the Authority because he received information from acquaintances from which it could be inferred that persons knew about his being fined for fast driving who could not lawfully know about the case. In the course of the inquiry, the Authority contacted the organs concerned, but no data surfaced that would prove an abuse of the data of the notifier by the police, and the Authority therefore concluded the inquiry. It should be noted in this respect that the Privacy Act affords a broad range of examination rights to the Authority for establishing the facts of data processing cases, but the Authority has no investigative powers.

III.2 Procedures Related to Data Processing for National Defence Purposes

In the autumn of 2018, contradictory press reports came out that member of parliament Márta Demeter published data concerning the persons flying in relation to an air carrying task of the Hungarian Army, and thus the Authority ex officio attempted to establish the facts of the case. It was stated at the on-site inspection held by the Authority at the Szentgyörgyi Dezső Air Base HA 59 that the member of parliament was provided information as required by law on the processing of the documents presented to her and their ‘non-public’ nature. The Authority found that Márta Demeter could not have accessed the information she presented as fact in her interpellation on 16 October 2018 from the documents she had been shown in the course of the document inspection. The documents that could be associated with her questions did not contain the personal data referring to the daughter of the prime minister that were published. The documents did not include any information on the natural person (the daughter of the prime minister) named in the question the MP published, excepting an identity of names. On the basis of the inquiry, the Authority found that member of parliament Márta Demeter published personal data on the

daughter of the prime minister in the National Assembly, in an open question requiring an answer in writing.

III.3 Procedures Related to Data Processing for National Security Purposes

III.3.1 Direct Access to Data by the National Security Services

Act CXXV of 1995 on the National Security Services (hereinafter: 'National Security Services Act') enables the national security services to request data by way of direct access from public organs, majority state-owned enterprises, and financial institutions defined in the Act on Credit Institutions and Financial Enterprises. Furthermore, the Counterterrorism and Crime Analysis Centre, in line with the special laws applicable to it, is entitled to maintain online contacts with cooperating organs and to established data connections ensuring direct data access.

With respect to data requests involving direct data access, there are several, both technical and legal issues that need to be resolved. IT systems ensuring direct data access, work organizations operating them, internal rules, etc. need to be made available at both the national security services and the organizations obligated to provide data. The National Security Services Act provides for specific rules on e.g. setting up electronic interfaces and the documentation of data provisions. The rules of the Act on direct data access have been in effect for several years, but, in our knowledge, the initial steps for creating the IT systems took place in 2018, following a survey of needs and opportunities.

The Hungarian Banking Association initiated multilateral negotiations to clarify the issue arising from the provision of data through direct data connection, at which top-level representatives of, apart from the Banking Association, the National Bank, and the commercial credit institutes, the Authority, the Ministries of Interior and Justice, and the National Security Special Service (hereinafter: 'the NSSS') participated. According to the conclusions of the meeting, the conditions of the legal regulation for establishing direct data connection between the NSSS and the credit institutions are in place. The participants requested the Authority to assess whether the pilot system set up to provide direct data access between the NSSS and a credit institution accords with the rules of the protection of personal data, with special regard to the obligation of credit institutions in protecting banking secrecy and confidentiality. On the basis of the request, the Authority examined the operation of the pilot system on several occasions at the NSSS and the credit institution participating in the development. The development of the pilot system, including, apart from the IT system, the work organization, the workflow at the credit institution, and the drawing up of internal rules, etc., is still in progress. The Authority follows the progress of the works, and assists it with comments and suggestions to ensure the protection of personal data.

III. 3.2 The Regulation of Using Concealed Equipment

Gathering Intelligence enables a drastic restriction of the right to the respect of the protection of personal data and privacy and residence (the singular site of privacy), and, moreover, in a way that, because of the secrecy of the intervention, the individual has little chance in practice to enforce his or her rights regarding data processing or seek legal redress for any possible infringement of law, and thus the regulation of gathering intelligence and its actual practice is always among the top priorities of the Hungarian data protection authority. In 2018 the new regulation of the field in the system of the new rules of criminal procedure brought about major changes. Enough time has not passed to be able to assess the effects of the new law material in detail and context. It is a welcome change in terms of the protection of personal data that the new provisions of law of concealed equipment define the nature of individual means and methods more precisely than the previous regulation. The regulation

of the area has fortuitously gone beyond the limits of criminal procedure, as, alongside the drawing up of the new rules, the correction of gathering intelligence for national security purposes also took place. The designation of the means and methods of gathering intelligence now includes the so-called equipment actions necessary for gathering intelligence (e.g. placing technical equipment and electronic data for the control of IT systems), when the lawfulness of their application was not obvious in the lack of legal regulation.

III.3.3 The Right of the Data Subject undergoing National Security Screening Procedure to be Informed

A data subject submitted a complaint to the Authority claiming that his request to be informed about the status of his national security screening was not fulfilled by the initiating organ (Office for Defence Economy, Ministry of Defence). According to the facts of the case established by the Authority, the organ initiating the national security screening of the data subject ceased to exist with succession, the director of the national security service therefore did not order the national security screening within the deadline provided for by the law, but, instead, contacted the successor of the organ that had initiated the screening asking whether, in view of the organizational changes, the continuation of the screening of the data subject was necessary or not. The successor of the initiating organ failed to provide a clear answer, and thus the national security screening was not ordered again. In the meanwhile, the data subject was in the awareness that he was undergoing national security screening, though the legal relationship in respect of which his national security screening had been initiated was called into question.

During the inquiry, the Authority found the following:

As part of the right to informational self-determination, everyone has the right to know who is using his or her personal data at what time and for what purpose. The exercise of this right may only be limited under the provisions of the Privacy Act. According to Section 15 (1) of the Privacy Act, as effective before the Amendment Act, the right of the data subject to be informed included being provided with information on the fact of data processing. The successor of the organ initiating the procedure was in the knowledge of the fact that whether the national security screening of the data subject was taking place or not, and was therefore subject to the data controller's obligation—including the provision of information to the data subject as prescribed by the Privacy Act—concerning the information on the data subject in its possession in spite of the fact that the national security screening was conducted no by the organ initiating it. The Authority found that the data subject's claim to being provided information concerning the status of the procedure involving the processing of his personal data should be assessed under the rules pertaining to his right to be informed pursuant to the Privacy Act.

The Authority requested the successor of the organ initiating the national security screening to answer requests for information that can be associated with the personal data of the requester, and the answering of which enable the data subject to follow the path of using his personal data, in accordance with the provisions of the Privacy Act. The right of the data subject to be informed may only be limited insofar as the protection of classified information and national security interest so require it. In its response to the requirement of the Authority, the successor of the organ initiating the screening stated that it would continue its data processing practice taking into account the findings and requirement of the Authority.

The authority examined the procedure of the Military National Security Service (hereinafter: 'the MNSS') conducting the national security screening. In the course of this, it did not find it objectionable that data controller decided, for prudential purposes, to seek affirmation from the successor of the organ initiating the screening on upholding the initiation instead ordering the screening (though the National Security Services Act does not allow for the deferment of starting a screening for such reason), because this was the only way to exclude the possibility of conducting a procedure needlessly, which in the end did prove to be needless. This measure accorded with the principle of data minimisation. Simultaneously, the deferment of ordering the national security screening for the reason mentioned infringed the enforcement of the right of the data subject to be informed due to exceeding the time limits of lawful data processing, because deviation from the time limits under law made the fact of data processing and the execution of the screening seem uncertain for the data subject. The Authority therefore requested the organ responsible for conducting a national security screening to inform the data subject of the actual time of starting the national security screening in order to avoid infringing the right of informational self-determination if starting the procedure is deferred for some reason in the future.

III.3.4 The Processing of Data Generated during the Review of the National Security Screening of a Member of Parliament

The deputy director-general of the Office of the National Assembly requested the opinion of the Authority whether the fact that a review procedure of the national security screening of a member of parliament found a factor of risk to national security or not was data accessible on public interest grounds or not.

According to the Authority, the national security service, within the scope of its duties and powers as defined in the National Security Services Act, conducts the review procedure, and performs data processing for national security purposes subject to the data-protection rules of the Privacy Act and the National Security Services Act, but the data controller of the document containing the results of the screening and submitted to the Speaker of the National Assembly is not the national security service but the Speaker of the National Assembly, and thus the data processing he carries out (presenting the report to a committee of the National Assembly or possibly publishing some of the data in the document) does not qualify as data processing for national security purposes subject to the Privacy Act, but falls within the scope of the GDPR. Under Article 6 (1) c) and e) of the GDPR, data processing shall be lawful if it is necessary for compliance with a legal obligation to which the controller is subject, or it 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. Pursuant to Article 6 (2), Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX. In the Hungarian jurisdiction, it is Sections 19 (1) and (7)–(10) and 72/B (8) of the National Security Services Act that provides for the tasks carried out in the exercise of official authority, for the performance of which the data on the factors of risk in the report on the national security screening or its review may be used in accordance with the laws cited. (In the case of classified data, the laws on classification shall also apply.) Under Article 8 (1) and (2) of the GDPR, Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the

purposes of academic, artistic or literary expression. For processing carried out for journalistic purposes or the purpose of academic artistic or literary expression, Member States shall provide for exemptions or derogations […] if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information. In accordance with Article 86 of the GDPR, personal data in official documents held by a public authority or a public body or a private body for the performance of a task carried out in the public interest may be disclosed by the authority or body in accordance with Union or Member State law to which the public authority or body is subject in order to reconcile public access to official documents with the right to the protection of personal data pursuant to this Regulation.

In the opinion of the Authority, the cited articles of the GDPR are corresponded to by Section 3 (6) of the Privacy Act, according to which data accessible on public interest grounds means any data, other than data of public interest, the disclosure, availability or accessibility of which is prescribed by an Act for the benefit of the general public. Under Section 26 (2) of the Privacy Act, the name of the person acting within the functions and powers of the organ performing public duties, as well as his functions and duties, executive mandate, his other personal data relevant to performing public duties, and his personal data to which access is ensured by an Act, shall qualify as data accessible on public interest grounds. As far as data on the existence of or immunity from a national security risk is concerned, this data is undoubtedly relevant to a member of parliament performing his public duties and is accessible on public interest grounds insofar as he is subject to national security screening under the National Security Services Act.

III.4 Participation in the Joint Supervisory Activity of Data-protection Authorities

III.4.1 Annual Review of the Privacy Shield

A staff member of the NAIH participated in the second annual review of the data protection agreement (the Privacy Shield Agreement) concluded between the European Union and the Unites State of America on 12 July 2016. The Union examination group consisting of members of the European Commission and the delegated experts of the European Data Protection Board and the delegation of the United States met in Brussels in October 2018 to discuss developments following the first annual review and issues related to the obligations under the Framework.

In the course of the review the parties discussed issues of certification and re-certification, compliance, complaint handling, and the raising of consumer awareness in connection with data processing for business and commercial purposes. With regard to data processing for national security and law enforcement purposes, the parties discussed the possibilities of legal redress and the ombudsperson procedures established for investigating data protection complaints for EU Citizens.

The Commission and the European Data Protection Board drew up a report on the results of the second annual review of the framework. In its report, the Board emphasized the importance of the framework, but also noted that, without appointing a permanent ombudsperson, effective remedy for EU Citizens cannot be guaranteed.

III.4.2 Borders, Travel and Law Enforcement Expert Group – BTLE

The group prepared an opinion on the proposal package on access to electronic evidence. The objective of the new rules is to make it easier and faster for police and judicial authorities to obtain the electronic evidence, such as e-mails or documents located on the cloud, they need to investigate, prosecute and convict criminals and terrorists. The new rules will allow law enforcement in EU Member States to better track down leads online and

across borders, while providing sufficient safeguards for the rights and freedoms of all concerned.
The proposal consists of two parts, a European Production Order and a European Preservation Order, as well as the order to designate a legal representative in the Union for the purposes of gathering evidence in criminal proceedings.
A European Production Order will allow a judicial authority in one Member State to request electronic evidence (such as emails, text or messages in apps) directly from a service provider offering services in the Union and established or represented in another Member State, regardless of the location of data, which will be obliged to respond within 10 days, and within 6 hours in cases of emergency.
The European Preservation Order will allow a judicial authority in one Member State to oblige a service provider offering services in the Union and established or represented in another Member State to preserve specific data to enable the authority to request this information later via mutual legal assistance, a European Investigation Order or a European Production Order. Both orders can only be issued in the framework of criminal proceedings and all criminal law procedural safeguards apply. The new rules guarantee strong protection of fundamental rights, such as the involvement of judicial authorities and additional requirements for obtaining certain data categories.
The group prepared a study on the methods of controlling the large-scale IT systems in the area of freedom, security and justice, which divides IT systems into three functional categories:
borders, asylum, migration (SIS II, VIS, Eurodac, EES, ETIAS);
police and justice cooperation (TCN-ECRIS, Eurojust, EPPO, Customs, Europol)
internal market (IMI).
In the framework of the coordinated control thus established, Member States and the European Data Protection Commissioner should meet at least twice a year, and report on the tasks accomplished. The tasks would roughly be equivalent to the already functioning control-group tasks.
The group also drew up the part of the report by the European Data Protection Board on the second review of the Privacy Shield Framework about data processing for national security and law enforcement purposes, which, among others, emphasizes the importance of appointing an independent ombudsman (for as yet only an acting ombudsperson fulfils the duties of investigating data protection complaints for EU Citizens).
Following the conclusion of the negotiations between the European Union and Japan on the protection of personal data, the Commission initiated the procedure for adopting the adequacy decision, as part of which it requested the Board to deliver its opinion. To prepare this opinion under Article 7 (1) s) of the GDPR, the Commission requested the International Data Transfer Expert Group (ITS) and the Borders, Travel and Law Enforcement Expert Group (BTLE). Following the delivery of the opinion of the Board, the Commission adopted the adequacy decision concerning Japan at the beginning of 2019.

III.4.3 Schengen Information System II Supervision Coordination Group (SIS II SCG)

The Schengen Information System (SIS II) the largest IT system in Europe, intended to handle the risk arising from the elimination of internal borders. As a result of development of the SIS II system, the introduction of new data categories, the system is efficient means in the fight against terrorism and cross-border law enforcement. With regard to the Schengen Information System, the Commission amended the regulation for the purposes of police and

judicial cooperation, border control, forcing back third-country nationals' illegal stay by the introduction of new categories and extended the scope of objects falling under alert categories to fake documents, highly valuable identifiable objects, and IT equipment. It has now become obligatory to enter refusal of entry or stay alerts in the SIS II.
Regulation (EC) No 1987/2006 of the European Parliament and of the Council on the establishment, operation and use of the second generation Schengen Information System (SIS II), which entered into force on 9 April 2013, provided for the establishment of a mixed type of coordination monitoring team, which came into being as the SIS II Supervision Coordination Group in 2013, and continued its activities in 2018. The SIS II SCG adopted a working document on logging of accesses to the system at national level. The group formulated recommendations concerning the mandatory logging, log fullness and minimisation, the identification of users, regulation of access to logs, training, enforcement of storage times, automatic deletion of logs, remote access, security, and security backups.
The European Data Protection Commissioner issued an opinion on proposals for ensuring interoperability between the large-scale IT systems of the EU published by the European Commission, and the group issued a letter in agreement with the opinion, and emphasized that the proposals are more about the inter-connection of systems than their interoperability. In the opinion of the group an opinion cannot be drawn up appropriately on the proposals, when the systems they concern are undergoing or about to undergo transformation.
The representative of eu-LISA, the operator of the SIS, reported in respect of the development of the central system that its capacity is continually increased. At the beginning of 2018, there were over 76 million alerts, meaning a 7% growth compared to the previous year.
The Authority was turned to in 17 instances concerning the processing of personal data in the SIS II. Most of these were questions on exercising data subject rights (requesting information and erasure), where the Authority provided general information to the notifier about the right of turning to SIRENE Office, its procedure, and the review the Authority may initiate. The duty of the SIRENE Office (Supplementary Information Request at National Entry) is to coordinate the responses to alerts in the SIS, and ensure that appropriate measures are taken when a person whose entry into the Schengen Area was rejected tries to enter the area again, or when stolen vehicles or identification documents are seized.

III.4.4 *The Visa Information Supervision Coordination Group (VIS SCG)*

The Visa Information System, alongside the Schengen Information System and the databases of Eurodac are operated by eu-LISA, the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice. The aim of the Visa Information System is to support the implementation of the common EU visa policy, consular cooperation, and consultation between central visa authorities. The Visa Information System is used at the consulates of the Schengen Area where visas are issued and at external border crossing points, where border guards check the identity of persons with biometric visas. The aim of VIS is to ensure the identifiability of persons not fulfilling the conditions of entry and stay in the area of the Member States. The VIS is accessible by law enforcement authorities, asylum authorities, and the Europol.
Visa Information Supervision Coordination Group (VIS SCG) delivered its opinion on the proposal amending Regulation (EC) No 767/200 (VIS Regulation), Regulation (EC) No 810/2009 (Visa Code), Regulation (EU) 2017/2226 (establishing the border registration

system), Regulation (EU) 2016/399 (the Schengen Borders Code), Regulation XX/2018 (Interoperability Regulation), and Decision 2004/512/EC (on the establishment of the VIS) and repealing Council Decision 2008/633/JHA (on accessing VIS). It is among the new aims of the common EU visa policy to improve the processing of short-term visa applications, the extension of the categories of VIS data, the extension of access to VIS by asylum authorities, facilitating the transfers of VIS data to third countries and international organizations, lowering the fingerprinting age for children to six, compulsory photograph taking when applying for a visa, and the extension of access to VIS for law enforcement purposes.

III.4.5 *The Europol Cooperation Board*

One case discussed in 2018 was the project European Tracking Solution (ETS) currently being prepared, which aims to provide a central European capacity for facilitating and supporting technical real-time, cross-border surveillance operations through encrypted channels.

III.4.6 *The Eurodac Supervision Coordination Group (Eurodac SCG)*

REGULATION (EU) No 603/2013 established the Eurodac system, enabling the countries applying the Dublin Regulation to establish by the comparison of fingerprints in the Eurodac System whether a third-country national illegally staying and claiming asylum has claimed asylum in another Member State. The Eurodac System assists determining the Member State responsible for examining an asylum application made in the EU. For the purposes of protecting personal data, the Member States sending data to the Eurodac shall ensure that the taking of fingerprints and the operations related to the processing, transfer, storage, and erasure of data are lawful. Data processing by the Eurodac is supervised by the European Data Protection Commissioner in cooperation with the national supervisory authorities (Eurodac SCG).
The Eurodac Supervision Coordination Group (Eurodac SCG) prepared a working document on the erasure of the fingerprints of persons who have obtained citizenship form the Eurodac, in respect of which it can be said that the practices of the Member States are not unified in terms of erasure, and unified application needs the drawing up of further requirements. At the meeting of the Eurodac SCG, the representative of eu-LISA reported on the latest developments of the IT system. In the first half of 2018, the Eurodac contained some 5.2 million fingerprints, and its capacity is 7 million (with plans to increasing it to 10 million). The most common faults in the system arise from the poor quality of fingerprints. The number of fingerprints taken from asylum seekers and those arrested for illegally crossing the external borders of the Member States has decreased, and the number fingerprints of those illegally staying in the Member States has increased.

IV. Freedom of Information (FOI)

At the beginning of this chapter, we wish to mention several phenomena and developments related to FOI alongside the most important Constitutional Court rulings. In last year's report we already pointed out that GDPR has influenced also FOI cases. The related provisions of the Privacy Act were left untouched by its 2018 amendment, yet there is an increasing number of cases, complaints, which belong in the 'common set' of the two informational

rights. This is especially true of manifestations freely spreading on the internet. Insofar as the right to the protection of personal data and the fundamental right related to the publicity of data—the right of access to data of public interest and data accessible on public interest grounds—are enforced together or in conjunction, the possible collision of constitutional rights has to be resolved in one way or another. A decision has to be made as to the protection of which interest serves the public interest better, and as to which concrete provisions of law and principles of law the decision can be traced back to. In these cases, the data subjects, persons whose rights were infringed, are either public persons (who by their positions in local or national public life become shapers of public opinion, yet at the same time they feel their privacy and personal data are threatened by others) or, quite to the contrary, persons fulfilling public offices (e.g. mayors) who choose improper means of 'exposing' infringements and pillorying others.

At the end of 2018, several submissions were filed with the Authority in relation to the publication of image recordings of mass demonstrations and the activities there in social media or various press organs. At mass events, private persons, parliamentarians and non-press organizations may naturally making video recordings, and, though the provisions of the Act on the Press do not apply to them, they are subject to the provisions of the GDPR, the Privacy Act, and the Civil Code. The lawfulness of the non-personal use, data processing, of such recordings is conditional on meeting various requirements under law, most emphatically among them, the lawful purpose of data processing and the related determination of appropriate legal basis (NAIH/2018/7556/V, NAIH/2018/7547/V).

The NAIH assumed a more intensive international role on the other fundamental right area in 2018. The most significant achievement of this was the international symposium presenting 'caselaw practices' in Budapest between 26 and 27 November 2018, which was attended by the staff members of national institutions for the supervision of the accessibility of public sector information from eleven countries (South Africa, Morocco, Germany, United Kingdom, Albania, etc.). Sixteen presentations were the basis of discussion, outlining the powers available to supervisory organs, the means of enforcing rights through the courts, the systems of publication schemes, as well as the cases of collision with other constitutional rights.

For a uniform judicial application of law and the enhancement of legal security, the comprehensive opinion of the workgroup analysing court practice entitled 'Lawsuits on providing access to data of public interest' was published. Under the provision of law, the leaders and members of the workgroups were the judges of the Curia, but as an external expert NAIH was also invited. As a result of two years' analysis, the comprehensive opinion included the analysis of the rulings sent by the courts to the Curia, separately discussing comments and suggestions on substantive and procedural law. For instance: judicial practice recognizes no extended interpretations in the case of references to bank and tax secrets, or when the requester of data access cannot define the scope of date requested with sufficient precision, as per the rulings studied, the courts proceed in good faith towards the

requesters, the reason being that the subject matter of the lawsuits is precisely the lack of information.
2018 saw the start of the review of the Directive 2003/98/EC of the European Parliament and of the Council on the re-use of public sector information (hereinafter the 'PSI Directive'). The public sphere produces an immense amount of data (e.g. meteorological data, digital maps, legislation, etc.), which are important resources of the digital economy. In its evaluation report, the Commission found that further measures are required in various areas; these include: the provision of real-time access to dynamic data via adequate technical means, increasing the supply of high-value public data for re-use, and tackling the emergence of new forms of exclusive arrangements and the use of exceptions to the principle of charging the marginal cost. NAIH also participated in forming the Hungarian position on the amendment of the PSI Directive—unfortunately, Hungarian preparedness with regard to open data had not been a success; though the Directive was transposed into Hungarian law, implementation has lagged behind.

IV.1 Constitutional Court Practice

For references' sake, the Constitutional Court adopted several major decisions on FOI:

- Decision AB 3077/2017. (IV. 28) (list of lawsuits pending over four years). The Constitutional Court rejected the constitutional complaint, because the name of a legal-person party to a civil lawsuit (complainant or defendant) does not constitute data of public interest, and therefore the controller (the court) shall not be obligated to provide access to the data.

- Decision AB 3/2018 (IV. 20) (The transparency of grants to natural persons by the Hungarian National Bank): The concealment of the names of winners of competitions by foundations undoubtedly managing public funds and performing public functions can be traced back to an omission by the legislator, because the personal effect of Act CLXXXI of 2007 on the transparency of grants from public funds does not extend to data controllers, and thus no personal data shall be accessible authorization by law lacking.

- Decision AB 3133/2018 (criteria of fulfilling wide-range data requests). The National Institute for Health Development rejected a request for documentation made during the examination to qualify a so-called psychoactive agent by reference to section 27 (5) of the Privacy Act. In its decision, the Curia highlighted that '*in view of the very special nature of the data requested for access, the restriction of publication, otherwise exceptional, is justified. According to the Curia, there is a genuine possibility (danger) that a publicly open specialist debate on the given very sensitive issue would put the persons involved in formulating professional opinion under major pressure, and this could certainly jeopardize the lawful operational order of the organ*

performing public function—the defendant—the fulfilment of its duties and powers without undue external influence, and thus especially the free expression of its data-generating opinions in the course of preparing its decisions. The assessment of drugs—and psychotropic or psychoactive agents qualified the same—is such an exceptionally special area that can result in a collision with not only lawful interests; it must however also be taken into account that the results of the decision-preparing work is regularly manifest in public provisions of law, and the list of agents concerned is continually changed, increased, and transformed.'
The Constitutional Court rejected the constitutional complaint, and emphasized that the data request by the claimant actually meant information with no actual quantitative limit and precise definition of scope, and was included in documents preparing decision making, and therefore the judicial interpretation of law was justified in applying the rule of automatic non-disclosure for the full decision-preparing process covered by the data request.

- Decision AB 3254/2018 (VII. 17) (the publicity of the foreign travels of a secretary of state): with respect to two concrete official trips by the state secretary for the Prime Minister's Office, the requester for data access wanted to know, apart from the subject matter of the negotiations (which was disclosed as a data of public interest), the names of the negotiating parties.
  The Constitutional Court rejected the constitutional complaint stating that these were personal data, the publication of which would require a concrete provision of law to qualify them as accessible on public interest grounds, not including sections 26 (2) and 27 (3a) of Privacy Act or when the data subject consents to the disclosure.

IV.2 Local Public Affairs—Questions of Creating Wide-range Local-government Publicity

Section 2 of Act CLXXXIX of 2011 on local self-government in Hungary regards the actual and effectual realization of publicity as a condition of self-government. It is thus a primary aspect in self-government operation that the principle of wide-ranging publicity is enforced, and all members of the community respect it. In practice however, the relation of local governments to FOI is variegated. The offices of some communities approach data access requests on an up-to-date 'fundamental rights' basis, while many others are not fully prepared, and regard data requests by citizens as harassment.
In the course of its inquiries and consultations, the NAIH also seeks to assume the role of a mediator between the parties, and assists mayors, local representatives, notaries, administrators, and officers of local-government companies in their work in the proper interpretation of law. (A member of our staff held lectures on the issues of local-government publicity for those responsible for data protection at Government Offices as invited by the State Secretariat for Territorial Public Administration and at a conference of notaries organized by the Hajdú-Bihar Government Office.)

IV.2.1 Fulfilling Data Requests

It should be borne in mind that 2019 is going to see local government elections in Hungary, and the activities of local governments and the related public sector information will receive greater public attention, for which data controllers will have to prepare. An indispensable condition ensuring FOI is for heads of organs to review their resources, and prepare their organizations to meet the requirements of changed needs by reorganizing, rationalizing, and expanding them.

In the practice of law of the NAIH, the organs of the local representative bodies constitute a unit from the perspective of ensuring FOI; that is, they cannot be regarded as separate organs performing public duties, and may not refer to any grounds that local government data access requests (e.g. access to declarations of personal assets, data of European Union tenders) should have been filed not with them. If there are internal rules on fulfilling data requests, the requests should be forwarded without delay under internal procedures to the person responsible for assessing and fulfilling them. Apart from this, notaries have a prominent role in coordinating, professionally and lawfully fulfilling or justifiably and lawfully rejecting requests.

IV.2.2 The Rights of Local Representatives

There is long-standing and particularly recurrent dilemma of interpretation with regard to local representative's right of access to information, which can only be resolved by the interpretation of the Local Government and Privacy Acts and the GDPR in conjunction. The local representative has no independent scope of duties and competences, his 'work as representative' consists in the participation in the preparation of decisions in certain matters subject to the competence of the representative body and its committees, and the organization and monitoring of their implementation. If the representative wishes to practice not his right to access information as a representative under the Local-government Act but the right of access to data of public interest, the rules under the Privacy Act must be applied when fulfilling requests to access data, but, in this case, the representative has no further entitlements than any other citizen, and has no right to access tax secrets, data in social welfare records, the personal data of public officials, and the employees of local government companies, or any other protected information. With the exception that these data are qualified as data accessible on public interest grounds by special provisions of law, or a local government decree based on the authorization of an Act authorizes the representative to access a type of data in order to fulfil his duties as a representative, or the local government assigns him as a member of a committee or individually (e.g. as a counsellor) to plan, organize, or supervise a duty in the competence of the local government. Complying with the principles of purpose limitation and data minimisation, the representative may need to access personal data (types of data) listed by law.

IV.2.3 The Data of Employees Accessible on Public Interest Grounds

The data of employees of local governments accessible on public interest was also a subject matter we often treated of. In respect of publicity, various categories of employment have to be differentiated with the proviso that the personal data of the person acting within the functions and powers of the organ performing public duties are also public when related to the fulfilment of the public duty, as several NAIH opinions, Constitutional Court decisions, and rulings by the Curia and the Budapest Court of Appeal unanimously point out (it is on this basis, upon assessing the given data request, that data concerning qualification or information about overtime work may be deemed as a personal data related to function and thus to be disclosed in spite of the fact that these are not listed by concrete law).

The widest circle consists of *public officials*. Under section 179 of the Act CXCIX of 2011 on Public Service Officials, the name, citizenship, the name of the public administration organ employer, the beginning of public service relationship, classification data, position, date of appointment to lead position, granting of title, and remuneration shall be data accessible on public interest grounds. It is important to note that the Privacy Act distinguishes between the accessibility of data, the dissemination of data and the publication of data; thus e.g. the proposals submitted to open sessions of local representative bodies containing personal data accessible on public interest grounds shall be published on internet websites for one year at most.

Under Act XXXIII of 1992 on Public-sector Employees, data of *public-sector employees of local-government institutions* accessible on public interest grounds shall be the name of the employer, the name of the public-sector employee, his or her position, and classification (i.e. no numeric data on remuneration).

The data of *employees* shall however not be data accessible on public interest grounds but personal data subject to protection. Employment contracts may be disclosed after anonymization (rendering unsuitable for personal identification), and employee data may be issued only in aggregated form, as statistical data. Under the Labour Code (Act I of 2012), the personal data of the employees of companies owned by local governments shall be transferred not even to local representative bodies, because, in terms of the continuance of the employment relationship, the representative body constitutes a third party. It is incorrect data processing practice to transfer the payroll with the data of employees included, in a way suitable for personal identification, in order to account for public subsidies. It must be noted however that section 2 of Act CXXII of 2009 on the More Economical Operation of Publicly Owned Enterprises, prescribes concrete data disclosure and internet publication obligations with regard to the officials of such companies.

IV.2.4 The Transparency of Public Funds and Government Subsidies

Section 27 (3) of the Privacy Act provides for the transparency of publicly funded contracts of services and state subsidies, specifying local governments and *ex lege* qualifying data related to the budget, the use of European Union funds, and the managing of local government assets as data accessible on public interest grounds. Any other party (not the

state) entering into such a contract shall be bound by the obligation to inform anyone thereof upon request. Data related to the names of beneficiaries of government subsidies, the place of implementation of the support programme, the allocation of public funds, management of public assets, and the denomination (type), subject matter, and names of parties to purchase, construction and service contracts worth HUF 5 million or more, and other data listed therein are accessible on public interest grounds, and must be published. In respect of the legal relations mentioned above, the names of natural persons qualify as data accessible on grounds of public interest. In the case of data qualifying as not relating to government subsidy, date on natural persons shall be protected (NAIH/2018/3091/2/V).

IV.2.5 Declarations of Personal Assets

There is a continued interest in accessing declarations of the personal assets of mayors and local representatives. Under section 39 (3) of the Local Government Act, the declarations of the personal assets shall be recorded and controlled by a committee provided for under the organisational and operational regulations (committee for declarations of the personal assets). The declaration of the personal assets of the local-government representative, excluding the identification data submitted for control purposes, shall qualify as data accessible on public interest grounds; we must however call attention to the fact that dissemination of these data is subject to the principle of purpose limitation, and their publication on webpages is governed by special provisions. Currently, Annex 1 of the Privacy Act does not provide for the obligatory publication of the declarations of the personal assets of local representatives, but no provision forbids local governments from nevertheless publishing them under organ-specific publication schemes (NAIH/2018/4196/V, NAIH/2018/1256/V).

IV.2.6 Local Governments and Digital Publicity

In the 21st century, wide-ranging publicity can be achieved digitally, by internet publication, in the most cost-efficient and citizen-friendly way (electronic FOI). The content and requirements of 'locally customary mode of publication' have definitively changed. Internet publication has come to parallel 'analogue' or customary modes of publication, such as billboards, gazettes, local television, etc., and will become almost exclusive in the coming decades. From the point of view of FOI, this the greatest challenge for local governments, which is corroborated by a significant number of submissions filed with the Authority.
In the framework of the programme entitled 'Local-government Companies—The Audit of the Economic Management of Companies whose Majority Owners are Local Governments', the State Audit Office notified the Authority several times on the deficient fulfilment of the electronic publication obligations of local governments and the companies they own, because the data of managing officials, supervisory board members, authorized signers, and employees entitled to disposal over bank accounts qualify as data accessible on public interest grounds under Act CXXII of 2009 on the More Economical Operation of Publicly Owned Enterprises. Without exception, all local government companies made up for the

deficiencies in accordance with NAIH notices (NAIH/2018/1224/V, NAIH/2018/1394/V, NAIH/2018/1597/V, NAIH/2018/1644/V).

Local governments are not obliged to run websites, but they are obliged to publish their data of public interest under the Privacy Act in the way and place of their choice (kozadat.hu, kozadattar.hu). In the practice of the Authority, local governments operating webpages serve the information rights of citizens appropriately when they publish the data required by the Privacy Act to be published thereon. The publication scheme in Annex 1 of the Privacy Act, the Government Decree 305/2005 (XII. 25) and Decree 18/2005 (XII. 27) of the Ministry of Informatics and Telecommunications 'assist' the compilation of the content of the public sector information repository.

Several submissions have been filed with the Authority due to the deficiencies of publication schemes or the data protection infringements they give rise to. Citizens like to take an interest in the activities of local decision makers, and data requesters regularly ask for information about the minutes of the meetings, decrees, proposals, agendas of the local representative bodies, and the invitations to and minutes of their various committees if this information is not found on the websites of local governments. This applies to the data on local government management, local budget conditions, and the details of spending public funds at local disposal. A 'popular' subject is the costs of events organized by local governments, and the contracts concluded to implement them, and the revenues of local festivals (NAIH/2018/2124/V).

IV.2.7 The Publicity and Live Coverage of Sessions of Local Representative Bodies

The publicity and live coverage of sessions of local representative bodies raise a number of practical questions. The invitations to, proposals, agendas, minutes, and resolutions of committee meetings of local representative bodies qualify as data to be disclosed. As a main rule, sessions of representative bodies are public, and anyone may participate at them. In Hungarian data protection practice, the local government or its agent provides live coverage—e.g. on the internet or local television; often audio recordings are made—of the sessions as per the local rules of organization and operation, but all those concerned have to be given prior notice thereof every time. (Notice may be made orally before the session or a notice displayed in a given space or on the webpage or social media site of the local television or the local government itself.) Those present at the sessions also have the right to provide live coverage or make audio or video recordings thereof subject to personality rights and the respect of human dignity. The publication of recordings of public sessions to inform the wider public is not unlawful, but, as stated above, personal data accessible on public interest grounds must not be disseminated in ways infringing the principles of purpose limitation and data minimization (NAIH/2018/6137/2/V).
Apart from those of closed sessions, citizens may access the proposals and minutes of local representative bodies. Resolutions passed at closed sessions of local representative bodies

are also public, and shall be published electronically, on the internet, under the Privacy Act. Data of public interest and data accessible on public interest grounds must be given access to even in the case of closed sessions. In terms of FOI, this means that data of public interest does not lose its public quality because it is generated at a closed session, and, even in the case of decisions made on persons at closed sessions, account should be made of whether data, types of data, processed there are rendered accessible on public interest grounds by law or not. Otherwise such data must be protected from unlawful access and publication; thus, the wording of public resolutions must not refer to data relating to natural persons. In the case of a (justified) complaint, the subject of the complaint was that the former employer of the complainant, the mayor's office of a community, had published the mayor's briefs on decisions made at closed sessions of the local representative body the website whereby anyone could tell that the complainant was involved in litigation against his former employer (NAIH/2018/7429/2/V).

IV.2.8 Social Media and Local Public Affairs

Communication and the provision of information increasingly take place on the internet, primarily social media, and it is small wonder that more and more communities and mayors have pages on the most popular social media provider (as well). The Authority received several complaints in this respect.

In one case, the Authority found that the name of the editor, administrator or moderator of the 'official' Facebook page of the town (mayor), qualifies as data accessible on public interest grounds under the Privacy Act, and it instructed the mayor's office to send the requested data to the requester (NAIH/2018/7338/V).

In another case, the mayor of a town published on his own Facebook page the letter of a local representative stating his resignation from being a representative. At the request of the writer of the letter, the letter was first removed from the Facebook page, and later posted again with redaction of the personal data of the former representative. The inquiry found that an elected local-government representative qualifies as person performing public duties, the resignation from being a local representative qualifies as a data of public interest, and the name of the representative qualifies as data accessible on grounds of public interest, but the personal identification data (place and date of birth, mother's name) are personal data always to be redacted.

The mayor of a community published photos of persons misusing the waste collection sites of the community on his own Facebook page. In the opinion of the Authority, the mayor would have proceeded lawfully by turning primarily to the organ competent to investigate criminal offences and infractions in order to identify the persons on the pictures (NAIH/2018/2866/5/V).

IV.3 The Act on Administrative Procedure vs. the Privacy Act, or Public Sector Information in Public Administration

In 2018, several complaints were filed with the NAIH where requesters sought to access the documentation of on-going administrative procedures (typically documents concerning tender procedures for the entitlement to provide local radio media services). In the opinion of the organ performing public duties, Act CL of 2016 on the Code of General Administrative Procedure (hereinafter: 'the Administrative Code') and *Act CLXXXV of 2010* on Media Services and Mass Communication (hereinafter: 'the Media Act') govern as *lege specialis* the accessibility and publicity of data of administrative procedures (procedure documents and decisions made therein), and thus section 27 (2) g) of the Privacy Act is applicable ('The right to access data of public interest or data accessible on public interest grounds may be restricted by an Act, with the specific type of data indicated, if considered necessary for the purposes of court proceedings or administrative procedures').

The interpretation and answering of questions related to the procedural and file access rules of the Administrative Code fall within the competence of the Authority only to the extent that they concern the two informational fundamental rights, but all possibilities of restricting the fundamental right of access to information must always be interpreted strictly (moreover the tendering stage of radio frequency allocation were completed in these cases). The fact in itself that the requested data of public interest are being used in an administrative procedure does not strip them of their quality of being data of public interest. The restriction of publicity in view of an administrative procedure can only be assessed in a concrete case. The NAIH has no competence to take a position on whether the data requester qualifies as a party or generally a third party to the administrative procedure commenced under the Administrative Code that formed the basis of the complaint. At every phase of the procedure, the party may access the files created in the course of the procedure, and he is entitled to do so even though he had not been party to the procedure earlier. Not being a party, the requester must appropriately substantiate his right to access a file containing personal data—in the event of the requester failing to do so or being unsuccessful in doing so, the organ preforming public duties proceeds lawfully, in the opinion of the NAIH, if it dismisses the request to access the file.

A third party may only access files containing personal data or protected data if he provides proof that becoming familiar with the data is necessary for the assertion of his right or for the performance of his obligation imposed by law, a court decision or a final decision by an authority. Again, the Administrative Code therefore only specifies the types of data that can be accessed under certain conditions. In the opinion of the NAIH, this section does not include any restriction with regard to data of public interest or data accessible on public interest grounds; interpreted, the provision only prescribes the redaction of personal and protected data.

On the other hand, access to the decision that has come into effect, in the opinion of the Authority, must not be denied from the complainant on grounds that the person of the party could be deduced from a summary of the decision (even though personal data have been redacted from it).

Under the Media Act, the procedures applied for tenders announced concerning the rights to provide linear media services using state-owned limited resources shall be governed by the provisions of the Administrative Code in conjunction with those of the Media Act, the Media Council shall thus provide information on the data included in tender offers only after the conclusion of the contract. In this respect, completed and on-going administrative procedures must be distinguished. If anyone wishes to have access to the files of a completed administrative procedure, this should be fulfilled as a main rule in the opinion of the NAIH.

In the opinion of the Authority, the restriction under section 27 (2) g) of the Privacy Act does not apply to completed procedures. It should also be noted that both the Administrative Code and the Media Act provide for restrictions concerning personal and classified data, but neither law prescribes the anonymization of data of public interest or data accessible on public interest grounds. In the complaint cases submitted to the Authority, it achieved the appropriate fulfilment of all access requests (NAIH/2018/291/V, NAIH/2018/819/V, NAIH/2018/1646/V).

IV.4 Rules of the Reimbursement of Costs Regarding Data Requests—Recent developments

In last year's report, we detailed the basic rules of reimbursing costs on the basis of Government Decree 301/2016 (IX. 30) on the Costs of Disclosure of Information (hereinafter: 'the Decree'). The experience of the last year is essentially the same, but the Authority issued its position on some new, untypical instances, with a view to the fact that the bodies performing public duties do not provide services when fulfilling requests for data of public interest, but comply with their obligations arising from the fundamental right enshrined in the Fundamental Law.

In 2018 most of the FOI cases consisted in complaints objecting to the legal basis of charging fees and/or disputing the amounts charged (39 in number). Ministries (Ministries of Finance, Agriculture, and Human Resources), local governments, companies owned by state or local governments, and public institutions were among the data controllers. The amounts determined showed a great variety; sums of a few 10 thousand forints were most usual, but there were charges running up to several hundred thousand, even million forints. (Hungarian State Treasury: HUF 5,414,856; Hungarian Rugby Alliance: HUF 1,972,666; Szeged Open-air Non-profit Ltd.: HUF 891,540 + VAT). The highest amount, HUF 11,482,540, was determined by the Police Headquarters of Budapest District IX, in a way not detailing the elements of costs to either the data requester or the Authority. (In this case, we turned to the National Police Captain.)

The efficiency and success of the NAIH as supervisory organ is proven by the fact that a significant proportion of the cases closed resulted in the data controller fulfilling data requests without charging fees or reducing the fees based on miscalculation and returning the fees that had been paid. This was the result of our inquiries of e.g. the Hungarian Rugby Alliance, the Ministry of Agriculture, the Budapest Police Headquarters, the Radioactive Waste Management Public Benefit Non-profit Ltd., Barcika Park Non-profit Ltd., and Budaörs Local Government. At the same however, it is true that several inquiries commenced last year were still unclosed at the time of drafting the report, as the positions did not come nearer even after several exchanges of correspondence.

It should be emphasized in this regard that charging fees is not obligatory. It is always for the given organ performing public duties to decide whether it wants to make use of this opportunity or not. If it does, it may only charge the actual costs of the data media used, delivery, and labour lawfully; no other element of cost may be taken into account.

Most problems occurred due to the reimbursement of the workforce necessary for fulfilling data requests, particularly because this element constituted the largest proportion of the fees charged to data requesters.

Fulfilling a data request necessarily involves certain amount workforce allocation—this is an institutional concomitant of the fundamental right to access data of public interest. According to the Decree, the cost of workforce may cover the time necessary for the identification, collection, and arrangement of the requested data, the time for the duplication, and the time necessary for the anonymization of data that may not be accessible. If this period exceeds four working hours, this cost element should be calculated in the following way: the working hours of the correspondent must be multiplied by the actual labour costs per hour of work (according to the Decree, this amount may not exceed 4400 HUF). Other contributions, bonuses, rewards and other benefits, such as fringe benefits cannot be taken into account. Importantly, fees must correspond to actual costs incurred, which might even be less than the amounts defined in the Decree.

In the consistently held opinion of the NAIH, the fulfilment of requests for data of public interest is not subject to VAT. This is undergirded by the opinion 'Tax question no. 2016/25 on determining fees to be charged for requests for data of public interest within the VAT system', issued by the competent department of the Ministry for National Economy in 2016. Additional work costs needed may be taken into account in determining the fee chargeable when, at the organ performing public duties,

1. the workforce needed for its ordinary operation
2. is required disproportionately, and
3. the period of using the workforce exceeds four working hours.

Accordingly, the period of disproportionate use of the workforce depends not on the fact that it exceeds four working hours. The three conditions mentioned must be met together.

On the basis of the criteria developed by the NAIH, during inquiries we asked, if necessary, what the number of staff was at the organ performing public duties, what functions the staff involved in fulfilling data requests held, what was the relationship between the functions of the staff involved in fulfilling data requests and the basic activity of the organ performing public duties, and what basic activities the fulfilment of data requests obstructed the organ from performing. We request the opinion of the data controller on why it considers that there is a disproportionate use of its workforce. We also take into account the technical infrastructure available to the organ (e.g. how many printers and scanners the organ has, and how long these were used for fulfilling the data request).

It is a question whether the data requested by the data requester are available in the form he requested. If not, what was the estimated workforce the production of the form he wished (the migration of existing data into processable Excel tables, etc.). It is not only the volume of data that counts but also the mode of accessing them (e.g. archived data).

It is also to be examined whether the data requested appear in the general Publication Scheme of Annex 1 of the Privacy Act; that is, whether the data are those that should have been published electronically by the organ. In the case of such data, no cost claim should have arisen in the first place, as the data request can be fulfilled by giving the precise internet link of the data under the Privacy Act.

The NAIH may ask what the ways of arranging the data into databases are (e.g. by manual selection or simple filtering in a digitized document). This fact has a significant effect on assessing whether there was a disproportionate use of the workforce or no.

In the case of workforce allocation, the NAIH requested data controllers to provide reports of how many staff and work hours they took into account, and what sums they calculated for each person in a given a position, and it also requested demonstration of what work processes were/are required by fulfilling data requests, and of how complex a duty it was/is to fulfil such requests (e.g. how many organisational units were/are needed to perform it).

If the justification of charging a fee had been the substantial size of the document, the NAIH took into account the size of the documents needed to be researched, systemized or copied for fulfilling the request.

If the data request is fulfilled electronically, the time required for making a copy may only be taken into account when

- the data required is not available in electronic form, or
- the time needed to make the copy is shorter than the time required to find the electronically available files.

In examining the cases of cost reimbursement, we seek to call the attention of data controllers to cost efficient ways of fulfilling data requests. In a concrete case e.g., the given organ had neither human resources nor technical means to provide the great amount of data requested, the NAIH, as mediator, successfully proposed that access to data should be ensured by way of enabling inspection, taking notes and photos (NAIH/2018/436/V).

According to the interpretation of law by the NAIH, if an organ performing public duties wishes to apply Section 29 (4) of the Privacy Act (i.e. to make the fulfilling of the data request subject to prior payment of a fee), it is obliged to notify the requesting party within 15 days of the receipt of the request. If the given organ exceeds this deadline, it may not charge a fee beyond it. No doubt, however, the provision is not clear as to whether the fifteen-day deadline for providing information on charging fees has an effect of absolute loss of rights. This deficiency of law has featured in several cases, and its resolution has been

unequivocal to neither the courts nor the NAIH. For, the data controller organ performing public duties, when, on the basis of its position in the legal issue, rejects to fulfil the data request—by reference to e.g. its not being a data controller with regard to the data requested or the data not being of public interest/accessible on public interest grounds—, has obviously not made a decision on charging costs. Charging a fee is connected to providing data of public interest, and it is related to the legal determination of the decision as a kind of additional matter. In order to orient legal practice, the NAIH took the position that, should the NAIH or the proceeding court, at the conclusion of the legal dispute, find that the legal position of the data controller had been wrong, and thus the requested data was to be disclosed, the 15-day deadline for determining the fee is recommenced as of receiving the notification on the administrative decision. The issue of interpretation and application of law mentioned can be satisfactorily be resolved by legislation. The NAIH notified the Curia of its position.

The Authority wishes to emphasize that the 15-day deadline for providing information under section 29 (4) of the Privacy Act is independent of the fact that the given organ has extended the time for fulfilment or not. The obligation to provide information applies in this case not to the extension of time for fulfilment.

Finally, the requirement of transparency in respect of reimbursing costs should also be emphasized. Transparency is served by appropriate information primarily. The more detailed the information, the more efficient it is. Unfortunately, we continue to receive information of malpractice in great numbers: e.g. 'with regard to the fulfilment of the data request, fees shall be charged', 'the cost of the data request shall be HUF x', from which no factual and legal justification of the determination can be discerned. The NAIH therefore requires, as a minimum, a breakdown of elements of cost, a report, in the case of additional allocation of workforce, on the number of staff and work hours and the hourly breakdown of sums per employee involved that were taken into account. Both remedy and NAIH inquiry procedures are facilitated if the data controller details the work processes required for fulfilling data requests. When substantial amounts of copying are needed, the provision of information has to detail this, e.g. the quantity of documents needed for fulfilling data requests. The requester must be notified of the possibilities fulfilling data requests without copying. In this regard, we must mention the practice of the Ministry of Finance that it does not provide information on cost elements of charging costs even when data requesters expressly apply for it, though, in the opinion of the NAIH, this is information which the ministry should have provided when determining the fee.
On its website, the NAIH published a Notice ('Tájékoztató') providing useful information on charging fees: http://www.naih.hu/files/Infoszab_tajekoztato_2018_06_30.pdf.

IV.5 Higher-education Publication and Publicity Issues

In its legal practice, the NAIH has consistently held that state-owned higher-education institutions are always organs performing public duties, while non-state-owned higher-education institutions are obliged to demonstrate the fulfilment of data requests before the public with regard to managing public funds and publication under special provisions of law. This is based on the annual financing agreement with the Government under Government Decree 389/2016 (XII. 2) on financing the basic activities of higher-education institutions, the list of which the NAIH requested from the competent ministry (NAIH/2015/6179/V, NAIH/2018/2301/V).

Copyright rules apply with regard to the content publicly funded university publications (section 27 (2) h) of the Privacy Act). As a result, the main rule is that as long as the author of a manuscript does not publish a university manuscript (either a diploma thesis or any other scholarly treatise and paper), the rules of free use do not apply, the work is subject to copyright protection, and it is only its author that is entitled decide on its publication. However, works produced in the framework of an employment relationship are subject to other rules. If producing the work is a duty resulting from such employment, the handover of the completed work qualifies as consent to its publication. In the event of the author's statement on revoking the work, the employer shall omit indicating the name of the author. Indicating the name of the author must also be omitted when the employer exercising its rights arising from the employment relation changes the text without the agreement of the author.

Diploma theses, dissertations, and other original intellectual products by students made during their enrolment are subject to different assessment. In the lack of a different agreement thereto, the contents of the works in the possession of the university library may be displayed on the computers placed in the university library for the scholarly research and study purposes of the students and visitors of the library and may be made accessible to the public if the said persons study the contents of the works not for purposes of generating income, because it would constrain students' learning, research, and professional development if scholarly works in the present or future possession of the university library were not accessible and readable at least locally, for a readership in the university library as broad as possible. The rules of free use apply to university publications with authorial consent.

With regard to university publications publicly funded, the question of the further use or reuse of publicly funded open-source research data likewise arises. Under section 3 (1) e) of Act LXIII of 2012 on the Reuse of Public Sector Information, public sector information managed by institutes of education and research, schools, universities, archives, libraries, and research institutes and organisations set up to forward research findings may not be released for re-use, and no law shall provide that they may be defined as public sector information obligatory to be made available or as cultural public sector information. As per

currently effective Hungarian law, the public sector information processed by universities constitute an exemption from rules on reuse.

It should be noted however that the open access to scientific publications is a topical question that has been on the agenda in the European Union for several years. The European Commission and the competent Commissioner have spoken up for open access in their press releases.

Many university teachers continue to have difficulties in reconciling themselves with the teacher data sheets on the website MarkMyProfessor (www.markmyprofessor), objecting to the comments on teachers, the content and style of these assessments. Our position is unchanged, the running of the higher education system is the duty of the state, thus all higher education institutions recognized by the state—regardless of their maintainers—are institutions performing public duties, and the teachers and employees performing duties related to education qualify as persons performing public duties and assuming a kind of scientific public role. In view of the fact that the purpose of the database on the website is to provide information to students about the level of the teaching provided by the given teacher and the current requirements, the name of the teacher may be given in relation to the teaching activity as per the original purpose insofar as she or he is on the staff of the institution. (The operator of the website is obliged to delete the data sheets of those teachers who, when no longer employed as teachers, request so from the data controller.) Persons performing public duties (just like those in public life) have to tolerate more in terms of the negative assessments made of them and criticisms of their professional activities, which, however, may not entail any disrespect of human dignity. The operator of the website shall be liable thereof.

IV.6 Environmental Information

Providing the public with access to environmental information is indispensable for ensuring the right to a healthy environment. The lack of such information can obstruct the public in taking part in decisions on the environment. Fortunately, the legal basis of access to such information is severally ensured; apart from the Privacy Act, section 12 (2) of Act LIII of 1995 on the General Rules of Environmental Protection lays down that information on the environment constitute data of public interest; moreover, section 4 (1) Act LXXXI of 2001 promulgating the Aarhus Convention obligates public authorities to 'to provide public access to the requested environmental information in the framework of national law'.
The law provides for exceptions to publicity, such as e.g. in view of the confidentiality of administrative procedures and the protection of personal data, but the exemptions 'are to be interpreted narrowly, taking into account the public interest in revealing the information'. Government Decree 311/2005 (XII. 25) on the Rules of Public Access to Environmental Information determines what data qualify as environmental data (e.g. data concerning the condition of the elements of the environment, environmental burden, measures related to the environment, and environment protection measures).

Several complaints were filed with the Authority on this subject matter, especially with respect to tree felling licences. The sudden disappearance of trees that have become parts of street imagery can become emotional issues.

Apart from these, complaints were submitted on the plans for the management of the high-water bed of the Danube, the construction project at Városliget ('City Woods'), the community transport development of a town, the amount of waste delivered at a waste site, the documentation of an administrative procedure on smell effects, and the noise pollution and operation of a battery factory.

In spite of the wide range of information involved in the requests dismissed, certain similarities can be observed in the justifications data controllers gave for their dismissals.

The Aarhus Convention provides for the dismissal of a limited few cases of environmental information requests, but the exceptions are to be interpreted strictly taking into account the public interest in revealing information. One possible justification of dismissal may be a request to access the internal communication of public authorities. The implementation guide to the convention[18] states: 'Opinions or statements expressed by public authorities acting as statutory consultees during a decision-making process cannot be considered as "internal communications". […] Moreover, once particular information has been disclosed by the public authority to a third party, it cannot be claimed to be an "internal communication".'

Though legally wrong, the reasoning that the data requester is not a party to the procedure where the decision was made often occurs. On the basis of the argument stated with regard to the provisions of the Administrative Code above, the entitlements of a party do not touch access to final administrative decisions adopted.

Another similar dismissal justification is the limitation of publicity of data grounding decision making. These decisions have to be made with circumspect deliberation and to be justified according to criteria laid down by the Constitutional Court in several decisions—data controllers nonetheless failing to abide in several cases. Data controllers failed to appropriately justify their holding back from the public the local-government opinion concerning the he high-water bed of the Danube and the World Heritage impact study made for the UNESCO World Heritage Committee; we thus established the infringement of the right to access data of public interest in these cases (NAIH/2018/7054/2/V).

Finally, it should be noted than whenever an organ performing public duties has the right of discretion with regard to access to data of public interest, we always call its attention to the fact that access to environmental data is indispensable for ensuring the right to a healthy environment.

IV.7 Other Cases in the Limelight

In 2018 several questions, submissions for consultation or complaints were filed with the NAIH, the subjects of which were the publicity of general charges of corruption. In these

18

The Aarhus Convention: An Implementation Guide: http://www.unece.org/index.php?id=35869

cases—as in the so-called Elios case—, the Authority is obliged to contact the competent prosecution and crime prevention organ because the restriction of publicity under section 27 (2) c) of the Privacy Act must be respected by all actors. According to the statement of the Public Prosecutor's Office, the full publication of the findings of the OLAF report on the cases in question would certainly hinder the interests of the investigation the criminal offences; this procedure-law constraint cannot be lifted until the conclusion of the investigation. (Note: as, according to the reports in the press, the Hungarian Government is removing the invoices of the public lighting projects implemented by Elios from the final invoice package to be submitted to the European Commission, the report has no relevance with regard to the publicity of data of public interest.) (NAIH/2018/1208/V, NAIH/2018/1221/V, NAIH/2018/1606/V, NAIH/2018/1824/V).

The Hungarian Football Federation requested an opinion on whether the referee and referee controller funds qualify as data of public interest. In accordance with the provisions of the Privacy Act, Act I of 2004 on Sports, and the Charter, the organisational and operational regulations of the Football Federation, and its regulation effective of 1 July 2018 and entitled 'Football competition rules for full-size and decreased pitches', in the course of this activity, the Football Federation qualifies as an organ performing public duties, and thus the names, the duties of the referees and referee controllers proceeding in the scope of the duties and competence of the Football Federation, and their other personal data related to their exercising its public duties—except for the personal data to be protected—are data accessible on public interest grounds. On the other hand, disclosure of the names of the referees and referee controllers a day before the championship event is appropriate practice, whereby the Football Federation causes no significant harm to the given referee or referee controller, fulfils the obligation to provide information appropriately, and also efficiently protects the outcome of matches from unfair influence (e.g. the bribery of referees) (NAIH/2018/5631/V).

A requester of data wanted to access information—primarily business information—about chicken-pox vaccine from the Ministry of Human Resources. The Ministry qualified the data as decision-preparing data, and referred to the fact that the business interests of the company producing the vaccine would be harmed if competitors were be able to know the precise of price at which it offered the product to the health system. The Authority found the argument to be substantiated, and accepted it (NAIH/2018/3256/V).

A complainant parent objected to the recognizable appearance of his minor daughter in the cover picture of a political article on the Hungarian Scouts Association. In the course of the inquiry, it turned out that the article in question was illustrated by a picture downloaded from the MTI (MTVA) Fotóbank ('Photobank'), and was used with content that differed from the original dispatch. Upon our notice, the illustrative picture was deleted; it was found that no media took over the article, and the internet search engines (Google, Bing) were notified to delete the content indexed earlier, and to index the new article with the new content.

With regard to the fact that most scouts are minors, the personal data of whom are to be protected under the GDPR, it is important that the children and their legal representatives be properly informed of data processing issues. The Scouts Association informed the Authority that, it calls the attention of participants at its public events, notices at registration

and venues that video, photo and voice recordings are made of the event where the participating person might be recognized. The Authority suggested, apart from this, to include the general notice in its organisational and operational rules (NAIH/2018/4601/V).

IV. 8 The Google Search Engine

The Authority sent letters of request to Google in several cases in 2018. These were directed at mapping actual practice, but there was also an instant where the Authority required, on account of the changes in the legal environment (Article 24 of the GDPR), that the data controller change its former position. We asked Google what the basis on which it ranks search results is, how the search algorithm works, what the criteria of ranking are, what measures it has introduced to comply with the provisions of the GDPR.
The following links provide further information:

- https://transparencyreport.google.com/eu-privacy/overview
- https://policies.google.com/privacy?hl=hu
- https://privacy.google.com/your-data.html.
- https://support.google.com/transparencyreport/answer/7347822/?hl=hu

In on concrete case, a complainant, a highly respected person, objected that the Google search result list included URL-s containing information about the complainant's deceased spouse and family life that are damaging and contemptuous. Google had dismissed the request earlier on grounds of public interest, but, upon the Authority's notice, it removed the links pointing to the contemptuous articles.

It should be noted here that deletion from the search list merely cancels the route of access, but the information continues to be available on the website. Should the data subject wish to have the full deletion of the data, she or he should turn to the operator of the website requesting the deletion of the data.

V. Supervision of Data Classification, Classified Data and Public Data with Limited Publicity

The thorough-going changes in data protection, the entry into force of the GDPR and the amendment of the Privacy Act in 2018, little affected the groups of cases of the Authority related to data classification. There are two obvious reasons for this. First, the classification of data in one part (perhaps the largest part) of the classification procedures limits not the right to the protection of personal data but access to data of public interest, and the legal regulation of data of public interest hardly changed in the reporting period. Second, the classification of such data usually takes place for the purposes of law enforcement, national security, and sometimes national defence; that is, this kind of data processing continues to be subject to the Privacy Act. The cases of data classification of the Authority in 2018 were characterized by continuity and the upholding of the practice established earlier.

V.1 The Problems of Repeated Classified Data

In the course of an authority procedure for the supervision of data classification but also with a general applicability, the question arises how can the unlawful limitation of data publicity be acted against when the subject of the procedure of the Authority is not the classification of the data but the repetition of the classification mark. (According to Section 7 (1) of Act CLV on the Act CLV of 2009 on the Protection of Classified Data (hereinafter: 'the

Classified Data Act'), no new classification procedure shall be conducted if classified information prepared by the own or another classifier earlier is also included in the information prepared, and in the course thereof no further information requiring own classification shall be generated. In such cases the classification mark of classified information prepared earlier shall be repeated, unless prohibited by the classifier of the information intended to be repeated […].)

In the case mentioned, according to the facts of the case established by the Authority, the documents generated in the open part of a criminal procedure at Central Chief Prosecution Office of Investigation had been given a repeated classification mark. The classified data had been created by way of intelligence gathering previously. According to the information provided by the Central Chief Prosecution Office of Investigation, the reason for repeating the classification was that the documents listed included classified data referring to the means and methods of gathering intelligence by the National Protective Service with judicial authorization. In the course of the investigation, the National Protective Service had expressly requested the Central Chief Prosecution Office of Investigation to maintain the classification of the evidence in the criminal procedure in order to protect the means and methods used. The Central Chief Prosecution Office of Investigation initiated the termination of the classification, but the classifier refused to do so. The Authority requested the documents containing the repeated classification. In the course of the procedure of the Authority, the classifier provided the information that it decided on the termination classification in respect of the classified data in the documents. In view of the fact that the classification of the data in the notification was terminated by the classifier, and the circumstances grounding the inquiry ceased to exist, the Authority terminated the inquiry. Though there was no opportunity to establish the lawfulness of the data classification as the classification, its repetition, was terminated, as a matter of principle it did arise what legal means are available for acting against the unlawful limitation on publicity when it can be established that the classification was lawful, but its repetition violated the enforcement of the right to the protection of personal data or access to data of public interest. (Such violation of law may occur when, in the repetition of a classification mark, the classification mark is applied to data the original classification had not been applicable to and the conditions of their classification under the Classified Data Act have not been met either.)

The problem is caused by the fact that, under the Section 63 (1) of the Privacy Act, the Authority, in its decisions adopted in authority procedures for the supervision of data classification, shall, in the event of any infringement of the laws pertaining to the classification of certain national classified data, require the classifier to modify, in accordance with the law, the level or term of the national classified data, or to have it declassified, but this provision does not apply when it was not the classification but the repetition of the classification that was unlawful. The reason why the unlawful repeater of the classification mark cannot be acted against pursuant to an authority procedure for the supervision of data classification is because in an authority procedure for the supervision of data classification under Section 63 (4) of the Privacy Act the client is the classifier. As a consequence, the repeater of the classification mark is not in the position of client but a witness, or a holder of the object of the inspection, in an authority procedure for the supervision of data classification, and therefore the sanction under Section 63 (1) of the Privacy Act does not apply. It can therefore be concluded that, under the effective Privacy

Act, the Authority can act against the unlawful repetition of classification pursuant not to an authority procedure for the supervision of data classification but an inquiry.

V.2 Further Data Processed in the Spy Trial

In last year's Annual Report, the Authority outlined the review of the data classification in the Spy Trial. In the procedure conducted in 2017, the Authority required the classifier to terminate the classification of data generated at the National Protective Service. In the course of our 2017 procedure it turned out however that there were data in the documentation of the Budapest Court of Appeal the classification of which was carried out not at the National Protective Service but the Office for National Security (hereinafter: 'the ONS'; its successor organization is the Constitution Protection Office). The Authority supervised the lawfulness of the classification of these data in a new authority procedure for the supervision of data classification. The documents subject to the procedure contained information gained by way of a polygraph examination. The examined documents included very detailed and sensitive pieces of information, such as reports and memos made at the various organizational units of the ONS, pertaining to some small particulars of the historical facts of the case. These documents may not be detailed any further, because some of the details of the case examined by the Authority might have an adverse effect on the foreign-policy and diplomatic relations of Hungary and may lead to inferences on the activities of the Hungarian national security organs, which might encumber the continuous intelligence capabilities of Hungary. The documents include content that obviously need to be defended with the following subjects matter:

Technical data concerning the structure of national security service and the rules of gathering intelligence;

Details of polygraph methodology, the circumstances and results of the polygraph examination of the staff members of national security services, including highly sensitive information on method, the publication of which would endanger trustworthiness and effectiveness of future polygraph examinations;

The information in the documents could be used for attempts at identifying and unauthorizedly influencing members of the national security organ;

Knowledge concerning the method assessing national security intelligence and specific measures;

Not public information concerning intelligence agencies of other countries and diplomatic negotiations with other countries;

Data concerning Hungarian national security intelligence sources.

On these grounds, the Authority established that the classification of the data examined in 2018 had been lawful, and the maintenance of their classification level as 'Top Secret!' continues to be justified.

V.3 The Qualification of the Implementation Agreements of Paks II Nuclear Power Plant Construction

The Authority received several notifications about the classification of the three implementation agreements between MVM Paks II. Atomerőmű Fejlesztő Zrt. [Nuclear Power Plant Development Corp.] and the Russian Joint-Stock Company Nizhny Novgorod Engineering Company Atomenergoproekt.

The Authority commenced an inquiry to establish whether the classification of the documents of the case violates the exercise of the right to access data of public interest and data accessible on public interest grounds, or if there is direct danger of this. The Authority

requested the classifier to provide a detailed justification of the classification, and conducted a document inspection, examining the documents concerned on site. The examination of the documents was hindered by the large volume and their complicated subjects matter and their being written in English. As the classifier reviewed the classification in the meantime, the Authority requested the classifier to send it copies of the review decisions and the documents concerning the review. Though the classifier terminated the classification of a significant part of the Paks II implementation contracts, the Authority wanted to clarify the justification of the classification of the remaining parts at expert level consultation. The classifier delivered to the Authority its opinion on the parts classified as 'Restricted'.

The inquiry found that the classification of the data in the implementation agreements meets the substantive and procedural requirements of the Classified Data Act. The classification procedure was conducted in accordance with classification proposal in and within the deadline prescribed by the Act. The classifier recorded its decision on classifying the data in writing, and had the classification marks written on the documents pursuant to the Classified Data Act. As far as the necessity of the classification is concerned, the Authority requested the classified several times to provide the justification of the classification, whereby it could be decided whether the given data content required the maintenance of the classification level or its validity period as a the right of access to data of public interest may only be restricted by classification to the qualification level required by protection under conditions prescribed by the Classified Data Act and for a period absolutely necessary.

Several difficulties arose with regard to the content of the classification, the distinction between public information and information to be protected, hindering the establishment of the facts of the case. First, the material to be examined was exceedingly voluminous. Second, the implementation agreements regulated an extremely wide variety of particular issues, making it difficult to answer whether the publicity of a given piece of data needed restriction. The classifier made the classification on the entire text of the agreements; that is, it was no the data principle but the document principle that was enforced. Classification however must apply to specific data content in line with the data principle, and it is necessary to review the justification of the protection by classification of given parts from time to time. Having consulted with the staff members of the Authority, the classifier terminated the classification of the significant part of the agreements in line with the data principle, and sent the justification of the parts requiring continued 'Restricted' classification to the Authority.

V.4 Access to Contracts Concluded by the Paks II Zrt.

Though not a classification issue in the strict sense of the word, the following details the fee calculation practice of the Paks II Zrt. in respect of its provision of information.

According to his complaint filed with the Authority, a complainant had submitted a data access request to the Paks II Zrt, requesting access to all the contracts of service and procurement worth over HUF 1 million the company had concluded between 1 January 2017 and the submission of the data access request. The company determined a fee of HUF 176,000 to be paid by the complainant by reference to the fact that the fulfilment of the request for data access required a disproportionate use of the workforce needed for its ordinary operation.

With regard to the company's calculation of fee, the Authority called its attention to the fact that it is the basic personnel salary that must be taken into account when determining the cost of workforce used, and not the thirteenth-month salary, the sum of optional extra-

salary benefits and C-tariff compensation, and contributions to voluntary pension funds, voluntary social security funds, voluntary benefit funds, social, training and healthcare funds, and personal income tax. The Authority also reminded the company that bodies with public services functions do not provide services when fulfilling requests for access to data of public interest and data accessible on public interest grounds, but comply with their obligations arising from a fundamental right.
The Authority proposed that the company further reduce the fee as access to the requested data of public interest is a priority public interest. Though Section 29 (3)–(5) of the Privacy Act does provide for a legal basis for bodies performing public duties to determine a fee for the costs of fulfilling a data access requests, they may decrease the fee charged or even omit charging a fee.

V.5 The Authority of a Member of Parliament to Access Classified Data
The Secretary of State for Public Administration at Prime Minister's Office requested the opinion of the Authority whether a member of parliament or a member of the European Parliament, in the possession of a user's authorization under Section 98 (2) of the Parliament Act, may have access to data in respect of which an authority procedure for the supervision of the lawfulness data classification is in progress or not.
The right of access to data of public interest is a fundamental right enshrined in the Fundamental Law. Under the Fundamental Law, fundamental rights due to citizens or everyone shall be construed in the relationship between individuals and the State. The fundamental right to access and disseminate data of public interest pursuant to Paragraph (3) of Article VI of the Fundamental Law is due to the individual as against the State. But this right is to identified with the right of the members of democratic public bodies to seek and access information which can be derived from the principles of the rule of law and is provided for by the Parliament Act. The consistent practice of the Authority is that the interpretation of the right of access to information of members democratic public bodies as provided for by a special Act and the examination of submissions concerning the right provided for by the special Act fall not within the scope of duties and powers of the Authority as defined by law.

V.6 The Supervision of the Lawfulness of the Transfer of the Powers to Classify data as 'Top Secret'
Member of parliament Márta Demeter filed a notification with the Authority that the cabinet head of the Prime Minister's Office may apply the minister's authority to classify data as 'Top Secret' pursuant to the Organizational and Operational Rules of the Prime Minister's Office. Under Section 4 (2) a) of the Classified Data Act, classifiers may delegate their classification powers in the case of data classified as 'Top secret' to their deputies, and the members of the Government to the secretary of state for public administration, the secretary of state, and the undersecretary. The cabinet head of the Prime Minister's Office does not belong among the persons fulfilling positions to whom the powers to classify data as 'Top secret' under Section 4 (2) a) of the Classified Data Act may be transferred, and thus the Authority commenced an inquiry as to whether the transfer of the classification powers of the minister leading the Cabinet of the Prime Minister's office resulted in a violation of law with regard to the protection of personal data and the exercise of the right to access data of public interest and data accessible on public interest grounds. The inquiry found that the cabinet head actually did not apply the classification powers transferred to him;

moreover, the minister leading the Prime Minister's Office terminated the transfer of powers to classify data as 'Top secret' in the course of December 2018, and thus the Authority terminated the inquiry in the case.

V.7 The Classification of Data in a Dispute over Real Estate

Action was brought to access data of public interest against the Hungarian National Asset Management Inc. (hereinafter: 'the HNAM'), because it rejected a request for access to data of public interest which concerned the documents about the Csillebérc Pioneer Camp, a piece real estate disputed, where the HNAM proceeded on the part of the Hungarian State. The Budapest-Capital Regional Court initiated an authority procedure for the supervision of data classification with the Authority to control the lawfulness of the classification.

During the authority procedure for the supervision of data classification, the classifier referred to the fact that the publication of the predefined financial and legal framework for the agreement to be concluded in order to settle the property-rights situation of the real estate, that is, premature access to the data by the contracting party, third-party contracting parties or the public at large would have created a negotiating situation leading to a conclusion of the contract disadvantageous to the Hungarian State or even preventing the property acquisition thereof and, furthermore, unlawful gain or advantage to citizens and business organizations. According to the classifier, the 'Restricted' mark for a maximum period was justified in order that, following the conclusion of the agreement between the contracting parties, no third party would be able to attain unlawful gain or benefit, or that these persons would not be able bring financial damage to the Hungarian by state by making claims based on such information.

In the course of the procedure, the Authority found the justification for the determination of the classification period unsubstantiated. In this regard it needed clarification why there was a need to further maintain the classification following the conclusion of the agreement closing the legal dispute between the parties and the fulfilment of the obligations arising thereof. The classifier failed to clarify who 'the third parties possibly concerned' would be, what claims they might make, and how the claims could result in unlawful gain or benefit. The Authority requested the classifier to provide further detailed justification, and to specify the claim, if applicable.

Thereafter the classifier stated that there remained no disputed matter between the parties concerning property and possession rights following the agreement, and did not justify the maintenance of the maximum classification period with any further reasons; in other words, that that publication would certainly affect the public interest to be protected following the conclusion of the agreement and the fulfilment of the obligations thereof.

The findings of the Authority are as follows:

Taking into account the fact that, according to the statement of the classifier, the dispute in question was closed by the agreement, and the acquisition and the entry into possession took place in accordance with the contract, the Authority established that the further maintenance of the classification was not justified. The publication of the data would not affect the content, conditions, or the bargaining position, of the agreement, and cannot cause any financial loss to the State. The publication of the data could not influence the public interest to be protected.

In the case of an agreement closing a dispute, it is the safeguards to be included in the agreement that are to exclude the possible claims of third parties, and which the parties concerned must guarantee. The classification of data may not serve the purpose of

preventing third persons from enforcing their claims by blocking data from publication. Following the conclusion of an agreement, the parties thereof have no right to judge the lawfulness or unlawfulness of claims arising not subject to it.
It turned out from the documents that the contracting parties undertook implied warranty and warranty of title for the entering into the possession of the property, and they guaranteed the that the real estate was free and clear of all liens, claims and encumbrances. In other words, the parties provided for the exclusion of possible claims related or concerning the real estate pursuant to the rules of civil law.
It is a constitutional requirement that the classifier, when deciding about the classification of data of public interest or accessible on public interest grounds, must take into account, besides the public interest in classification, the public interest in publicity, and should decide for classification when the purpose of classification is proportionate to the public interest in publicity. Articles 38 and 39 (2) of the Fundamental Law of Hungary, raised the requirements of the transparency of managing public funds and national assets and the classification of data relating to public funds and national assets as data of public interest to constitutional level. In the case of data relating to public funds and national assets, the significant weight of the public interest in access data must be taken into account pursuant to the principles of transparency and the purity of public life.
The following reasons corroborate the interest in the publicity of the data:
The dispute over the property rights of the real estate has been in progress for decades, certain details of which have been known to the public, and command public interest;
The dispute between the parties has been concluded by a binding agreement, and the claims related to the real estate have been resolved;
Classification of the data had been partially terminated by the classifier, as this was a condition of concluding the agreement in the matter disputed and the contract of sale, and of entering it in the real-estate registry;
Certain information about the utilization of the real estate have been published in the press, and these also command public interest.
As a result of the occurrence of the legal facts defined by the agreement, the public interest to be protected by classification is no longer affected by publication. The reasons justifying classification over the interest in the public access to the data have ceased to exist.
The Authority agreed with the classifier's opinion that the publication of the data classified could have resulted in financial damage to the Hungarian State. The publication of the predefined financial and legal framework for the agreement to be concluded in order to settle the property-rights situation of the real estate would have enable the contracting party—and third-party in a legal relationship with contracting party concerning the real estate—to negotiate an agreement to the disadvantage of the Hungarian State, requiring additional resources from the budget. The publication of the data on the legal and financial framework classified in the interest of concluding the agreement could thus have resulted in an agreement disadvantageous to the Hungarian State, causing financial loss. However, the Authority also found that that it was not justified to maintain the classification of the data for the future, because even in the case of meeting all the conditions stipulated by the Classified Data Act, data may only be classified for a period absolutely necessary. Therefore, the Authority established the violation of the laws concerning classification, and ordered the classifier to immediately terminate the classification. The classifier did not bring an action against the decision of the Authority before a court within 60 days of its communication, and thus the classification of the data was terminated following this deadline by course of law.

VI. International Affairs and Public Relations

This chapter summarizes the international activities of the Authority.
We present international conferences, including the Berlin Working Group and the workshop complaint handling colleagues of data protection authorities hosted by the Authority.

VI.1 The Modernisation of the Council of Europe Personal Data Protection Convention

Adopted by the Council of Europe in 1981, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, so-called Convention 108 (promulgated by Act VI of 1998 in Hungary) was the first significant international legal instrument binding to the Member States. For four decades, it provided for the framework of data protection and the basis of national and international regulation thereof. After seven years' preparation, the Protocol (CETS No. 223) amending Convention 108 was adopted on 18 May 2018, and was ceremonially opened for signature on 10 October 2018. Hungary signed the instrument on 9 January 2019. According to Secretary General Thorbjørn Jagland the modernized convention, which data protection experts dub 'Convention 108+', is singular instrument globally for cooperation in the regulation of the protection of personal data.

The modernisation of Convention 108 pursued two main objectives:
to deal with challenges resulting from the use of new information and communication technologies and
to strengthen the Convention's effective implementation.

The purpose of the modernized convention is to ensure that the transborder transfer of personal data takes place with appropriate safeguards and to provide consistency with international normative frameworks, including the regulation of the European Union. The reviewed convention enables accession for all Member States of the Council of Europe and international organizations.

The most important innovations of the Convention:
stricter requirements in the course of data processing through the application of the principles of proportionality and data minimisation
the extension of the concept of sensitive data (genetic and biometric data, trade union membership, ethnic origin);
obligation to notify personal data breaches;
greater transparency in data processing;
new rights for natural persons in the application of automated decision making, which have particular significance in the development of artificial intelligence;
stricter accountability of data controllers;
the formation of a clear system for transborder data transfer;
reinforced powers and greater independence for data protection authorities, and the strengthening of the legal basis for international cooperation.

VI.2 International Conferences in Budapest

VI.2.1 The 63rd meeting of the Berlin Working Group, Budapest

63rd meeting of the Berlin Working Group was held in Budapest, at Grand Hotel Margitsziget between 9 and 10 April 2019, organized by the Authority with 53 participants. According to feedback, participants found it successful and professionally rewarding. The agenda of the two days of meeting was as follows: the standards for data protection and personal privacy in cross-border data requests for criminal law enforcement purposes; drafting of opinion on the data protection challenges of smart cars and intelligent transport systems; review of the data protection concerns about intelligent infrastructures/cities; drafting opinion on the

data protection challenges of artificial intelligence; review of data protection concerns of intelligent games; obtaining parental consent for data processing concerning children; intelligent television and the protection of privacy. Two documents were adopted at meeting: 'On Smart/Connected Cars' and 'The standards for data protection and personal privacy in cross-border data requests for criminal law enforcement purposes'.

VI.2.2 Data Protection Case Handling Workshop 27–28 November 2018

After the 2012 workshop, the Authority hosted again a regular meeting of the staff members of European data protection authorities specially concentrating on practical cases.
Over 50 experts participated representing 14 EU and 7 non-EU authorities. Based on feedback and proposals, the agenda focussed on authority procedures and current data protection issues with special attention to cross-border data protection matters resulting from the coming into force of the GDPR. Following brief presentations, discussions concentrated on data transfer to third countries, the cooperation of EU and non-EU national authorities under Article 50, the use of publicly accessible personal data, and the issues of camera surveillance and right of access.
According to feedback from participants, the workshop was successful. On the proposal of the Hungarian authority, the hosting authority is going to fulfil a sort of secretariat role when new workshops are organized, assisting the maintenance of contacts and cooperation between national authorities.

An international meeting to present 'Case-law Practices' took place in Budapest between 26 and 27 November 2018, gathering staff members of national authorities supervising data publicity from 11 countries. This meeting is discussed in the chapter on Freedom of information.

VI.3 The Joint workshop of Consumer and Data Protection Authorities

Social media platforms often raise issues and concerns that have consumer and data protection aspects simultaneously, and thus the cooperation between consumer and data protection authorities needs to be emphasized. It was in this framework that the DG for Justice and Consumers of the European Commission organized the second joint workshop for the staff members of consumer and data protection authorities in Brussels on 23 November 2018, where delegated experts of the NAIH and the Hungarian Competition Authority also participated. The workshop was organized around lectures and case studies on the synergies between data and consumer protection, and as a conclusion, the Commission outlined the following possibilities for promoting and strengthening the actual cooperation between consumer and data protection authorities:

- The establishment of a common 'wiki' surface where the two disciplines can communicate and share experiences and good practices;
- The establishment of a working group (on voluntary basis) that would develop guidance on practical cooperation and implementation between national authorities. It was clear from the discussions at the workshop that it would be useful to share good practices of cooperation or to develop forms or templates whereby the authorities could conclude cooperation agreements or memoranda of understanding.
- The development of common guidance for enterprises in certain sectors for consumer and data protection compliance;

- A unified interpretation of the fundamental legal terms relevant for consumer and data protection (e.g. the principle of fairness) for a coherent application and implementation of law.

VII NAIH Projects

VII.1 Projects STAR I and STAR II

Together with the Vrije Universiteit (VUB) in Brussels and the British Trilateral Research Ltd (TRI), the NAIH participates in two data protection projects co-funded by the European Union.

Between 1 November 2017 and 31 October 2019, the STAR project (Support Training Activities on the data protection Reform), belonging to project REC-RDAT-TRAI-AG-2016 with number 769138 and a total budget of €357,968.50 and total EU funding: €283,439.46, compiles and tests training material (presentations and manuals) for data protection authorities and data protection officers on the GDPR.

Between 1 August 2018 and 21 July 2020, the aim of the STAR II project (Support small And medium enterprises on the data protection Reform, belonging to project REC-RDAT-TRAI-AG-2017 with number 814775 and a total budget of €560,580 and total EU funding: €448,544, is to support small and medium enterprises throughout the EU to comply with the General Data Protection Regulation. The project provides support to the appropriate enterprise taking into account the structures and needs of SMEs to establish their appropriate practices and promotes the unified application of the GDPR, cross-border cooperation, and the spread of good practice throughout the Member States. In the framework of the project, the NAIH operates dedicated email hotline (kkvhotline@naih.hu.) from 15 March 15 2019 for a year, receiving questions from SMEs in the EU. Apart from answering the questions, a manual will be compiled on the basis of issues raised and questions frequently asked by SMEs, which will be accessible and usable throughout Europe.

VII.2 Project IJR of the NAIH to support the preparations for the application of the GDPR and the implementation of its specialist tasks

In the framework of the KÖFOP 1.0.0. – VEKOP-15 priority government project based on Government Decision 1004/2016. (I.18.) Korm., the Integrated Legislation System (Integrált Jogalkotási Rendszer (hereinafter: 'the IJR ') was established to decrease the administrative burdens of budget organs.

In the framework of this project, the procedural, administrative, information technology and security development of the NAIH aligning to the changes in law related to European Union obligations.

In April 2017, the first amendment of funding contract of the IJR project under Government Decision 1585/2016 (X. 25) Korm., which includes the NAIH among the consortium partners and the tasks supported by the project and arising from the GDPR. As consortium member, the NAIH joined the IJR Project taking into account its fundamental aims and system of means.

The fulfilment of the requirements under the GDPR requires a full-scale optimization, redesigning of the IT areas of NAIH and their realization. The organizational framework of

the NAIH also has to shift towards authority operational requirements, implying a tighter and more controlled approach to operation. IT development, support and operation also has fall in line.
Under the JJR Project, the data breach notification system for data controllers was established in 2018, as the GDPR requires the notification of personal data breaches involving the damage to confidentiality, integrity, and availability of data as of 25 May 2018. The competent supervisory authority of the Member State, the NAIH, not only receives but also asses the notifications. As detailed in the above, the Authority may obligate the data controller to take measures and provide information to data subjects on the basis of the contents of the notification and information obtained. Assessing a data breach, the Authority may decide to commence an authority procedure. The data breach notification system is to support this activity.
In the framework of the IJR Project, an integrated, intelligent and decision-preparing module was developed, the IT security and organizational implementation of systems also took place in 2018.
The project is developing a system meeting Union and domestic requirements and capable of handling administration at far greater complexity and volume.

VIII Annexes

VIII.1 The Register of Data Protection Officers (DPO)

Under Article 37 (7), the data controller or processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.
Under Section 25/L (4) of the Privacy Act, the controller or the processor shall inform the Authority on the name and the postal and electronic mail addresses of the data protection officer, as well as on the change of these data and it shall publicly disclose such data.
As of 17 September 2018, the Authority made available a dedicated electronic surface for data controllers and processors to notify data protection officers.
Under Section 70/B (1) and (2) of the Privacy Act, for the purpose of keeping data subjects and controllers informed, the Authority shall publish concerning the data protection officer notified to the Authority:

- his name,
- his postal and electronic mailing address,
- the name of the controller or the processor he represents.

The data listed shall be accessible for public interest grounds.
The Authority regards notification of a DPO in the DPO notifications system as done when the DPO approves of the data sent to him by the Authority to the e-mail address recorded in the system within 15 days.
If the DPO fails to approve or confirm the notification on the basis of the e-mail sent to his address recorded in the system within 15 days, the Authority shall regard the notification as not done, and shall not publish the DPO data.

The DPO data in the public Register of Data Protection Officers are accessible to anyone at the website of the Authority (https://dpo-online.naih.hu/DPO/Search).
The Data Protection Officer notification system received 1786 notifications in 2018.

VIII.2 The Financial Management of the NAIH in 2018

2018 saw the seventh year of operation and management of the National Authority for Data Protection and Freedom of Information.

VIII.2.1 Revenue Appropriations and Performance Data in 2018

The NAIH budget for 2018, initial appropriation, was HUF 1,084,100,000 for 2017, of which the special staff appropriation was HUF 631,300,000, health and pension levies HUF 121,400,000, supplies expenses HUF 200,900,000, and the accumulation-purpose appropriation HUF 131,000,000.
The adjusted appropriation for 2018 was HUF 1,182,356,000, including the original appropriation, the balance of 2017 including commitments of HUF 67,558,000, and the others revenue of HUF 111,145,000 from the EU project STAR I and II. Additional revenues included the operation-purpose revenue of HUF 16,391,000, other services+VAT revenue of HUF 1,840,000. There was revenue from equipment sales of HUF 43,000 and BCR income of HUF 266,000. The wage compensation amounted to 1,056,000 HUF. The figures are shown in the following table:

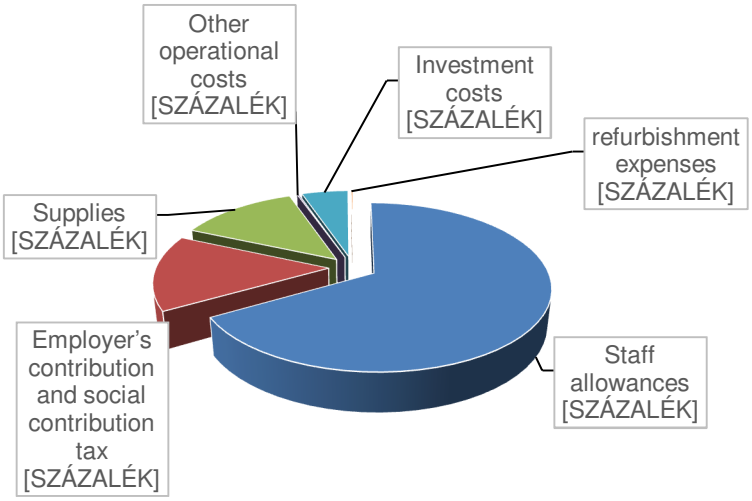
VIII.2.2 Expense appropriations and performance data

The initial budget appropriation was HUF 1,084,100,000. The adjusted expense appropriation was HUF 1,182,356,000, of which the performed special staff appropriation was HUF 629,693,000,000, performed health and pension levies were HUF 137,578,000, supplies expenses HUF120,865,000, and the accumulation-purpose appropriation HUF 48,770,000, and other operational costs were HUF 1,651,000.
The figures are shown in the following table:

Denomination	Initial appropriation thousands	Adjusted appropriation	Performance	2018 Balance Including Commitments
Initial appropriation	1,084,100			
Revenue related to the power of the state		266,000	266,000	
Services revenues		1,440	1,440	
Invoiced turnover tax		400	400	
Exchange rate profit		1,669	1,669	
Damages payed by insurer		36	36	
Other operation-purpose		14,643	14,643	

revenue				
Other operation-purpose funds (STAR I-II)		11,145	11,145	
2017 balance		67,558	67,558	
Central, governing agency subsidy	*1,084,100*	*1,085,156*	*1,085,156*	
From this: wage compensation, guaranteed wage minimum		*1,056*	*1,056*	
Total revenue appropriation:	**1,084,100**	***1,182,356***	***1,182,356***	-
Staff allowances appropriation	631,300	632,461	620,693	11,768
Employer's contribution and social contribution tax	121,400	139,833	137,578	2,255
Supplies expenses appropriation	200,400	218,925	120,865	98,060
Other operation-purpose expenses	-	1,651	1,651	-
Investment-purpose expenses	115,100	151,851	47,253	104,598
refurbishment-purpose expense	15,900	2,635	1,517	1,118
Other accumulation-purpose expenses		35,000		35,000
Expenses appropriation	**1,084,100**	***1,182,356***	***929,557***	***252,799***

Distribution of performed expense appropriations



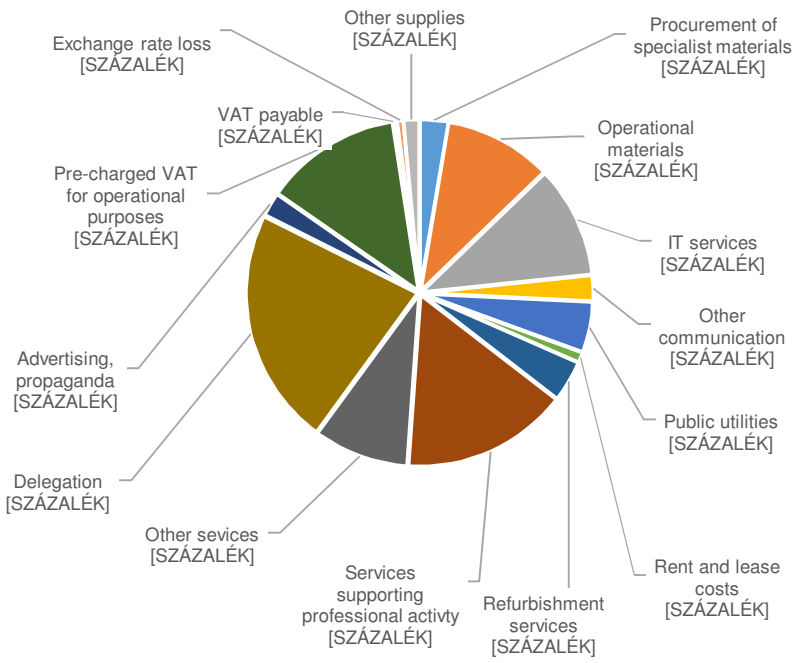
67% of the adjusted appropriations for 2018 were made in the form of personal allowances. The employer's contribution and social contribution tax was 15% of the total expenditure. The priority supplies appropriations amounted to 13% of the total adjusted budget. Investment and refurbishment expenditures amounted to 5% of the total budget. Other operating expenses were below 1%.

The balance of the Authority's core business in 2018 amounted to HUF 252 million, of which HUF 102 million including commitments and HUF 150 million were transferred back to the central budget. This is because the Authority's task and staff expansion did not result in the planned placement task in 2018, the execution of these tasks being shifted to the 2019 financial year.

VIII.2.3 The Distribution of Supplies Expenses

The following graph shows the distribution of supplies expenses in percentages.

The distribution of supplies expenses in 2018



For the most part of the material expenses, the delegation expenses are made up of HUF 27,006,000, i.e. 22%. The introduction of the GDPR in 2018 led to a significant increase in the number of journeys made in EU cooperation. Pre-charged VAT for operational purposes - because our Authority is not in a reclaiming position - is 13% of the total material expenditure, which is HUF 15,575,000. The value of the service supporting the professional activity was HUF 18,913,000. The value of operating materials was HUF 12,246,000, and for the use of IT services the Authority paid HUF 12,750,000. In total, our Authority paid HUF 5,742,000 for public utility charges.

VIII.2.4 Revenue from fines

The fine the Authority imposed and received amounted to HUF 40,236,000, which was entirely the proceeds of the central budget.

VIII.2.5. Development of the Authority's staff

The number of staff planned for 2018 was 114. The significant increase in the number of staff was carried out in several stages, as the staff allowances appropriations of our 2018 budget provided for it. Recruitment is still in progress, which unfortunately is limited by our current placement problem to be solved as soon as possible.

VIII.3 Participation of the President of the Authority at Professional Conferences and Events in 2018

VIII.3.1 International Events

31 January 2018 – Budapest – International Scientific Conference on Cyber Security in Public Service – *The General Data Protection Regulation and its Effects on Public Services*

5–6 March 2018 –Vienna – DATAPROTECTION 2018, Data & Democracy – Digital challenges for the cities - *Main Data Protection Challenges for Local Government Data Processing*

19–20 March 2018 – Geneva - Hungary's sixth periodic report on the implementation of The *International Covenant* on *Civil* and *Political Rights in simplified reporting procedure before the* UN Human Rights Committee,

27-28 March 2018 – Washington – International Association of Privacy Professionals' (IAPP) Global Privacy Summit – *round table talks*
3-4 March 2018 – Tirana – Conference of European Data Protection Authorities – *round table talks*

19-21 June 2018 – Strasbourg - 36th plenary meeting of the Committee of Convention 108 – *round table talks*

17 September 2018 – Berlin – Networked Oversight – New Approaches for Cooperation of Security and Intelligence Review Bodies in Germany and Europe – *roundtable talks*

25-26 September 2018 – Brussels – European University Association Expert Group Meeting – Open Access / *round table talks*
4-5 October 2018 – Paris - Centre for Information Policy Leadership (CIPL) - GDPR workshop on "Accountability under the GDPR – how to implement, demonstrate and incentivize it" – *round table talks*

12-13 November 2018 - Paris – IMODEV Conference - ACADEMIC DAYS ON OPEN GOVERNMENT AND DIGITAL ISSUES - *Protection of fundamental rights in the light of freedom of information*

The Academic Days on Open Government & Digital Issues is a conference organized by IMODEV at University Paris 1 Panthéon-Sorbonne, and its aim is to **bring together the various stakeholders to discuss issues related to open government globally through a scientific approach** by favouring a broad and multidisciplinary dimension. This multidisciplinary event associates law, political science, economics, management, mathematics, computer science, social science, history, sociology, environmental science, arts, and all other subjects or fields which may be related to these issues. The organization of the Academic Days is based on the experience of OGP countries that efficient cooperation

and communication between governments and civil society is of top significance in the realization of transparent and open government.

VIII.3.2 Domestic Events

16 January 2018 – Budapest, Novotel Budapest City – Conference of the Hungarian Association of Hotels and Restaurants on the New Data Protection Regulation - **The New European Data Protection Regulation and Its Hungarian Aspects**

24 January 2018 – Budapest, Bankcentrum – ***Hungarian Chamber of Commerce and Industry Information Event on the GDPR – Hungarian Aspect of the New European Data Protection Regulation***

25 January 2018 – Budapest, State Audit Office Glass Hall – ***Focus: Ethical Public Finance Leadership Training, State Audit Office and Joint Conference of the Faculty of Economics of the University of Miskolc and Book Launch Roundtable***

1 February 2018 – Budapest, Hotel Hungaria City Center – Infosphere Conference – **The New European Data Protection Regulation and Its Hungarian Aspects**

5 February 2018 – Debrecen, House of Nonprofit Economic Development Organizations – 'GDPR - EU General Data Protection Regulation - Legislation affecting the Life of Every Business' – Conference organized by the Chamber of Commerce and Industry of Hajdú-Bihar County – **The New European Data Protection Regulation and Its Hungarian Aspects**

14 February 2018 – Budapest, Petőfi Sándor Community Centre –Training for members of the Hungarian Association of Pharmaceutical Manufacturers on the EU General Data Protection Regulation – **The New European Data Protection Regulation and Its Hungarian Aspects**

15 February 2018 – Budapest, MÜPA – Medical Tribune GDPR – 'The Sick, the Doctors, Industry, Data, and Data Protection' conference – **The New European Data Protection Regulation and Its Hungarian Aspects**

27 February 2018 – Budapest, Marriott Hotel – Portfolio Conference, 'GDPR Summit 2018 data processing rethought' –*The* GDPR ***here at home– the most important changes in background legislation***

2 March 2018 – Budapest, Danubius Hotel Arena – 2018 ***GDPR Comprehensive - Data Protection for Beginners and Advanced Program – Renewal of Data Protection Regulation***

12 March 2018 – Szeged - ***EU General Data Protection Regulation - Legislation affecting the lives of all businesses" organized by the Csongrád County Chamber of Commerce and Industry and the Institute of Labour Relations and Social Security Training at the University of Szeged - GDPR from the Business Sector Viewpoint***

13 March 2018 – Budapest – Wolters Kluwer Specialist Conference: 'GDPR in Practice' - **The New European Data Protection Regulation and Its Hungarian Aspects**

13 March 2018 – Budapest, Fortuna Ship Nelson Room Association of Hungarian Detectives, Club Day**– The New European Data Protection Regulation and Its Hungarian Aspects**

21 March 2018 – Budapest, Budapest Music Center – Danubian GDPR Summit Conference – **The Limits of Publicity and Privacy**

21 March 2018 – Budapest, Groupama Aréna – Microsoft Future Decoded Conference–***What should be done for compliance from the authority's point of view? What will and how will the authority supervise?***

22 March 2018 - Balatonakarattya – Hungarian Army Data Protection Conference - **Tasks and competences of the NAIH as of May 25, 2018 and the status and activities of the European Data Protection Board**

4 April 2018 – Budapest, Lurdy Ház – "How to Meet the GDPR Requirements?" - a Professional Day organized by Menedzser Praxis Publisher - **Resolutions, Recommendations, Sanctions – Advice on how to Meet NAIH Expectations**

11 April 2018 – Budapest, Hotel Hungaria city Center – Infosphere Conference – **The New European Data Protection Regulation and Its Hungarian Aspects**

14 April 2018 - Hollókő, Hotel Castellum – ***Professional Conference organized by the Equal Treatment Authority - Provisions Relevant to EBA in GDPR and the planned Amendment of the Privacy Act***

17 April 2018 – Szombathely, Agora Savaria Cinema – 'GDPR - DATA PROTECTION CONFERENCE - Basic Information on the Application of the New Data Protection Regulation' conference organized by the Department of Commerce and Industry of the County of Vas - **The New European Data Protection Regulation and Its Hungarian Aspects**

7 May 2018 – Budapest, Hotel Hungaria City Center – Infosphere Conference – ***Application of the new data protection regulation in Hungary, the cornerstones of preparation and control, expected sanctions***

9 May 2018 - Budapest, Aquaworld Resort Budapest – Cyber Risks Conference – *Fasten your seatbelts* ***… - The GDPR and Data Protection checklist***

10 May 2018 - Budapest – National Judicial Office, Hungarian Justice Academy– Data Protection Professional Day – ***Milestone in Data Protection, the GDPR is entering into force***

14 May 2018 - Kecskemét, Neumann János University, Chancellor's Office– Data Protection Professional Day p - **The New European Data Protection Regulation and Its Hungarian Aspects**

15 May 2018 - Budapest, Villa Bagatell –AmCham exclusive GDPR Breakfast – ***Roundtable Talks***

15 May 2018 - Budapest, Aquincum Hotel Budapest – joint official consultation of the Hungarian Brand Association and the National Commercial Association **- The New European Data Protection Regulation and Its Hungarian Aspects**

17 May 2018 - Budapest, King Sigismund University – Competitiveness 2018 Conference – ***Data Protection Challenges in a Digital World***

22 May 2018 - Siófok, Prémium Hotel Panoráma – First National Conference for Private Security– **The New European Data Protection Regulation and Its Hungarian Aspects**

31 May 2018 - Balatonkenese – National Competition Authority – Professional Day – ***The GDPR's consequences on internal data processing***

7 June 2018 - Budapest, Hotel Griff – Accreditation World Day organized by the National Authority for Accreditation – The Creation of a More Secure World– ***The GDPR, the security of our personal data***

7 June 2018 - Budapest, Magyar Telekom Headquarters – ISACA Conference – **The New European Data Protection Regulation and Its Hungarian Aspects**

14 June 2018 - Budapest, *Institut* français – Personal Data Protection - Big data - French-Hungarian-European Conference - "Connected health": ethical and legal issues related to the protection of interconnected personal health data - **Protecting health data**

18 June 2018 - Budapest, Dunacorso Restaurant – 10th Annual Sedona Conference International Programme on Cross-Border Data Transfers and Data Protection Laws – ***Roundtable Talk***

22 June 2018 - Budapest, University of Physical Education – Professional Conference organized by SPORTJUS Hungarian Association Sports Lawyers– ***The GDPR and sports***

7 September 2018 - Debrecen – The Annual Conference of the Hungarian Association of Economists – **The Experiences of Applying the New EU Data Protection Regulation**

11 September 2018 - Deloitte Legal Law Firm – Professional Breakfast 'Modern Technologies and Employment' – **roundtable on workplace data processing and the criteria of the authority**

19 September 2018 - Budapest, Hotel Hilton – Portfolio – GDPR 2.0 Conference – **Changes in Background Regulation – Schedule and Sectoral Negotiations**

27 September 2018 **–** Budapest, Groupama Aréna – ITBN Conf-Expo – **roundtables on the first experiences of applying the *GDPR***

1 October 2018 **–** Balatonföldvár, Sceptre Training Centre and Hotel – Ministry of the Interior National Catastrophe Protection Directorate Third Police Data Protection Conference – ***The Relation between the Amended the Privacy Act and the GDPR***

1 October 2018 **–** Siófok – 15th Insurance Conference and Exhibition – ***The Relation between the Amended the Privacy Act and the GDPR***

2 October 2018 **–** Budapest – 'The Impact of the Internet on Children and Young People' conference sponsored by the International Child Safety Service and the European Union 'Safer Internet Programme' - **Education - Child Protection - Community Network**

9 October 2018 **–** Budapest, Rozmaring Restaurant – lecture and consultation on the importance, interpretation and of the GDPR – T**he New European Data Protection Regulation and Its Hungarian Aspects**

30 October 2018 **–** Budapest, Láng Community Centre – ITOSZ, 'GDPR READY 2018 – Specialist Conference' – T**he New European Data Protection Regulation and Its Hungarian Aspects**

5 November 2018 **–** Budapest– Professional Data of the Catholic Charity Service – T**he New European Data Protection Regulation and Its Hungarian Aspects**

7 November 2018 **–** Budapest – Zukunft Personal Hungary Conference – ***Panel discussion on the GDPR***

7 November 2018 **–** Budapest– Internal Affairs Scientific Council, International Multidisciplinary Conference on Security - **Data Protection, Data Security in Public Service**

VIII.4. Authority Events in Pictures

The Berlin Working Group session in Budapest on 9 April 2018

The founding meeting of Project STAR II in Budapest 10 September 2018

Freedom of Information Case Handling Workshop session in Budapest on 26 November 2018