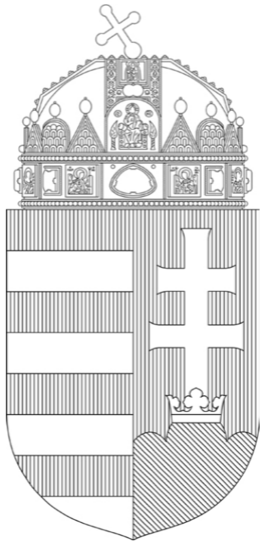
Annual report of the

National Authority for Data Protection and Freedom of Information (NAIH)

2017

National Authority for Data Protection and Freedom of Information
Budapest, 2018



Preface

To the Reader

In the life of EU data protection authorities, the year 2017 was clearly spent in the spirit of preparation. After four years of preparation, the two elements of the EU Data Protection Reform Package, the GDPR and the Police Directive, were adopted in 2016, and both EU acts will enter into force in May 2018, with the difference that while the Regulation is directly applicable, the rules of the Directive must be transposed into the national laws.

With 2018 an exciting time begins; the norms of data protection will be in a sense redoubled: community norms in a broader sense will be applied in a mandatory, uniform system, but there will be privacy complaints where the primacy of national law—and national differences—will remain either because this is allowed for by EU legislation or because they are areas not covered by EU law. Think of data processing operations for the purposes of national security and of the courts acting in their judicial capacity.

The EU data protection reform is intended to respond to the challenges of rapid technological progress and globalization, which promotes, helps, and in no way inhibits economic progress. Uniform application of data protection rules prevents abuses, 'scams', data controllers will no longer be able to choose between EU countries for cost reduction or easier terms, as expectations and sanctions—from a data protection perspective—will be the same or similar across the EU.

At the same time, we may face interesting and exciting challenges in the future as there are categories and factors in the application of law that are strongly dependent on the legal and cultural background of the country. Such as 'fair trial', the best interests of the child or the assessment of the circumstances of data processing affecting 'rights and freedoms of natural persons'.

The expectations are high regarding the new regulation on all sides, yet, as the head of the Hungarian data protection authority, I am convinced we are ready to fulfil our tasks.

Budapest 1 March 2018

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, 2017 was the sixth year of its operation. As in previous years, we show by way of data and charts how the tasks of the Authority were fulfilled, what changes and trends could be observed in the content and volume of the notifications we received, the challenges we faced in the last year. The diversity, numeracy, and diversity of our tasks can be well illustrated by the objective, yet diverse and highly informative overview of numbers and data, giving a specific picture of the past year.

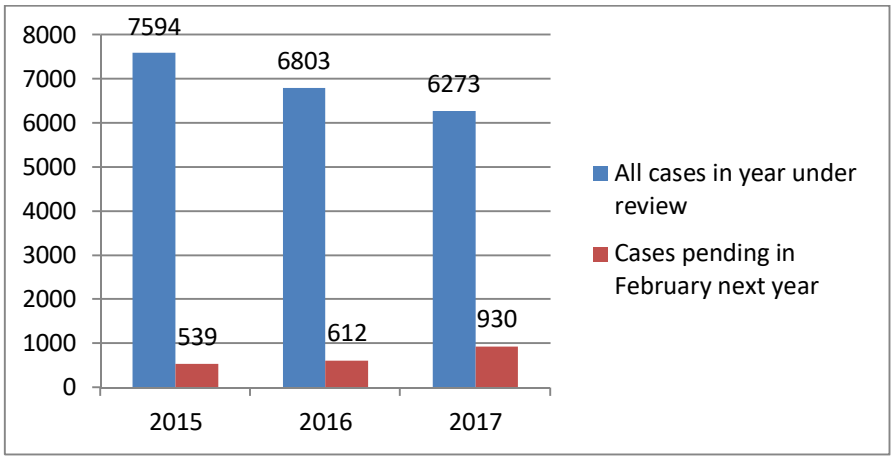
In 2016, the electronic registry book contained a total of 6,273 cases, 530 cases less than in the previous year. The obvious reason of the decrease is that notifications to the Data Protection Register increasingly come electronically which does not require registration. In the Data Protection Register in 2017, we processed more cases, a total of 26,728, than any time before, and 'only' 2,522 required filing. The detailed description and analysis of the data will show that there was no significant decrease in the number of cases involving other meaningful tasks of the NAIH; indeed, in certain areas quite to the contrary, marked increase could be observed.

Out of the cases filed in 2017, data protection administrative proceedings started in 68 cases. Out of 6,273 cases, 2,792 were treated as matters of investigation. In comparison with the previous years, the number of investigations increased by 130.

Other files were related to the tasks set out in Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (hereinafter the 'Privacy Act'), to matters related to the data protection register, activities related to legislation, delivering opinion on legislation, international affairs, data protection officer's conference, data protection audits, and BCR cases, cases related to control of classified data, files and administrative documents related the Authority's internal affairs, operations, and management. Details of these data protection administrative proceedings are further particularised in the chapters on Data Protection and Control of Classified Data.

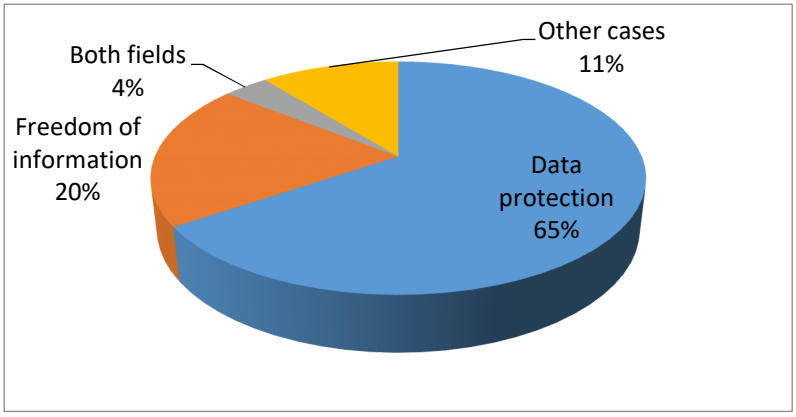
Of the ongoing cases in 2017, 930 cases were not finalized by of 1 February 2018, 14% of all cases, i.e. a total of 688 cases, were re-registered in 2017 from 2016.

Registered and Pending Cases of NAIH between 2015 and 2017



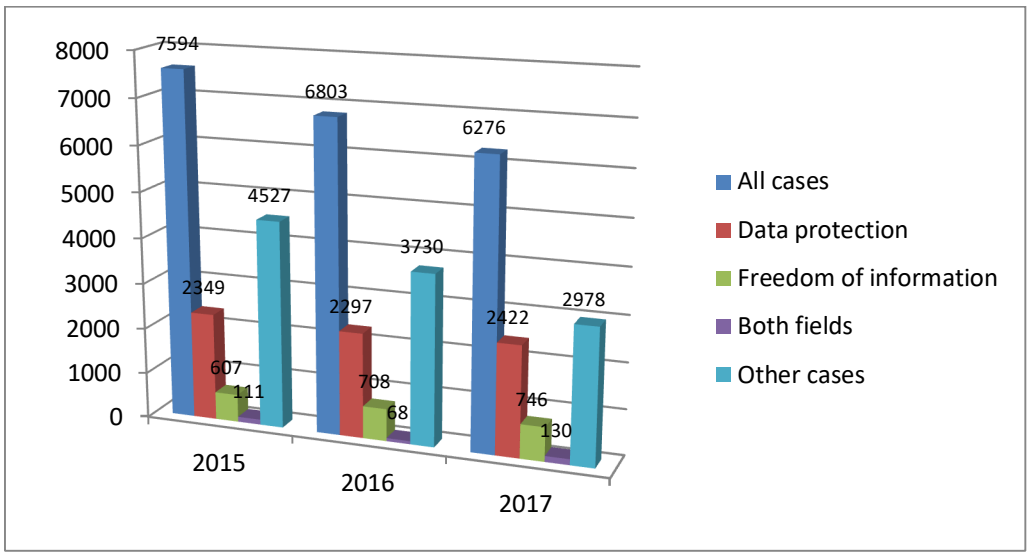
Under the Privacy Act, the primary duty of the NAIH is to control and enhance the enforcement of the right to protect personal data and rights to access and disseminate data of public interest and data public on grounds of public interest. The following diagram shows, from the point of view of information rights, how the individual incoming files affected the protection of personal data and the disclosure of data of public interest. In accordance with the practice of previous years, this diagram does not include cases related to the management of the Data Protection Register (a total of 2,575 cases concern the Data Protection Register), as they do not directly affect any of the fundamental rights, or, because of their significant number, the actual fundamental rights composition would disproportionately change.

Distribution of Cases by Informational Rights in 2016
(Without the cases related to Data Protection Registry)



The breakdown of our cases by information rights is as follows: 2,422 cases (65%) concern data protection concerns (2016: 2,297); 746 cases (20%) concern freedom of information (708 in 2016) (2016: 68), 130 cases (4%) concerned both fundamental rights (68 in 2016); 400 other cases (11%) concern the Authority's other duties (479 in 2016); and, not taken into account here, 2,575 cases (3,251 in 2016) concern the Data Protection Register. As mentioned in the introduction, the number of filed cases concerning the Data Protection Register was 676 less, but the number of cases involving information rights increased. 24% of the cases—all together 876 cases, 100 more than in the previous year—concerned in some way or another the fundamental right to access and disseminate data of public interest and data public on grounds of public interest. Overall, this means that the number of cases involving data protection and data disclosure has increased. As far as rates are concerned, cases concerning freedom of information increased by 2% over the previous year.

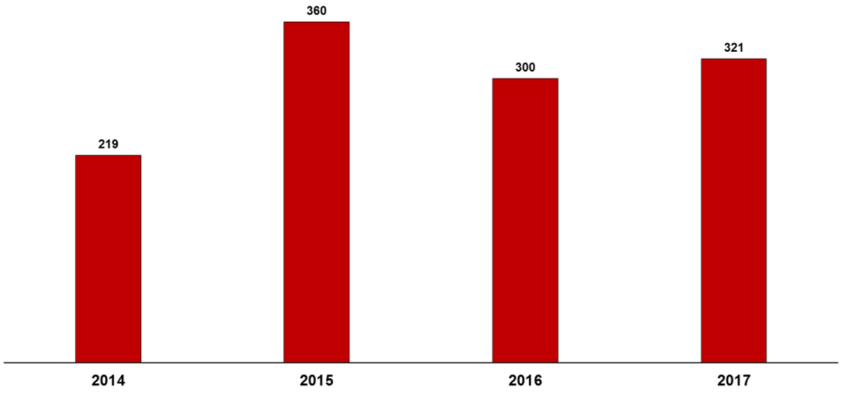
Distribution of Incoming Files by Fields between 2014 and 2016
(Other cases also includes cases related to Data Protection Registry)



In 2017, we had 321 cases of delivering opinion on legislation, which means 21 more than the previous year.

The Authority operates a legislation monitoring system, and regularly follows codification activity relating to information rights, and, if necessary, ex officio delivers its opinion on draft legislation unsent to it or modifications proposed to bills already on the parliamentary agenda.

Reviewed Draft Bills between 2014 and 2017



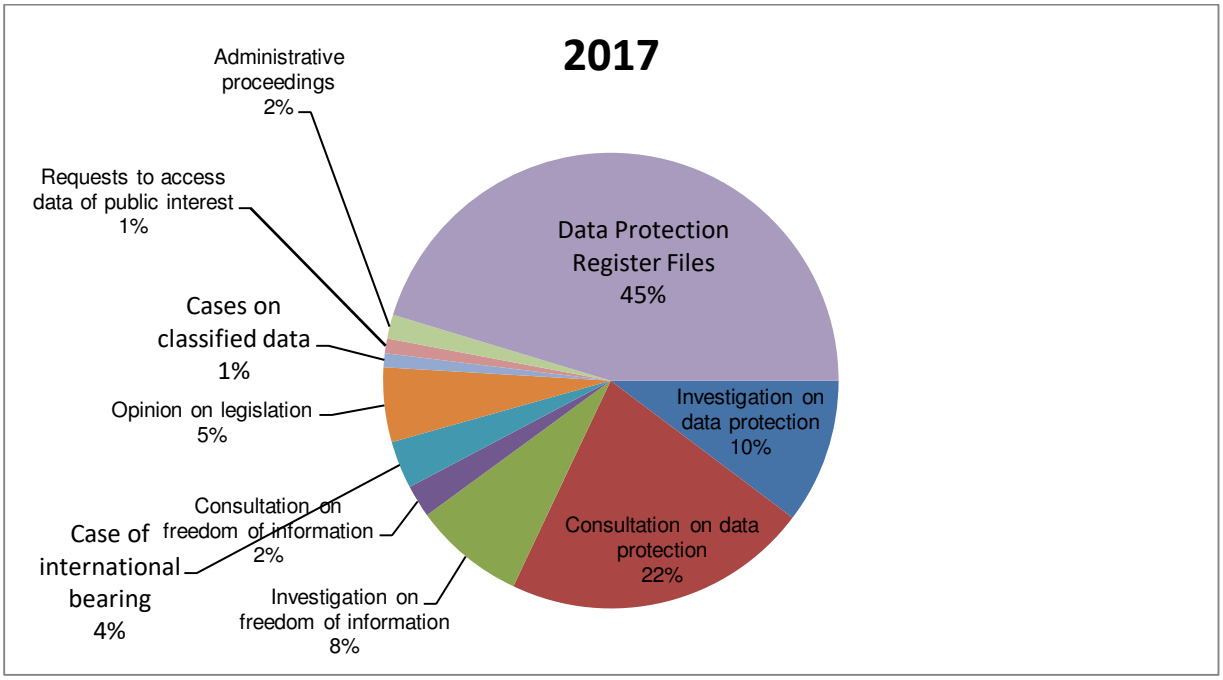
In the cases we examined in 2017, we initiated a total of 33 amendments to law, of which 31 concerned data protection and 2 the disclosure of data of public interest. A total of 581 observations were made in our opinions on legislation. The activities of the NAIH concerning legislation are set out in detail in Chapter VIII.

Sometimes our competence cannot be determined on the basis the subject matter and the content of notifications sent to the Authority; in some of these cases, the notification is transferred to the competent bodies, which took place in 31 cases, of which three cases were transferred to the Commissioner for Fundamental Rights.

Of the applications requesting the initiation of investigation proceedings, 231 concerning data protection, and 90 concerning disclosure of public data were rejected. The number of rejected cases increased by 37 compared to the previous year.

The following diagram illustrates how the proportion of cases filed with the Authority requiring substantive action, proceedings, and response related to each other.

Substantive cases 2017



A total of 1,033 cases were brought under effective investigation, which is 43 cases more than in 2016. Of these, 585 (56%) concerned data protection, and 448 (44%) freedom of information. This year again, there was a tendency of increasing the number of investigations in both information fields, and it should be emphasized that the number of notifications generating investigations on freedom of information was 40 more than in the previous year and that their share increased by three percent compared that of data protection cases.

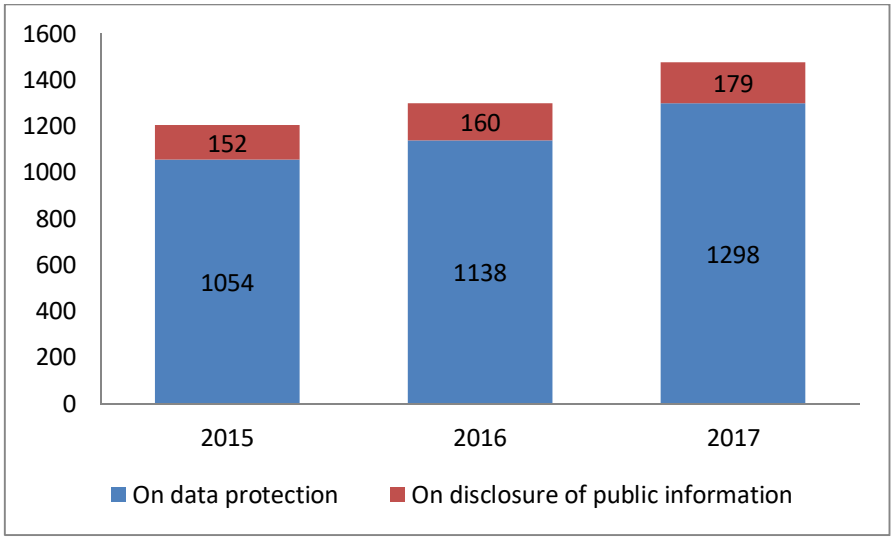
Out of the 1,033 cases investigated up to January 2018, we found unlawful data processing practices in a total of 564 cases. The number of infringements increased by 82 compared to 2016. Out of the cases where infringement was established, 279 concerned the processing of personal data and 285 to the disclosure of public data. The number of violations established increased in both data protection cases (30) and freedom of information cases (52). Thus, 2017 was the first year since the establishment of the Data Protection Commissioner in 1995 that the Hungarian institution supervising data protection and freedom of information found more infringements concerning the disclosure of public information than infringements of right to informational self-determination in a given year.

In addition to the Authority's investigations, it is important to highlight the 1,370 consultation cases in which substantive legal opinions were delivered, and the number of which is growing continuously every year, increasing by 72 in 2017.

The steady increase in the number of consultation cases is due to the short time required to prepare for the application of the GDPR (General Data Protection Regulation) and to answering questions that require a correct interpretation of the regulation. In addition, it is related to the Authority's consistent practice of law enforcement, proceedings, and fining. Consultations, delivery of opinions, and the provision of information on best data-processing practices also contribute significantly to our efforts in promoting the enforcement of information rights under Article 38 (2) of the Privacy Act and their being implemented in everyday practice.

Out of the consultation submissions, 1,237 concerned data protection and 133 disclosing data of public interest and data public on grounds of public interest. In our consultation cases, there was a clear trend that the number of requests concerning data protection was rising again and the number of consultations on disclosure of information was decreasing. The details of consultation cases and the trends are shown in the graph below.

The Number of Submissions Concerning Information Rights between 2015 and 2017



The Authority also receives notifications that do not meet the conditions for initiating investigation proceedings, or, in the examination of the consultation cases, it could also established that a data controller's practice did not fulfil legal requirements, and delivering our opinion prevented an unlawful situation or its direct threat. In 2017, we found and prevented infringements of law in 105 cases, 61 data-protection and 46 cases of freedom of information, which was 31 cases more than in the previous year. In this group, the number of cases involving freedom of information increased (33 cases).

Other Priority Cases

A total of 58 investigations concerned the processing of qualified personal data or data of public interest, and the number of our confidentiality cases decreased compared to the previous year. Chapter IX deals with investigations of cases of control of classified data.

In 2017, we had a total of 116 cases of international bearing, and 74 other cases also had a foreign aspect (e.g. notifications concerning EU or third-country data controllers or data processors and international data transfers). International issues and activities are described in chapter X of the report.

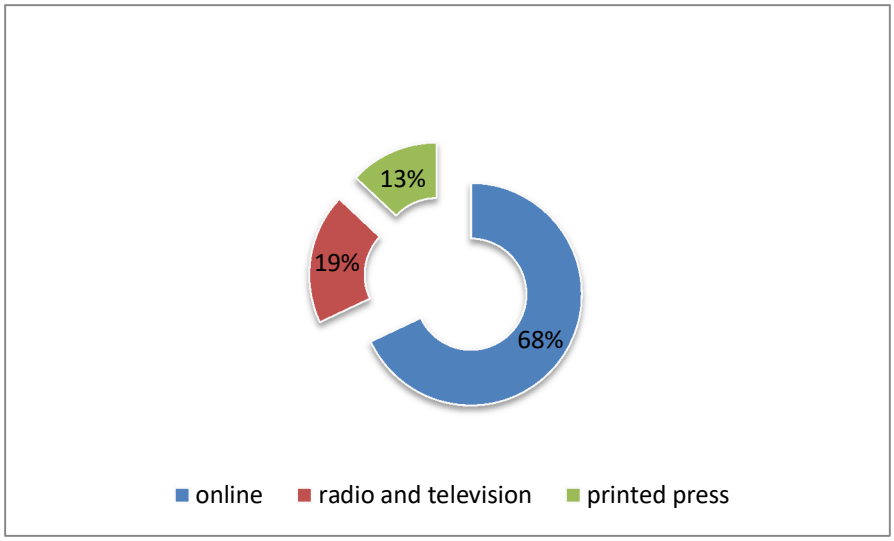
The number of data-protection audit cases was 15, out of which 7 audits were completed in 2017. The number of files on Binding Corporate Rules (BCRs) was 62. The total number of cases of BCR approval by the Authority was 14. Audit and BCR cases are discussed in Chapter VI.

The NAIH received 53 requests for data of public interest in 2017, all of which it answered. The number of data requests increased slightly (+6) compared to the previous year.

I.2. The Media Presence of the National Data Protection and Information Authority

By way of summary, between 1 January 2017 and 31 December, the NAIH disclosed a total of 4,284 news items to the media, which was more than 2000 less than in the previous year. Of the media types, online media covered the Authority's activity the highest number of times (2926; 68%). The printed press featured the NAIH in 537 cases (13%), the electronic media in 821 cases (19%).

The proportion of NAIH's appearances in the various media in 2017



II. The first 25 Years of Hungarian Data Protection from the Data Protection Act to the GDPR

The 25-year history of Hungarian Data-protection Regulation

At the beginning of this historical outline, mention should be made of the fact that the rule-of-law constitution related to the change of regime in 1989 broke with the state-centric approach, as it essentially intended to limit not the state's citizens but the state itself. Fundamental constitutional rights, on the one hand, ensure the freedom of the citizen against state power, and, on the other hand, they require the state to actively enforce these rights. In the spring of 1990, a provision was introduced to the amended Constitution (on the German example) which prohibited the amendment of the substantive content of the fundamental rights. The burden of shaping the practical interpretation of this latter definition rested on the Constitutional Court. The most important and pioneering action in the field of data protection was the AB Decision 15/1991 (IV. 13) which declared the universal use of the personal identification number as unconstitutional, and defined the right to informational self-determination. Information rights were provided for by the chapter on fundamental rights and duties in the Constitution.

In addition, the most important step in the Hungarian data protection regulation was adoption of the Data Protection Act 25 years ago in 1992. 'The adoption of a general law should also be undertaken, because it is necessary to outline somewhere the value system that specific laws may detail but not curb. The model role of the informatics law is all the more necessary, because there is no other legislation on the agenda fundamentally touching the rights of citizens. It should also be noted that the actual enforcement of the rights of access and rectification, etc. will be established by judicial practice. This is usually typical or even necessary where personality rights are concerned,' wrote László Sólyom in 1988, while the informatics law was being prepared.[1]

The first Hungarian data-protection law (Act LXIII of 1992 on Personal Data Protection and the Publicity of Data of Public Interest) had had its own precursor. With the approval of the President of the Council of Ministers, the Department of Computing and Applied Statistics of the Central Statistical Office had had a team of experts to draft a Data-protection Standard in the early 1980s. At this time, the processing of the data of citizens by state organs was not restricted by any law, and organized and public data collection was mostly restricted to census activities by the state. It was no coincidence that the Constitutional Court declared the relevant law manifestly unconstitutional and annulled it in 1991. In 1989, the Council of Ministers adopted a resolution on drafting a bill on the processing of personal data and disclosure of information of public interest, which was progressive in terms of information rights, but still in the spirit of 'socialist democracy'. At the beginning of 1990, the draft bill was completed, and, as a result of the opinions received during the administrative consultation, an independent monitoring body, the institution of the data protection commissioner, already appeared.

In the spring of 1992, the government submitted bill no. 4544 prepared by the Ministry of Justice, requesting an urgent hearing by Parliament, with a total of 140 amendments being received (most of which were rejected at last decision). The act was finally promulgated on 11 November 1992, and entered into force six months later.

Unlike European regulations, the Data Protection Act was not a 'data protection' standard, but it was a law on information rights, that is, in addition to the protection of personal data, it included the guarantees of freedom of information, and empowered the Data Protection Commissioner to supervise the two freedoms—as special ombudsman, starting to operate from 1995. 'From the outset, starting to process the first citizens' complaints, the Data Protection Commissioner's Office constantly experienced the very positive fact that the members of Hungarian society—regardless of their financial situation or education—are 'sensitive' and committed to protecting their personal data, and confidently contact this special rights-protection organization for help and information.'

In 2000, international recognition was achieved with the recognition of 'adequate level of protection' and with the 2002 pre-accession, EU expert report on the situation of data protection in Hungary. With accession to the EU, a transition period began, when the 'soft' means of the Ombudsman began to be reinforced by amendments of law, and the aim was transformation to be an authority.

'The new Fundamental Law revised the system of protecting fundamental rights in 2011. An independent data protection authority, in line with international requirements, could operate only completely independently from the organization of the unitary fundamental rights commissioner. From 2012, the National Authority for Data Protection and Freedom of Information has operated on the basis of Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (the Privacy Act), and has received notifications and requests on data protection and the freedom of information on that basis.

[1] Sólyom, László: 'Adatvédelem és személyiségi jog' in: *Világosság,* 1988/1 (January).

From May 2018, however, a new period begins in Hungarian institutional data protection, as the primacy of national regulation ends, and a single, direct-effect EU regulation takes over the primary (though, it should be added, not exclusive) regulatory role. Currently, all EU Member States are preparing to respond to this challenge.

III. The GDPR—Stages of Preparation for the Application of the EU Regulation in 2017

(Abridgement)

The report presents the opinions of the Article 29 Working Group under Directive 95/46/EC that assist the preparation for applying the GDPR in respect of data portability (2), data protection officer (3), identification of the competent lead supervisory authority (4), data protection impact assessments (5), administrative fines (6), data processing at work (7), reporting personal data breaches (8), data protection impact assessments (9), NAIH authorisation powers under GDPR (10), codes of conduct (11), authorisation powers concerning data transfer to third countries (12), certification (13), practical issues of enforcing the GDPR (14).

IV. The Police Directive

(Abridgement)

The implementation of DIRECTIVE (EU) 2016/680 into Hungarian law—by way of amending the Privacy Act—has not been completed. This chapter of the Report sums up the requirements of the Directive.

[…]

With regard to the future application of the Directive, a complainant detained in a prison in Hungary turned to the Data Protection Authority. Inmates may legally store in their cells, with the consent of the prison authorities, electronic storage media (e.g. pendrives, DVDs) for documents and correspondence from official bodies and their attorneys-at-law in electronic form. Such media are regularly inspected by the prison's computer technician for prohibited content. After such a check, the complainant got his pendrive back with data belonging to other inmates (court and attorney-at-law's correspondence). In addition, the pendrive had recordings of other inmates made by the prison's camera surveillance system. The NAIH contacted the prison, which investigated and acknowledged the incident. In this case, it should be noted that it qualifies as personal data breach under the Privacy Act currently in force, and such breaches shall have to be reported to NAIH upon the entry into force of the provisions of the Police Directive.

V. Data Protection

V.I. Statistics

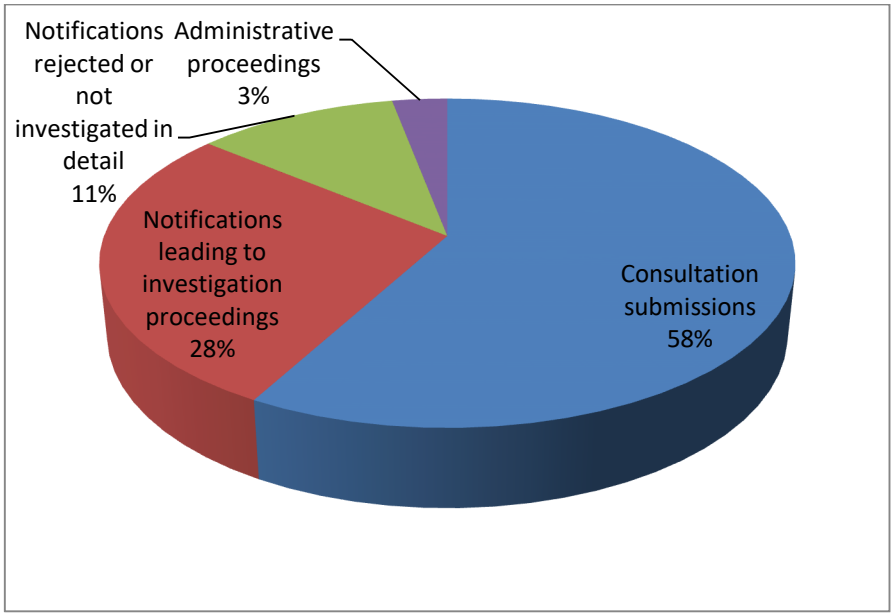
In 2017, the management of data protection cases was carried out in accordance with the established procedural order but also in the spirit of the new act on general administration procedure and the preparation of the new General Data Protection Regulation.

58% of data protection cases were of a consultation type last year. Consultation submissions are usually characterized by the fact that a citizen or a data controller seeks advice or information about a case concerning data processing he or she describes, or to obtain an opinion by the Authority on its lawfulness.

The information and opinions formulated in these cases have an important role to play in enhancing the law-abiding conduct of data controllers and thus effectively contributing to the prevention and elimination of breaches of law, or shaping best practices, and calling the attention of data subjects to individual enforcement rights, the possibility of requesting information, alteration or erasure of data, the importance of data-protection rights consciousness.

In 2017, the proportion of investigation proceedings compared to all cases was 28%, an increase of 22% compared to the previous year. The Authority found infringements of law in 47% of the data-protection notifications leading to investigation proceedings.

Data protection cases in 2017



Also in 2017, the number of new investigations that were pending and the number of new investigations started in 2017 were higher than the number of administrative proceedings. Prior to the initiation of administrative proceedings, we took into account the experiences of any examination history and the cases mandatory under the Privacy Act. In many cases, the administrative proceedings covered the controller's entire data processing related to the subject of the complaint in addition to the examination of individual complaints, so the Authority also examined the general data processing practice of the data controller. In the course of administrative proceedings, establishing an accurate knowledge of the data processing and the facts of the case, as well 'regulatory demonstration' of law infringement are carried out under more formalized procedural rules, hence these procedures take longer.

In the course of 2017, 17 administrative proceedings were initiated, thus, together with proceedings pending from the previous year, a total of 68 were in process the last year. The Authority launched fewer new administrative proceedings compared to 2016. One of the reasons for this was the preparation for the General Data Protection Regulation, which was a burden on not only the Authority but also the data controllers.

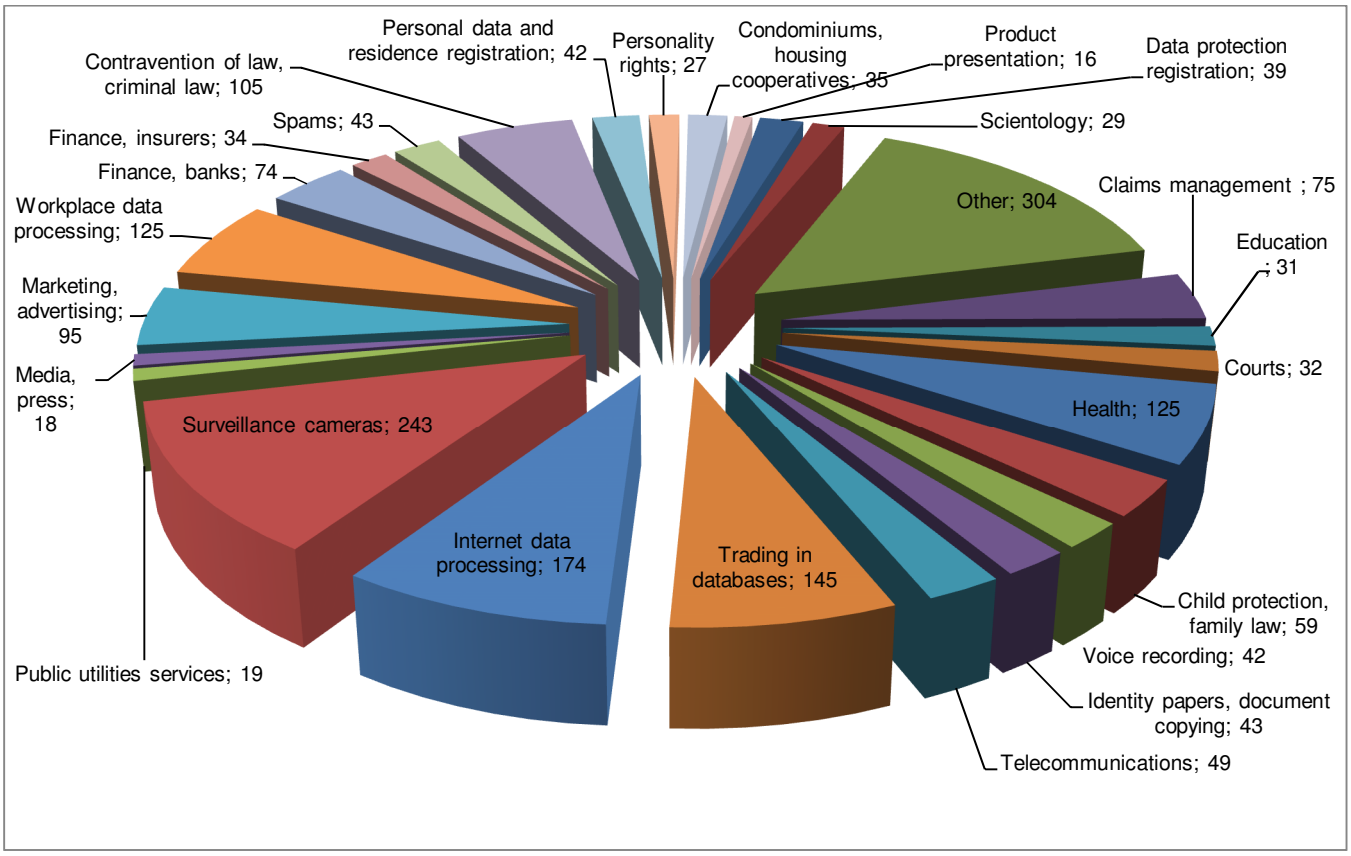
The Authority included among the ongoing administrative proceedings the cases with a 2017 file number, in which the proceedings were aimed at verifying the enforcement and execution of decisions made in previous years. The final closure of these cases was delayed by lacking or inadequate enforcement.

In 2017, the Authority made decisions in a total of 27 administrative proceedings, including the 20 cases pending from previous years. In its decisions, the Authority could impose fines in only 14 cases due to the fact that small and medium-sized enterprises were the data controllers. Until drafting the report, the Authority issued 4 further decisions, in two of which it fined breaching data controllers.

In 2017, the Budapest Court of Public Administration and Labour issued verdicts in reviewing 20 decisions of the Authority that were substantive and appealable by way of remedy. The review cases were concluded in 15 cases with the Authority prevailing and in two cases of partially prevailing, and three cases were lost by the Authority. Judicial decisions were made, with 3 exceptions, regarding the revision of decisions made in previous years.

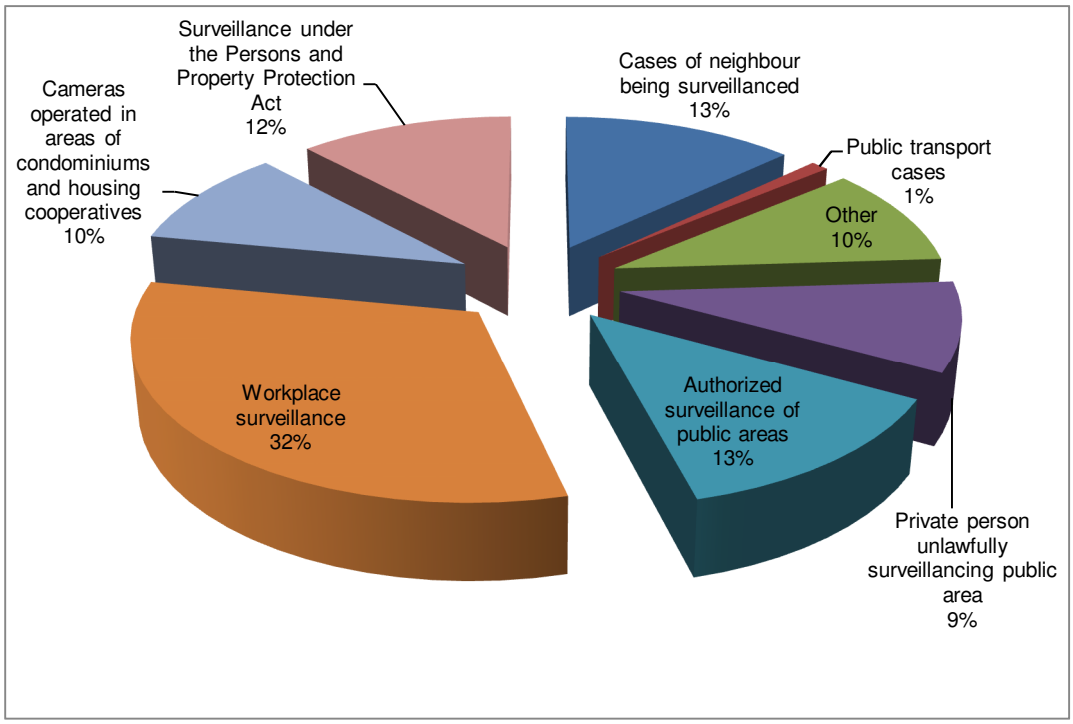
Data protection submissions—complaints, reports, and requests for consultation—concern a wide range of questions of public administration and privacy, which means that a wide variety of letters touching many fields are addressed to the Authority. An application for an inquiry or for an answer to a question might involve several areas. The chart below shows the number of submissions received touching various areas.

Frequency of submissions by types of case in 2017



The Authority received a large number of submissions and consultation requests in 2017 concerning surveillance camera data processing systems. ‘Surveillance camera’ cases were the most common type of case this year; in proportion, most submissions were filed on this subject.

Surveillance-camera cases 2017



As can be seen from the above diagram, submissions for camera observation are diverse and can be categorized into several categories. There are many cases of overlap in the case types, as in the previous year; it was often the case that an investigation was conducted where the data controller against whom the complaint was filed monitored public space and neighbouring real estate simultaneously.

V.2. Submissions Requesting Information on the Enforcement of the GDPR

In 2017, in order to prepare for the application of the new General Data Protection Regulation (GDPR), several data controllers requested the Authority to provide information on the interpretation of the provisions of the GDPR.

An EU Regulation is a legal instrument that applies directly—without transposition into national law—in all Member States. The GDPR is thus also directly applicable, but it allows several derogations from its provisions, or it requires the national legislator to enact additional clarifying legislation. The amendments of law needed for the implementation of the GDPR in Hungary being under preparation last year and now, the Authority based its provision of information on data controllers' questions on the text of the Regulation and on the opinions issued by the Article 29 Working Party.

The main questions by data controllers and the responses given to them were as follows:

1) In the case of consent-based data processing, must new consent be sought from data subjects for processing existing databases with a view to the provisions of the GDPR?

Under Recital (171) of the GDPR, processing already under way on the date of application of the Regulation should be brought into conformity with the Regulation. Where processing is based on consent, it is not necessary for the data subject to give his or her consent again—if the manner in which the consent was been given is in line with the conditions of the Regulation—to allow the data controller to continue such processing after the date of application of this Regulation. Should the consent not meet the requirements under the Regulation, articles 7 and 8 in particular, consent has to be obtained again.

2) By issuing a new notice complying with the provisions of the GDPR, can data processing that has been under way for years be continued without obtaining new consent?

With regard to transparent provision of information as provided by Article 12 (1) of the GDPR, notices on data processing must be reviewed. However, revised notices cannot make up for consent by data subjects if their consent does not meet the requirements of the GDPR.

3) Does the GDPR include any exemptions for small enterprises?

According Article 30 (1) of the Regulation, the data controller or processor shall make records of its processing activities in order to prove its compliance with the Regulation. Article 30 (5) of the GDPR exempts enterprises employing fewer than 250 persons if the processing they carry out is not likely to result in a risk to the rights and freedoms of data subjects, the processing is occasional, or the processing does not include special categories of personal data.

4) Will the data protection officer need any specialized data-protection training?

The data protection officer must be appointed on the basis of professional aptitude, an expert-level knowledge of data-protection law and practice in particular, and the ability to fulfil the duties under Article 39 of the GDPR. The required level of expertise shall be established on the basis of the type of processing carried out by the data controller or processor, as well as the protection required by the personal data they control.

5) Will state-owned bodies with public service functions need to employ data protection officers?

GDPR does not define the concept of 'public authority or body'. In Article 37 (1), it does determine cases in which the data controller and the processor shall designate a data protection officer.

In determining this, Guidelines WP243 of the Article 29 Working Party provides assistance (http://naih.hu/29-es-munkacsoport-iranymutatasai.html). On this basis and GDPR definition lacking, the concept of public authority or body must be defined under national law. The Guidelines also states: 'A public task may be carried out, and public authority may be exercised not only by public authorities or bodies but also by other natural or legal persons governed by public or private law, in sectors such as, according to national regulation of each Member State, public transport services, water and energy supply, road infrastructure, public service broadcasting, public housing or disciplinary bodies for regulated professions.' And though, under the GDPR, these are not required to appoint DPOs, the Working Party recommends private-law bodies to do so as good practice.

The GDPR allows only a small range for legislation by Member States on data protection officers (see Articles 37 (4) and 38 (5)), thus determining whether the appointment of a data protection officer is required or not by a public authority or body is to be based on the GDPR.

6) When the Authority finds a breach of law in the course of its investigations, shall it always impose a fine, or will it have other appropriate measures at its disposal?

Recital (148) of the GDPR provides that in order to strengthen the enforcement of the rules of the Regulation, penalties including administrative fines should be imposed for any infringement of this Regulation, in addition to, or instead of appropriate measures imposed by the supervisory authority pursuant to the Regulation. If the fine likely to be imposed would constitute a disproportionate burden to a natural person, a reprimand may be issued instead of a fine.

Recital (150) of the GDPR also states that in order to strengthen and harmonize administrative penalties for infringements of this Regulation, each supervisory authority should have the power to impose administrative fines. The GDPR defines several circumstances to be weighed when imposing a fine. Article 83 (4)–(6) provides for more factors to be considered than under Hungarian regulations currently in force.

7) May the Authority suspend the operation of a company if it has been found to have infringed any provisions of the GDPR?

The GDPR and the Privacy Act provide for the legal effects to be applied for infringements of data protection law. They do not however include such powers for the Authority.

V.3. Law-enforcement Data Processing with a View to EU Data-protection Reform and the Related Practice of the NAIH

The European Parliament and the Council adopted the new EU data-protection package on 27 April 2016, the two elements of which are the regulation defining the general framework of data protection (Regulation (EU) 2016/679—the GDPR) and the directive protecting the personal data processed for law-enforcement purposes (Directive (EU) 2016/680—Police Directive).

While the GDPR shall be directly applicable throughout Europe as of 26 May 2018, the Police Directive has to be transposed into the national laws of the Member States by 6 May 2018. The transposition of the provisions of the Police Directive is currently under way.

The authorities of the Member States have to process and transfer increasing amounts of personal data as part of the struggle against international crime and terrorism. The improvement of cooperation between the authorities concerned in this respect requires the building of a clear and more coherent regulation of the protection of personal data in the Union.

The scope of the Directive is broader than that of the Framework Decision, as it includes data processing for law enforcement, crime prevention (including the struggle against terrorism, organized crime, and cybercrime), as well as protection against and prevention of threats to public security, data generated during the administration of punishment, and companies and organizations processing data for law enforcement (such as private-run prisons).

Like the GDPR, the Directive expands the framework for data protection by new legal institutions, which are to be used by organizations processing data for law enforcement purposes. Like the GDPR, it provides for the principles of data protection by design and data protection by default, which must be applied by law enforcement agencies and bodies at the beginning of all procedures related to personal data (for example creating new databases). Detailed and extensive obligations arising from the performance of the data protection impact assessment and the prior consultation with the data protection authority, as well as the recording and journaling of data processing activities are also of utmost importance. In addition, the persons responsible for data processing shall be accountable for their work, and the authorities shall appoint data protection officers, who shall be responsible within the organization for the protection of personal data and require the notification of personal data breaches to the national supervisory authority.

All in all, the provisions of the Directive oblige the data controllers to cooperate more closely with the data protection authorities and to further enforce the criteria those authorities propose. Given the fact that the number of data transfers abroad is expected to increase and the new terms and conditions for their prior approval and control will be provided by the Directive, the prior control of data protection authorities may play a greater role than before.

During 2017, the NAIH received a number of submissions and complaints on data processing related to law enforcement. In most cases, complaints were related to the data processing of various investigative authorities (police, tax authority, prosecutor service), public space surveillance agencies (police, public safety office), and prison agencies.

One of the 2017 investigation cases to be emphasized in respect of the future application of the Directive was outlined in Chapter IV above.

V.4. Data Processing by Surveillance Cameras

As seen in the statistics part, most of the submissions and complaints filed with NAIH last year were on the operation of public-area surveillance and property-protection cameras. Furthermore, there was a large number of complaints on cameras and camera systems in condominiums.

V.4.1. Cameras and Camera Systems in Condominiums

a) A major group of complaints were those where possible breaches of law concerning surveillance cameras were due to primarily unauthorized access or illicit surveillance of an area.

Act CXXXIII of 2003 on Condominiums (the Condominiums Act) regulates the setting up and operation of surveillance cameras in condominiums.[2] It is an important rule that the setting up and operation of an electronic, closed-system surveillance system may be decided upon by the members' meeting with an affirmative vote of two-thirds of all units owned separately by co-owners. That is to say that for a valid decision of the members' meeting on the setting up and operation of a surveillance camera system requires an affirmative vote of the two-thirds of all co-owners, not the two-thirds of the co-owners present at the meeting.

No surveillance camera may be directed at the door or window of separately owned living or non-living quarters even if located in a jointly owned building, part of a building or area, nor can it be placed in a jointly owned and used room where surveillance—due to the purpose of the room—could damage human dignity.

b) Household Data Processing in Condominiums

In the case of another large group of complaints, the complainants objected to one or more residents of the condominium installing and operating surveillance cameras in common property. It is important to point out that this data processing is different from the above, because in this case the main rule is that a resident cannot install a camera to surveillance the jointly owned part of the condominium, its premises and area. If, therefore, the camera cannot be placed in such a way that its field of view includes solely the property of the owner or owners who intend to install it, it cannot be lawfully installed and operated.

The legal basis for data processing in this case is not the provisions of the Condominium Act. Section 2 (4) of the Privacy Act provides for an exception that its provisions do not apply if data processing is solely for the personal purposes of a natural person. Thus, the legislator created the possibility that, in some cases, the rules of the

[2] Section 25 of the Condominiums Act.

Privacy Act need not be applied for recording images. Such is the case, for example, when a natural person installs cameras on his or her property for protection purposes.

However, it cannot be ignored even in this case that the camera operator must notify those intending to enter the area monitored by the camera by means of, for example, a notice or a pictogram indicating camera surveillance at the entrance of the property. According to the Authority, this exception must be interpreted narrowly, since it is to be avoided that a particular data processing be subjected to an exception by a unilateral statement or arbitrary decision of a natural person. Accordingly, the above provision of the Privacy Act may only—in accordance with the judgment of the Court of Justice of the European Union[3]—mean an exception to the provisions of the Privacy Act if the phrase 'for his or her personal use' holds for the entire duration of the data processing by the natural person.

Thus, if the field of view of the cameras is directed outside the private area of the person processing data with the camera system, such as a public area, jointly owned parts of a condominium or any other area owned by a third party, it cannot be considered to be 'a purely personal or household activity'**.**

V.4.2. Further Common Complaints about Surveillance Cameras

V.4.2.1. Camera Surveillance at Work

The Authority receives several submissions on instances of a data controller as an employer installing cameras in a workplace to surveillance employees. According to the consistently held opinion of the Authority for several years, cameras may not be operated with the primary and explicit purpose of monitoring employees and their activities. The use of an electronic surveillance system, the—even undeclared—purpose of which is to influence the behaviour of employees in the workplace, is unlawful.

With regard to the obligation to provide information, it is important to emphasize that the employer has to specify for each camera for what purpose it is installed in the given area and which area and equipment the camera's field of view is directed to. The employer can thus justify to the employees why it is necessary to monitor the area. It is unacceptable practice when the employer provides general information to the employees of the use of an electronic surveillance system in the workplace. The use of a hidden camera is forbidden.

In one case, the Authority found that the data controller had not provided adequate prior information on the data processing and its circumstances to its employees and to third parties visiting the stores operated by the data controller, and that it had operated the cameras in the given stores in violation to the principle of purpose limitation. The Authority found as regards the operation of the surveillance cameras that the data controller had failed to indicate the legal basis of its data processing clearly, and had therefore to clarify that.

With regard to data control for the purposes of the control of employees, the Authority also mentioned the fact that respect for human dignity constitutes an absolute limitation of camera surveillance. As a result of this principle, cameras cannot be operated to monitor employees and the activities they carry out on a permanent basis without express purpose. Against this background, the use of an electronic surveillance system that is intended to influence workers' behaviour in the workplace is unlawful. During the proceedings, the Authority found that the data controller had infringed the principles of purpose limitation and necessity under Section 4 (1)–(2) of the Privacy Act. The Authority also found that the data controller had failed to define precisely the legal basis for the data processing during the period under review when referring to Section 11 (1) of the Labour Code, the rules of Act CXXXXIII of 2005 on Persons and Property Protection and on the Activity of Private Detectives (hereinafter 'the Property Protection Act'), and the declarations signed by employees; that is, the data processing reviewed had no legal basis. The Authority imposed a fine, and ordered in its decision that the data controller end the unlawful processing of data by disassembling the cameras, transferring them, or changing their field of view (Case no: NAIH/2017/984/H).

V.4.2.2. Surveillance Cameras in Shops

Both in the above case and in the complaints received by the Authority, there is a recurring problem that data controllers perform inappropriate camera surveillance in the shops they operate.

The rules governing such data processing are laid down by the Property Protection Act. It is important to point out, however, that these provisions are to be applied in conformity with the Privacy Act. Data processing under the Property Protection Act is therefore lawful when the data controller always complies with the basic provisions of the Privacy Act when processing data: the basic principles of the purpose limitation and fair data processing.

Another important constraint on the use of electronic surveillance systems is that no camera can be placed in a room where surveillance might damage human dignity.[4] During the constitutional review of the Property Protection Act, the Constitutional Court stressed the importance of the respect for human dignity.[5] There are a number of

[3] http://curia.europa.eu/juris/celex.jsf?celex=62013CJ0212&lang1=hu&type=TXT&ancre
[4] Section 30 (3) of the Property Protection Act.
[5] Section III.2 of the Decision 36/2005 (IX.5) AB.

other tools for preventing property-related violations of law and criminal behaviour that do not damage human dignity while effectively protecting property in the technical sense. In the light of the above, the Authority holds that no camera can be operated where there is a possibility to make image recordings of data subjects in an intimate position detrimental to their human dignity.

The Authority was notified that a hidden camera system had been installed in a department store. The hidden cameras were devices that seemed to be smoke detectors, but they had cameras in them capable of taking image recordings. The Authority found that these devices were clearly 'camouflaged' cameras that, at first glance, did not appear to be surveillance devices for most of the data subjects. The controller acknowledged the installation of hidden cameras, but argued that the devices, although connected to a system, were not used due to their poor quality images, and were removed after the Authority began its proceedings. The Authority ordered the data controller to remove the hidden cameras (NAIH/2017/5072/V).

V.5. Data Protection Concerns with Regard to Claims Management

V.5.1. The Prohibition of Making Environment Studies and Photos of Real Property

In each of the cases, the Authority emphasized that there is no need to carry out an environmental study to assess the solvency of a debtor to enforce a claim. In several cases, the Authority also ordered data controllers to terminate the data processing objected to, and to delete photos of pawned real property made without legal basis.

V.5.2. The Needlessness of Examining Creditworthiness

There is no legal obligation for financial institutions dealing with claims management to assess the creditworthiness of debtors, to assess the income status of a natural person or a natural person's household. Consequently, the legal basis for processing data on property and income situation can only be the consent by the data subject. As processing data on property and income situation of data subjects is not required by law for claims management companies, and, as their processing is not necessary for the purpose of collecting them, the processing of these data can be regarded unlawful.

V.5.3. The Lack of Providing Prior Information

There were several cases in which the Authority had to deliver an opinion on the data-protection aspects of file-transfer transactions, which involve a number of similarities with the purchase of claims, but, in so far as it is transfers of valid contracts, not arrears claims that are concerned, claims delayed and contractually performed must be approached in different ways.

The data subject is entitled to request information on the processing of his or her data at all stages of the data processing; thus the provision of prior information must be complete and transparent in relation to all the planned data processing operations connected to the basic legal relation. Thus, during the transfer of the claim, the data subject must also be able see in advance whom the creditor will hand over the claim to, under what conditions and at what fees.

The Authority repeatedly called the attention of the submitters to their right of being informed by the data controllers, and that it is expedient to request information about the elements of the claims (fees, costs, etc.) and their legal basis.

V.5.4. Third Persons—the Prohibition of 'Seeing Neighbours'

In 2017 too, the Authority deemed the surveillance of third persons, the so-called practice of 'seeing neighbours', as a serious data-protection abuse. It is unacceptable that the personal data of third person wholly uninvolved in the legal relationship giving rise to claim management, typically neighbours, are processed, are entered and even systematized in databases.

V.5.5. Refusal to Erase Data

It is a general experience of the Authority that claims management companies do not always fulfil the requests of data subjects to have their personal data deleted; for example, they fail to delete telephone numbers in spite of requests, and wish to use them on the basis of legitimate interests (see section V.15 for a more detailed discussion).

V.6. The Requirement of Providing Prior Information

By the experience of the Authority in 2017 likewise, data controllers failed to give enough attention to the requirement of providing prior information.

The data controllers must provide prior information to the data subjects whereby they will understand what effects the data processing is going to have on their privacy. Though data controllers do compile privacy notices, these often do not meet the requirements under the Privacy Act.

As explicated in the recommendation on the provision of prior information on the webpage of the NAIH,[6] the mere repetition of the text of the laws is not acceptable practice, as the essence of a data-protection notice is the presentation of the way the data controller complies with legal requirements and of the practice it develops in order to do so. The repetition of the texts of legal provisions may be difficult for some data subjects to follow, and these provisions make the data processing notices too complicated and cumbersome.

In case no. NAIH/2017/4318/V, the Authority found that, though the data controller did have its rules of data processing in place, and that these were available for data subjects, it was based on clumsy legalese, and often repeated the very text of the Privacy Act.

It is a recurrent problem that the data-processing notices are incomplete, e.g. they do not provide information on the identity and accessibility of the data controller; often the purpose of the data processing does not transpire clearly, or the purpose is presented in far too general or not easily intelligible terms. Consent by the data subject can only be regarded as a lawful basis of data processing when it is based on appropriately detailed and unambiguous prior information.

V.7. Cases of Processing Photo and Scanned Copies of Identity Documents

In 2017 several submissions were filed with the NAIH describing that the data controller—often an insurance company or insurance brokerage, a service operating an online commercial space, or solicitor acting as solicitor—required the data subject to submit photo or scanned copies of his or her official identity, residence, tax identity, and ATM cards (hereinafter 'documents') referring to reasons related to the provision of the given services.

One of the preconditions of the lawful processing of the data content as well as the photo and scanned copies of the documents is that the data controller has the appropriate legal basis to do so. The legal basis of data processing may be for instance a provision of law prescribing and authorizing data processing, a statement of consent[7] by the data subject (subject to meeting all the conditions of a valid consent)[8], or if processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, under the condition that the legitimate interests do not limit the right of the data subject to the protection of his or her personal data and privacy.[9]

Valid consent given, however, data processing is lawful only if it meets the principle of purpose limitation;[10] in other words, the processing of the data content of the photo or scanned copies of the documents is necessary for exercising a right or fulfilling an obligation; in the lack of which the processing of the data content of the document copies qualify as stockpiling. A further condition is compliance with the principle of necessity,[11] according to which only the data essential for the given data-processing purpose and only for a period essential to it. With regard to the validation of registration data, for instance, it is unjustified and unlawful to process the photos and signatures and the photo or scanned copies of the documents they are included in if these data were not necessary for the registration.

It is important to note with regard to processing copies and photocopies of documents that according to the main rule under Act CXXXVI of 2007 on the Prevention and Combating of Money Laundering and Terrorist Financing in effect until 26 June 2017, the service providers[12] under its scope were not permitted to process copies of the official certificate suitable for the proof of identity and the official certificate for the proof of address in the framework of customer screening, only the data of these documents defined by this, the former Act on Money Laundering (such as surname and forename (birth name), address, and nationality)[13]. As a consequence, the general practice of data controllers to obtain photo or scanned copies of personal identification documents was unlawful. An exception to this general rule was the cases under enhanced customer due diligence, [14] where, upon concluding a contract with the service provider, the customer was not physically present for identification purposes or for the verification of his identity, which most frequently happens in our time when contracts are concluded online. Under enhanced customer due diligence, the customer was obliged to submit to the service provider the certified copies of the documents specified by the applicable provision of the former Act on Money

[6] www.naih.hu/files/tajekoztato-ajanlas-v-2015-10-09.pdf
[7] Section 3 (7) of the Privacy Act.
[8] Section 5 (1) of the Privacy Act.
[9] Article 7 f) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[10] Section 4 (1) of the Privacy Act.
[11] Section 4 (2) of the Privacy Act.
[12] Section 1 (1)of the former Act on Money Laundering.
[13] Section 7 (2) of the former Act on Money Laundering.
[14] Section 14 (1) of the former Act on Money Laundering.

Laundering: certified copies [15]of the official certificate suitable for the proof of identity and the official certificate for the proof of address were thus acceptable for this purpose; mere photocopies of these documents would not suffice for compliance with identification obligation.

Replacing the former Act on Money Laundering as of 26 June 2017, Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing (hereinafter 'the new Act on Money Laundering) brought about a change in the legal assessment of copying documents. The new Act on Money Laundering regulates the data that can and must be processed by service providers in essentially the same way as the former Act did;[16] however, there is a significant difference in that—excluding the case of simplified customer due diligence, which can be regarded as an exception rule—the new Act requires service providers to make copies of the documents presented to them for the purpose of verification of identity even the case of general customer due diligence, not only enhanced due diligence.[17] As a main rule, if the customer is not present physically for the purpose identification and verification of identity, which obligation may only be substituted if the service provider applies the enhanced customer due diligence measures provided for in its internal policy.[18] In the opinion of the Authority, however, the provisions of the new Act requiring 'document copying' do not constitute a legal base for processing the personal data—the image, signature, identity number—the Act does not specify.

In a complaint giving rise to an examination under Section 52 of the Privacy Act—still to be judged in accordance with the provisions of the former Act on Money Laundering—the complainant objected to the employees of the insurance company he filed a notice of loss with under an insurance policy making photocopies of his certificate of personal identity and official certificate for the proof of address, and ATM card.

In the opinion of the NAIH, the applicable provisions of the Act on the Business of Insurance may provide a legal basis for the processing of certain personal data of the complainant's ATM card,[19] but only to the extent necessary for the fulfilment of claims and for the evaluation of claims arising from the contract. Neither the provisions of this act nor any other law provide a legal base for photocopying the ATM card. Legal authorization providing a lawful base for data processing lacking, the Authority regards the processing of the data not specified by the Act as unlawful under both the former and new Act on Money Laundering; furthermore, the data processing objected to by the complainant not only lacked a legal basis but also contravened the principles of purpose limitation and necessity (data minimization) as per the Privacy Act (it was stockpiling); and was thus unlawful in the light of the provisions of the new Act on Money Laundering and the Privacy Act.

Several submissions were filed with NAIH in which the complainant objected to the practice of document copying by persons involved in the activities of attorneys at law.

One submitter requested information from the NAIH whether an attorney-at-law taking part in the transfer of ownership of real property may photocopy the certificates of personal identity and official certificates for the proof of address (hereinafter 'address card'), and the tax identity card of the owners of the property—with reference to Rule no. 1/2017 (10 July) of the Chamber of Hungarian Attorneys-At-Law (hereinafter 'the Chamber')—and may the owners be requested to provide a statement of consent.

With reference to the applicable provisions of the new Act on Money Laundering,[20] under which the attorney-at-law is obliged to perform customer due diligence and to report when involved in activities of an attorney-at-law in the transfer of ownership of real estate property, the Authority found that the attorney-at-law is required—in performing customer due diligence for verifying the identity of the customer under the new Act on Money Laundering—to request the presentation of official certificate suitable for the proof of identity and the official certificate for the proof of address, and also to make photocopies thereof.

V.8. Health

1) In the field of healthcare data processing, the most important event in 2017 was the launch of the Electronic Health Service Area (EHSA) in practice. Through the interconnection of healthcare providers and the provision of a unified communication space for them, the EHSA will enable more effective cooperation between service providers and recipients, simplify the availability of data and documents generated during provision of healthcare services, will provide the healthcare industry with a unified and effective analysis of available data, simultaneously ensuring the right of self-determination of data subjects.[21]

The specificity of the data processing associated with the EHSA is that it is to primarily considered as data processing authorized by law (Section 5 (2) (c) of the Privacy Act), in which the data subject can exercise his or her right to self-determination by way of his or her own decision. In the course of the data processing, the data

[15] Section 14 (2) of the former Act on Money Laundering.
[16] Section 7 (2)–(3) of the new Act on Money Laundering.
[17] Section 7 (8) of the new Act on Money Laundering.
[18] Section 17 (1)–(3) of the new Act on Money Laundering.
[19] Section 135 (1) of Act LXXXVIII of 2014 on the Business of Insurance.
[20] Section 73 (1) b) of the new Act on Money Laundering.
[21] https://e-egeszsegugy.gov.hu/fooldal.

subject has several significant decision-making powers, such as it is up to his or her discretion who is to access and what personal and special data of his; this is therefore primarily data processing based on consent. However, even in the latter case, the law prescribes the main conditions of data processing; thus the legal basis of data processing has a dual character. By default, a practitioner can only access data belonging to his or her own field, but the patient may limit or expand the accessibility of his or her data through the portal. Additionally, a user may request notification of uploading the documents concerning him or her, and can also keep track of who and when they access his data.[22]

In two submissions, healthcare workers requested to know whether they could be lawfully compelled to take out their new type of personal identification certificates for use in connection with the EHSA.

As of 1 November 2017, all publicly funded service providers are required to join the Electronic Health Service Area through their computer systems. Logging in to the EHSA is possible for natural persons (family doctors, health care staff, etc.) after a so-called two-factor identification. The essence of this is that, after entering the name/password, a second security element is required for logging into the system, which may be a proprietary or a biometric identifier. By virtue of an agreement with the Ministry of Interior Affairs, the system operator can ensure a uniform identification that guarantees the secure operation of healthcare IT system using the e-certificate for personal identification.

The use of the services of the EHSA can only be realized by complying with serious security requirements, which are prescribed by the highest security level of the system for all users. The use of the e-certificate for personal identity for logging in provides a secure identification for both the identification of the patients and the system-user doctors, healthcare employees, and pharmacists.

For the use of the EHSA, such identification method is required that has already been applied, and ensures the appropriate level of security, and has no cost implications for either the developers or the users. This method of identification is the e-certificate for personal identity, i.e. the identity card with storage capacity.

The new type of identity certificate enables the association of different accessibility rights for the various applications.[23] Essentially, this means that this identification for use with the EHSA does not involve unauthorized access for anyone to elements of the identity card—fingerprints, tax number—other than those required for identification.

As taking out the permanent certificate proving personal identity is free of charge, puts no financial burden on users, and, as the differentiated accessibility rights and data security requirements—with particular view to the processing of a large amount special personal data—entail identification without any doubt, the legal and technical conditions being provided, the Authority found no reason to be concerned about compelling the users of the system to take out the identity card (*NAIH/2017/4198/V, NAIH/2017/4895/V).*

According to the agreement concluded by the Authority and the Public Healthcare Supply Centre (hereinafter PHSC), the parties hold consultations on a quarterly basis, the employees of the PHSC present recent developments, of which an efficient exchange of information takes place between the parties; there is also an agreement that the Authority notifies the data-protection officer of the PHSC of any issues that arise during practical enforcement and that the Authority receives information of.

2) Copying health records, ensuring the right of access, continues to be the subject of several complaints to the Authority. However, in these cases, it is usually not the practice that the service provider does not want the documentation to be made available to the data subject, but the details of the release are problematic.

While a data subject complained that the institution did not send the documentation electronically, and was thus meant to go and fetch it personally, which was a burden for her not living in the area, another complainant expressed concern about how safe the electronic transmission of special data was if the identity of the requester could not be established.

The Authority does not prohibit the electronic transfer of a copy of the requested healthcare documentation to the patient, in particular where a large cost or sacrifice would burden the data requester if required to appear personally in the institution's premises for the purpose of receiving a copy of the health records. However, the precondition of this is the adoption of a procedure guaranteeing data security (for example asking control questions from the data subject when access to data is requested electronically), in which case the institution is obliged to ensure compliance with data security requirements (NAIH/2017/2169/V).[24]

---

[22] http://www.kormany.hu/hu/emberi-eroforrasok-miniszteriuma/egeszsegugyert-felelos-allamtitkarsag/hirek/megkezdodott-az-elektronikus-egeszsegugyi-szolgaltatasi-ter-probauzeme.

[23] The Deputy State Secretariat of the Ministry of the Interior for Registration Management provides clear information to the public on the storage-capacity certificates proving personal identity on its webpage, kekkh.gov.hu, http://www.kekkh.gov.hu/Eszemelyi/mit_tartalmaz_a_tarolo_elem

[24] Section 7 of the Privacy Act.

Otherwise, the Authority promotes electronic transfer of data insofar as the data subject is capable of receiving it; in case of personal receipt, a data carrier once purchased is cheaper than photocopying a large document; moreover, it is ecologically more reasonable to hand over to the data subject electronically rather than in printed-out format the documents stored electronically.

A case pending for a long time was closed in which the heirs of the data subject requested access to the expert opinions by the institution's employees on the circumstances of the death, but the healthcare provider refused to oblige referring to its right to defence in the civil litigation.

Though the scope of the Privacy Act includes only living persons, its criteria and principles are also applicable in the law of reverence for the deceased in the way heirs can exercise them. Access to documents arising in the event of death is, in the opinion of the Authority, is a quasi-extension of the right to self-determination of the data subject, part of the right to receive information under Section 13 of the Health Act, which is exercised not by the data subject due to the circumstances but by the heirs. The way to do so is by the exercise of right to become acquainted with data[25] and the provision of information thereof. In the course of the examination, the Authority found that the employees made personal remarks in the expert opinions that do not constitute the personal data of the data subject, it therefore ordered that the expert opinions be disclosed to the heirs in such a way that the remarks were blacked out. The data controller obliged (*NAIH/2016/456/V).*

In one case, the Authority also conducted administrative proceedings on a refusal to issue health records. The complainant had requested the documentation of the operations performed on him earlier on by the data controller, because of his unsatisfactory condition following the operations, and had wanted become acquainted with whole material of the interventions in order to find a final solution to his health problems. The data controller did not respond to the complainant's requests. The Authority found that the data controller infringed the law, and that it was to impose not a warning as a sanction under Act XXXIV of 2004 on the Definition of, and Aids to, Small and Medium-sized Enterprises, because, according Section 12/A (2) thereof—'there is no room for forbearing to impose a fine if the infringement damages or threatens human life, physical integrity or health'—imposing a fine is appropriate. According to the Authority, though it is not entitled to take a position on medical issues, knowledge of content of the documentation of former treatments may have an impact on the choice of further treatments, and it is therefore necessary for identifying the current state of health. Since the data controller possesses the documentation—it cannot be obtained from other sources—conduct threatening health can be established.

The court upheld the Authority's decision in respect of the infringement, but did not find the sanction appropriate, because it found that the Authority did not seek evidence to demonstrate that the infringement would indeed threaten the complainant's health. Thus, in this respect, the Authority will initiate new proceedings (NAIH/2017/472/H).

In his submission, a family doctor stated that a company involved in screening for hearing loss sent pre-printed personal invitations to screenings to patients in the various districts. In the course of the investigation, the NAIH found that the family doctors did not transfer data on those belonging to their districts, the company only posted the letters filled in and addressed by the doctors, and the data subjects, having received the invitations, may contact the company.

In the opinion of the Authority, family doctors are not legally authorized to use the data of patients they provide basic services to for the promotion of the activities of a profit-oriented business enterprise. This data processing activity constitutes data processing for direct marketing purposes, other than the data processing for the purposes of providing basic services, for which the prior consent of the data subject is required.

In addition to the lack of this legal basis, the letter received by the data subjects did not provide any information that the doctor did not transfer the patient's data on to a third party—the company—, and the data subjects are left unaware of the course and purpose of the data processing. As the submission also maintained, it is misleading, however, that the patients receive a letter in the name and signature of their family doctor inviting them for a screening, while it is unclear for them how the company knew that the addressee had a hearing loss. In addition, the wording of the letter is misleading, because it seems not an option but a compulsory test, as the doctor calls for participation. The letter is ambiguous to the patients, as they believe it is a compulsory screening programme that they are obliged to participate in, all of which is certified by the family doctor's stamp. These circumstances also violate the requirement of fair data processing.

[25] Section 24 (11) of the Health Act states: 'In the case of a patient's death, his legal representative, close relative, or heir shall have the right, upon written request, to become acquainted with health data that is, or may be, related to the cause of death, and data that is related to the medical treatment preceding death, furthermore to inspect the medical record and to be provided by copies thereof, at his own cost.'

According to the Authority, the promotion of screening for hearing loss can be carried out without sending personal invitations, the general practitioner could provide information about the screening during consultation, or poster in the waiting room could call the attention of patients to the possibility of the screening. The Authority called on the company to terminate the practice objected to, which the data controller fulfilled (NAIH/2016/3246/V).

4) Submissions requesting consultation on health issues showed a variegated picture. There were questions about online appointments, transfer of personal health-history sheet, the mode of operation of surveillance cameras at healthcare provider premises, which obviously differs from other modes of surveillance due to the special personal data being processed at a healthcare institution.

In the case of healthcare provision, camera surveillance can only be applied in exceptional cases. The principle of purpose limitation is fulfilled, for instance, in nursing when the patient's condition is so serious that his continuous monitoring is unavoidable; the establishment of this is a medical professional issue.

Camera surveillance can also be applied when healthcare workers cannot perform their tasks under the Act on Health without a method less infringing on the privacy of patients. The use of cameras must be limited to what is most necessary. As a consequence, only live images may be looked at; the recording and storage of images is unacceptable (*NAIH/2017/2440/V*).

A query was received on the fact that a regional specialized agency requested disclosure of non-anonymous data of patients for the purpose of supervising family doctors.

For judging the circle of data requested by the agency, it must be examined whether data identifying persons are unavoidably necessary for the control purpose, or this purpose can be achieved by the transfer of anonymized data, whereby the procedures applied by the doctored can be supervised, but the identity of the patient remains unknown. It is up to the agency conducting the supervision to prove the necessity of identifying the patients (*NAIH/2017/2876/V*).

In another submission, a psychiatrist requested the opinion of the Authority as to what data of a patient could be transferred to the public guardianship authority, and how to do so—when there is neither a request by the authority and consent by the patient thereto nor explicit authorization under law—when the mental condition of the patient suggests initiating a procedure to place him or her under guardianship. In the submission, the clinic informed the Authority that it often happens that the ambulance bring to the psychiatric ward patients with severe mental deterioration (mental disorder). The social worker often cannot track down any relative or helper, no one makes inquiries about them, and they often live in their homes alone.

As per the provisions applicable of the Health Act and the Health Data Act, the data controller is exempt from medical confidentiality primarily when the patient or the person entitled to make declarations instead of him or her has provided written authorization to do so. In certain cases medical confidentiality may be breached without the consent of the patient—such as when law prescribes data processing, transfer or disclosure, or when emergency or the threatening condition of the patient or others so requires.

In the opinion of the Authority, the protection of the vital interests under Section 6 (2) of the Privacy Act, disease and threat to life are such unavoidable reasons whereby enforcing the right to the protection of personal data cannot obstruct the protection of life, physical integrity, and health, or the prevention of any threat thereto.

Section 189 (2) of the Health Act[26] referred to in the submission does not provide sufficient authorization for data transfer. In the opinion of the Authority, the personal and health data of a psychiatric patient may only be transferred to the guardianship authority if the patient certainly has no relatives, or the protection of his or her vital interests can be established, or the purpose of the data transfer is the protection of the physical integrity and health of the patient; furthermore, the immediate threat to the patient cannot be avoided without placing him or her under guardianship. Deciding this question points beyond the scope of the Authority.

Beyond the above, commentary to Act V of 2013 on the Civil Code should also be taken into account, which states the following with regard to placement under guardianship under Section 2:28: 'If the guardianship authority learns of the necessity of placement under guardianship—either by way of official proceedings or notification—it first notifies the close relatives entitled to initiate litigation, and, if any of them fail to initiate litigation within sixty days of that, the guardianship authority shall initiate the proceedings for placement under guardianship.' With a

[26] Section 189 (2) of the Health Act states: 'The rights of a psychiatric patient as set forth under Sections 6–25 shall be restricted, while receiving healthcare services, only in keeping with the specifications of this Act, and only to the degree and for the duration of time absolutely necessary, excepting the provisions of Section 193, and only if the patient's behaviour qualifies as dangerous or immediately dangerous. However, the right to human dignity shall not be restricted, even in this case.

view to this, the clinic is entitled to notify the guardianship authority if the necessity of placement under guardianship is deemed unavoidably necessary in the light of the above (*NAIH/2016/5693/V*).

V.9. The Processing of Children's Data

V.9.1. Data Processing Related to Parental Responsibility

The NAIH received a number of submissions in which a parent living separately or divorced complained that she or he did receive no information from either the spouse or any other institution about the data concerning minors. In many cases it is because joint or exclusive parental responsibility is disputed. If an institution provides information, the other parent objects to the data processing.

The fundamental problem therefore is the question of the parents' getting acquainted with their child's data, the right of the parent to receiving information about the child's personal and special data[27].

The Authority found in an investigation proceedings that if a parent living separately is seeking information about the child's data, the institution is obliged to inform him or her.

'In the practical application of law, healthcare providers presume a joint exercise of parental responsibility, and they are only entitled to deny the provision of information if they have satisfied themselves beyond all doubt that the parent inquiring is not entitled to legal representation and/or parental responsibility' (NAIH/2017/48/V).

The NAIH turned to the Secretary of State for Education due to the fact that, in one of the investigation cases, a pedagogical agency had not informed the father of a child living separately and apart that a committee of experts was to hold an examination, and had omitted to do so by reference to the fact that it had found the mother's statement that she was entitled to represent the absent parent sufficient.[28]

In the opinion of the Authority, this regulation and practice render the exercise of the absent parent's rights impossible. It is a matter of concern that one parent can consent to the processing of the child's personal data or to the expert examination by making a statement that he or she has the right to make a declaration on behalf of the other parent.

In view of the above, the Authority asked the Secretary of State for Education that a the Ministry of Human Resources Decree should be amended so as to exclude legal presumption in the case of consent to the processing of the personal data of the child, that is, both parents should be considered.

A notifier turned to the Authority, because he requested information about the data of his children form a Family and Child Welfare Centre, but was denied on grounds that his request failed to specify the purpose and legal basis of the data processing.

The legal basis for the processing of documents relating to minors is laid down in Section 136/A (1) of Act XXXI of 1997 on the Protection of Children and Guardianship Administration (hereinafter as the 'Child Protection Act'). The Authority found that the notifier may access the personal sheet of the child in the child protection registry, and may request extracts and copies thereof—thus the questions the notifier asked in connection with the children that can be answered from the datasheets and documents mentioned above must be answered—unless the right to parental responsibility is limited, and she or he is not entitled to do so because of the limitation.

Against this background, the questions raised by the notifier in connection with the children that can be answered from the datasheets and documents mentioned above must be answered. If the parent requests copies of the documents, they must be given. The right to copy is explicitly mentioned in the legal provision, and it cannot be narrowed or restricted to the right of access.

[27] Section 3 (2) of the Privacy Act states: '"personal data" shall mean data relating to the data subject, in particular by reference to the name and identification number of the data subject or one or more factors specific to his physical, physiological, mental, economic, cultural or social identity as well as conclusions drawn from the data in regard to the data subject.' Section 3 (3) of the Privacy Act states: '"special data" shall mean: personal data revealing racial origin or nationality, political opinions and any affiliation with political parties, religious or philosophical beliefs or trade-union membership, and personal data concerning sex life.'

[28] Section 14 (2) of Decree 15/2013 (II.26) of the Ministry of Human Resources on the Operation of Pedagogical Agencies states: 'In order for the expert examination to begin, both parents exercising parental responsibility must be present. In case of doubt, it shall be deemed that the parent present is entitled to represent the parent absent. The parent present shall be informed thereof, and his or her relevant declaration shall be obtained. The parent is obliged to cooperate during the examination, and shall be entitled to present at it without disturbing it.'

V.9.2. The Processing of Children's Personal Data for Purposes of Political Activity

Several inquiries were received by the Authority from journalists about the conditions of politicians visiting educational institutions to appear together with pupils and students in photo images, and how these can be disclosed in the media.

Politicians regularly attend events where children are present. In reports of such events, stories published in printed or online newspapers, there often are photographs of the students of an institution alongside the participating politicians. For this reason, the Authority set out, in a case opinion (NAIH/2017/5206/V), the data protection requirements that are essential for respecting the privacy of children and their constitutional right to the protection of personal data.

In the above mentioned data processing activities, the best interests of children and minors need to be taken into consideration primarily when their personal data, such as their photographs, are disclosed either online and offline. Children's personal data deserve special protection as they are less aware of the risks associated with data processing, its consequences, and the associated guarantees and rights.

The Authority laid down guarantee requirements in respect of consent as the legal basis of data processing. Data controllers must have the written consent from the legal representative to the data processing for each photo taken of a child under the age of 16. Parents may in many cases make a statement at the beginning of the year consenting to the publishing their child's photos on the school website. It must be emphasized, however, that this general consent is not an adequate legal basis for disclosing photographs in any public media. Informed consent of the data subjects must be obtained for each individual case—each data processing.

In providing information prior to obtaining consent, particular attention is to be paid to make the information clear and easy to understand for both the parent and the child. Care should be taken to ensure that the information clearly identifies the purpose of data processing, the possibilities and means of exercising the rights of the data subject, the means of legal remedy, and the possible future effects of processing special data on the child's private life. Furthermore, children should be given the opportunity to express their views on data processing, and, if they do not wish to appear in recordings of such public events, they must be given the opportunity to voice their opinion without further adverse consequences.

Prior to the disclosure of image recordings, even if the data controller has the required written consent, the parents should be given the opportunity to withdraw the previously given consent.

Finally, the Authority emphasized that special attention should be given to the right of the data subject to erase his personal data if it is no longer needed in connection with the original purposes of data processing, if the consent was withdrawn, or if the processing of personal data is otherwise unlawful. 'That right is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet.'[29]

V.10. Cases Related to the Social Networking Site Facebook and the Opinion of the Authority

V.10.1. Over the last few years, several citizens' complaints were received by the Authority in connection with the data processing and profiling practices and security measures of the social networking site Facebook. Most often, complainants filed notifications or queries with the Authority about the use and change of names, the blocking/deleting of user profiles without prior notification or related procedures.

One of the most common questions was about the lawfulness of requesting document copies. There are two reasons why Facebook requests the scanning or a photo of a certificate of identity:

• Verification of ownership of account: to prevent someone else from logging into the account.

• To confirm the user's name: under the terms of use of Facebook, users give their real name and data when registering.

In the case of documents provided by users for checking names, all data (document number, address, etc.) can be blacked out with the exception of parts required for identification. The document provided by the user in digital form is not retained, stored, it is for identification purposes only.

In connection with blocked Facebook profiles, section 14, 'Termination', of the Terms of Service of the social networking site, lays down the conditions.[30]

[29] Recital 65 of the General Data Protection Regulation.

[30] 'We can stop providing all or part of Facebook to you immediately if, in our sole discretion, you clearly, seriously or repeatedly violate this Statement or our policies, including in particular our Community Standards, or if we are required to do so by law. We will notify you by email or the next time you attempt to access your account.'

A number of inquiries filed with the Authority formulated complaints regarding the hacking of profiles, creating fake profiles, and offensive entries. In order to avoid hacking of Internet profiles, the NAIH recommends that data subjects change their passwords to include at least 10 characters of lower and upper case letters and numbers, and log out of their accounts after each use, especially if a computer used by someone else, or they access their accounts from public computers.

V.10.2. Data on Facebook users in Europe are processed by Facebook Ireland Ltd. Complaints about the data controller can be filed with the Irish Data Protection Commissioner, the regulator in charge Facebook's European supervision. The NAIH consulted the Irish Data Protection Commissioner on the practices and procedures of Facebook regarding the use of names, name changes, and requests for copies of documents, which informed the NAIH that it had audited the social networking site's name check procedure during in 2011–2012, and found it proper. The Irish partner authority confirmed that the documents provided by the users to Facebook are deleted after the identification of the user. The consultation is still in progress, as the NAIH objected to Facebook's information practices.

V.11. The Blockchain Technology

A Hungarian citizen requested the NAIH to deliver its opinion on the data protection issues of the use of the virtual currency bitcoin and the blockchain technology underlying it.

The first representative of the blockchain technology was the virtual currency bitcoin on the digital market. In a blockchain, data are stored in so-called blocks, which practically function as small databases. If new data are added to the decentralized database of the blockchain by the users, they will be stored in a new block. In the course of making blocks, a chain is created, hence the name 'blockchain'. A blockchain is valid if it is headed by a so-called 'genesis block' (the first block made), and if all the transactions made with the data in them are valid. There is only a single, straight way back to the genesis block.

The system stores not only the data in the block but also all the operations made with them within the system. Data transactions are carried out without actual data movement between blocks; instead, the system merely attributes to the individual data in the block it is stored in the user entitled to dispose with it. The system adds the digital signatures of the users to the data stored in the blocks, and it is on this basis that it determines which user is entitled to dispose with the dataset in the given block.

The basis of the blockchain-technology storage is a decentralized system in which there is no central entity or any other external organ that controls the transactions made with data in it. The blockchain is stored not by a central data controller but by practically all users on each of their computers.

The blockchain technology underlying the bitcoin system was developed to enable a virtual currency system to be used anonymously, as there would be no need of providing personal data for carrying out bitcoin operations. Nevertheless, it is possible to conceive of a system using blockchain technology where blocks store personal data, as well; thus, for example, personal data could be linked to the data stored in a block and used fundamentally for payment.

If the blocks in a chain are used also for storing personal data, the question arises who qualifies as the data controller. In accordance with the concepts of the Privacy Act outlined above, the data controller is primarily the legal or natural person that determines the purposes of processing data, makes and executes decisions concerning it. Due to the fact that the blockchain is a decentralized system where there is no central entity exercising supervisory rights over system operations and data transactions, it is the individual users that practically carry out the data processing.

With regard to the blockchain, thus, each user who adds blocks and data within them to the system (e.g. one who 'mines' in the bitcoin system) simultaneously qualifies as a data controller, as well. Over time, the user who adds data to the system will receive the exclusive right of disposal over his or her data stored in the block, and can therefore determine which transactions he or she wants to use the data for. If the right of disposal over the personal data in a block is transferred to another user, thenceforth this user (the addressee of the data) obtains exclusive rights over the data, and thus qualifies as the data controller.

Under effective law, the legal basis of processing personal data stored in the blockchain is the consent of the data subject or the legitimate interest of the user. Should the data subject not consent to the storing of or carrying out operations with his or her personal data by the user entitled to dispose of data stored in the block, or should the user not be able to prove a legitimate interest in data processing, then data processing is unlawful. In respect of the personal data processed in a blockchain, the data controller must provide all-round information upon request by the data subject within 25 days.

V.12. Personal Data Breach

We regard as personal data breach the unauthorized processing of personal data, in particular unauthorized access, alteration, transfer, disclosure, deletion or destruction, as well as accidental destruction or damage that may be attributed to violations of data security rules.

The Authority investigated several minor and major breaches. The following major cases took place:

- An insurance intermediary did not actually have the consent of the notifier for the transfer of data, and there was no legal provision under which the breaching insurance intermediary would have been exempt from the obligation to keep the insurance secret confidential. The insurance intermediary failed to satisfy himself that the notifier had actually consented to the transfer of his personal data with regard to the person introducing himself as the representative of the notifier, that this person had actually been entitled to access the notifier's personal data, and the person introducing himself as the representative of the notifier had been entitled to modify the notifier's personal data on the insurance intermediary's website (NAIH/2017/477/V).
- A company sent documents related to a home-insurance policy to a client via electronic mail that were not signed by the client, and the personal data contained in the documents transferred were nor the client's data. The staff of the company sent the documents in question to the client, mistaking the client for another one with the same name (NAIH/2017/4691/V).
- The Authority received several notifications regarding the data processing related to an online ticketing system operated by a transport company. The notifiers complained that the online ticketing system of the company did not meet data security requirements, and several notifiers complained that, based on press reports, it was likely that third parties were allowed access to their personal data given during the registration.

A database containing the registered users' personal data collected from the database of the online ticketing system operated by the company was accessible to unauthorized persons. The Authority found that data security had been damaged to such an extent that unauthorized access to data, that is, a personal data breach, had occurred (NAIH/2017/3979 / H, NAIH / 2018/356 / H).

In this regard, the Authority found the following, as well:

While designing the data processing, the data controller had failed to take the technical and organizational measures and to set out the procedural rules that serve the security of the data. The absence of such measures is also proven by the fact that the company was unable to establish that personal data breaches had occurred in relation to the data processing it carried out.

In the contract with the data processor, the company 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.

In addition, the company 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.

Based on the above, the Authority imposed a data protection fine on the data controller, 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 registered users thereof. It also required that the company ensure the proper fulfilment of the data security requirements.

V.13. The Data-protection Register

As in recent years, the Authority received several consultation submissions in which citizens/organizations asked whether they were to report their data processing to the Authority for recording in the data-protection register, or asked various other questions about the data-protection register.

Under the regulation currently in force, the Authority keeps a registry of the personal data processing of data controllers in order to support data subjects seeking information; wherein all important circumstances of data processing, its purpose, legal basis, and duration have to be indicated.

The Authority keeps the register on all data-controller activities not subject to exemption under the Privacy Act, such an exemption being inter alia data processing on employees by the employer as data controller.

Currently, the regulation is that data controllers are obliged to report to the Authority their data processing before commencement; however, this rule will change. Unlike the Directive or the Privacy Act, the GDPR does not

contain any regulation on the authorities of the Member States keeping a national data-protection registry by. Article 30 of the GDPR obligates data controllers and data processors to maintain a record of processing activities under their responsibility. This will mean that data controllers and processors will keep their own records of their activities, and shall not have to report thereof to the Authority. The obligation to report to the current register will cease as of 26 May 2018.

Many telephone calls come to the customer service of the Authority in this regard. It can be stated that, in many cases, the callers regard their obligation to report more important than complying with requirements laid down by other regulations in spite of the changes in regulation.

The GDPR prescribes an obligation to notify in two instances: the competent authority shall be notified of the name and access of the data protection officer and personal data breaches. The NAIH provides special surfaces for these on its website.

V.14. The Protection of the Whistleblowers

The NAIH received several submissions where complainants objected to the fact that they had made whistleblowing or complaint notices to data controllers, who, proceeding, disclosed the identity of the whistleblower without his or her consent to the body or person complained against.

In the opinion of the Authority, the concept of consent cannot be construed broadly so as to cover all data processing activities, thus to include data transfer, rendering data accessible to a given third party, a body or person the data controller has subjected to examination.

The practice of deeming consent granted under Section 6 (6) of the Privacy Act to transferring personal data of a complainant on the basis of the lack of an explicit request to process the personal data fully or partially private and the filing of the request does not comply with the provisions of the Privacy Act, especially in view of the fact that complainants may not be aware of the possibility of the private processing of their personal data. In this regard, it is particularly important to bear in mind the provision of Section 6 (8) of the Privacy Act: If there is any doubt, it is to be presumed that the data subject failed to provide his consent.

If the data controller has no unambiguous information as to whether the complaint submission can be transferred to the body or person subjected to proceedings in a way that renders the personal data of the complainant accessible, it must request the consent of the complainant prior to transferring it.

If the data controller holds that the proceedings cannot be carried out without the identification of the complainant, it must inform the complainant thereof in order that he or she can, exercising his or her right to informational self-determination, weigh his or her interests in the proceedings or the protection of his or her personal data, and so decide on the fate of his or her personal data.

Beyond the above, data controllers must take into consideration the principle of necessity in processing complaint submissions; if the examination of the complaint does not necessitate the processing or transfer of the name of the complainant, the data of the complainant must not be transferred to the body or person subjected to examination even if the complainant consented to it.

A complainant stated in his submission that he had initiated a disciplinary action against his attorney-at-law at one of the chamber of the attorneys-at-law (hereinafter 'the Chamber'). Before initiating a preliminary inquiry for the disciplinary action, the Chamber transferred his submission on to the attorney-at-law in a way enabling the recognition of his personal data without his prior consent, which the attorney-at-law later used for initiating a civil court case against the complainant. The activity of the attorney-at-law objected to concerned several persons other than the complainant, and the activity subjected inquiry could have been examined without knowing the name of the complainant, and the Authority, in its proceedings, therefore found that the Chamber, lacking obligatory data processing, had violated Sections 5 (1) of the Privacy Act and the requirement of data security under Section 7 (2) of the said act.

V.15. Legitimate Interest as Legal Basis

The two most fundamental legal bases are consent by data subjects and mandatory data processing. Section 6 of the Privacy Act, however, adds to these two the case in which it provides for, in the absence of the consent by the data subject and an explicit legislative provision, under certain conditions, special data processing for the purposes of legitimate interest. Legal basis under Section 6 (2) b) of the Privacy Act was conceived in this way, according to which personal data may be processed even if obtaining the data subject's consent is impossible or it would give rise to disproportionate costs, and the processing of personal data is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, and enforcing these interests is considered proportionate to the limitation of the right for the protection of personal data.

The personal data of the data subject may also be processed under Section 6 (5) (b) of the Privacy Act, because if personal data are recorded under the data subject's consent, the controller shall—unless otherwise provided for by law—be able to process the data recorded where this is necessary for the purposes of legitimate interests pursued by the controller or by a third party, if enforcing these interests is considered proportionate to the limitation of the right for the protection of personal data, without the data subject's further consent, or after the data subject having withdrawn his consent.

In addition, data controllers may apply as a legal basis Article 7 f) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter 'the Data Protection Directive'. Under Article 7 (f) of the Data Protection Directive personal data may be processed if processing is necessary for the purposes of the legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject. In joined cases C-468/10 and C-469/10, the European Court of Justice found that Article 7 f) of the Data Protection Directive has direct effect, and thus data controllers may rely on this legal basis before the courts of a Member State. This legal basis will also be applicable under Article 6 (1) f) of the General Data Protection Regulation.

By the regulatory experience of the NAIH, data controllers are often not aware of when they can rely on a legitimate interest as a legal basis, or, if they do, they do so wrongly.

It is general practice, for example in data processing related to workplace control, to electronic observation systems in particular, that employers operate surveillance camera systems based on employee consent. The Authority has repeatedly explained why the consent cannot be used as a legal basis. Nevertheless, it is still not widely known to employers that data processing may based on legitimate interest as a legal basis, and, if known, they rely on this legal basis without justifying their necessary and legitimate interest in data processing by the results of an interest balancing test carried out prior to the processing of data.

Other general examples include financial institutions dealing with claims management which, in their data processing notices, justify the legal basis of their data processing founded on interest balancing by only literally quoting Sections 6 (1) and (5) of the Privacy Act. In their notices, they do not indicate which legal bases are used for the processing of what data, which legitimate interests are applied in what cases, and also rely on the legal basis of interest balancing without justifying it by the results of a balancing test carried out prior to the commencement of data processing. It is common to deliberately omit the balancing to avoid data erasure.

Regardless of whether the data controller refers to the Privacy Act, the Data Protection Directive or the General Data Protection Regulation effective as of 25 May 2018, the balancing test must in all cases be performed. The balancing test is a three-step process that identifies the legitimate interest of the data controller and as the counter-weight, the data subject's interest, his or her fundamental right, and ultimately, based on the balancing, it must be established whether the personal data can be processed or not. When performing the test, the data controller has to take into account a number of criteria depending on the data processing, but in all cases it is required that the results of the test—why the data controller considers that his interest in the data processing may proportionately limit the interests and rights of the data subject—should provide information to the data subjects.

Documenting the balancing test is also important, because the General Data Protection Regulation has raised the principle of accountability to the highest level, according to which the data controller is responsible for compliance with all other data processing principles, data protection requirements, and also verifying such compliance.

For example, the Authority examined the issue of legitimate interest as a legal basis in the following specific cases.

In data protection administrative case no. NAIH/2017/280 /H, the complainant objected to an electronic surveillance system at his workplace, an elderly home, and that the employer had failed to comply with the obligation to provide information on the surveillance system.

In the Director General's instructions on the operation of the camera system, the data controller referred to legitimate interest as the basis of data processing, the monitoring employees. The data controller stated that it is typically elderly residents of the institution that stay in the areas monitored by the cameras, thus they can be regarded as data subjects, and the same persons are the recipients of the data—in the interest of whom the camera system is in operation. Therefore 'the balancing of interests could not be carried out in our Institution in a formal logical, paradigmatic sense, as the data subject and the recipient of the data coincide, form a mathematical set, and constitute a monopolar system.' In its decision, the Authority ordered the data controller, inter alia, to carry out balancing test to justify the legal basis referred to. This, the data controller fulfilled at the end of the proceedings.

In examination proceedings no. NAIH/2017/435/V, the basic problem objected to by the complainant was that the staff of an electricity supplier took photographs of his real property classified as personal data in order to prove

their failure to access the property for replacing the gas meter, the obstruction of which by the consumer is deemed to be a breach of contract. As a legal basis for data processing, the data controller referred to Section 6 (1) a) of the Privacy Act, but, on the basis of its first reply in the course of the investigation, it could not be established that the data controller had developed and conducted a balancing test prior to the data processing based on legitimate interest, and whether it was generally aware of, and whether or not it applied, a test applicable for the balancing of the interests in question.

Given the above-mentioned shortcomings, the Authority ordered the data controller to develop an appropriate balancing test, and to make his findings available to the relevant customers. Finally, the data controller submitted an acceptable test, and thus the Authority closed the case.

V.16. The Right to be Forgotten

In our information society, with freely uploadable and editable content on the Internet becoming general, content control is increasingly seen as a priority, that is to say, the right of data subjects to request the deletion of online information relevant to them. In 2017, the Authority received several requests regarding the right to be forgotten.

The most important decision on this issue is the 'Google judgment',[31] the points of which the Authority outlined in a brochure,[32] and uses to assess similar cases ever since.

There are basically two types of situation that can be distinguished. The first is when the data subject requests the operator of the website disclosing the information, the data controller, to delete his or her personal data or to remove the entire entry. The second is when the data subject requests the operator of the search engine concerned (most often Google) to remove the link in question from the search results. Deletion from the hit list of Google's search engine is not the same as deletion by the data controller. While the former deletes only the access path technically, the latter can erase the data completely.

The ECJ clearly pointed out in its judgment that the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information relating to that person, and the data protection authorities of the Member States, the NAIH included, derive their practice from this judgment. In several cases, however, Google as data controller simply refers to the right of public access as a stronger interest, and does not comply with requests for cancellation.

Following the 'Google judgment', the right to being forgotten increasingly became the focus of regulation, and this necessarily brought about a need to formulate the principles laid down by the judgment in law. This was what took place with the adoption of the GDPR applicable from 25 May 2018, which expressly mentions the right to be forgotten beside the request for the erasure of personal data.[33]

In the GDPR, the right to be forgotten is involved in the provision that a data controller who has made personal data public is not only obliged to erase data in the cases provided for but also to inform other data controllers that the data subject has requested the erasure of any links to his or her personal data. The GDPR also sets out the limits of the right to be forgotten. In the future, a data controller shall not be obliged to comply with the request of a data subject, for example, if data processing is necessary for the exercise of the right to freedom of expression or the right of access to information, or if it is justified by the data subject fulfilling a public role or being a public actor. In all other cases, the data controller must ensure the right to be forgotten and delete the link containing the personal data without delay.

V.17. Data Processing at Sziget Festival

I) *Data processing examined*: the Authority received several complaints regarding the VOLT Festival and the Sziget Festival, in which the notifiers complained of the organizers' admittance practice of scanning the identity cards of the visitors and not adequately informing the data subjects of the circumstances of data processing, including the purpose and duration of storing copies of the identity cards.

II) *Investigation by the Authority*: When admitting visitors to the festivals it organizes, the data controller assigns entry wristbands to them by recording their personal data via scanning their identity cards. The proof of identity with a photo identity card is therefore a prerequisite for participating at the event. During data recording, the bar code of the entry wristband is read, then the identity card is scanned and assigned to the wristband. Where the identity card has a chip from which the scanner can read the required data on the basis of the so-called MRZ code, the data are recorded; however, in the case of the older types of identity card, the scanner reads only the

[31] Judgment of the Court of Justice of the European Union, 13 May 2014, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González: http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=-CELEXCELEXCELEX%3A62012CJ0131

[32] NAIH Brochure on the criteria used in assessing cases related to erasure of data from the list of results of Google's search engine. https://www.naih.hu/files/2015-07-29-Tajekoztato_Google_talalati_list_eltavol.pdf

[33] Article 17 of the GDPR.

personal data (name, date of birth, type of document, its number, country/nationality, gender), not the profile picture, and so it is necessary to scan and store it.

According to the company's statement, the new admittance system was introduced due to the increasing number terrorist attacks in Europe. In their view, the identification of the visitors when receiving the wristband significantly reduces the risk of a terrorist attack.

The company indicated consent by the data subject as the legal basis for data processing, and argued that the processing of the personal data of visitors upon admittance is a degree of restriction not disproportionate to the aim pursued, namely the protection of the visitors' right to live and the prevention of other abuses. In addition, they emphasized that the application of the system they developed—through general and specific prevention—is capable of forestalling or preventing terrorist acts.

III) *Findings*: The Authority reviewed all applicable legal bases for the data processing examined and evaluated the provision of prior information practice of the data controller.

a) According to the Authority, consent cannot be considered to be an appropriate legal basis where there is no other data processing or paid service available without consent. There is therefore no real choice for the data subjects concerning admittance data processing.
b) Although the data controller did not apply it in its rules, it argued for the application of another legal basis, that based on legitimate interest, in the course of the investigation procedure. In assessing this, the Authority examined the conditions for applying it, that is to say, the existence of certain elements of the balancing test (identification of the legitimate interests of the data controller or of a third party, the determination of the data subjects' interests, the examination of whether it is absolutely necessary to process personal data for achieving the purpose, and the final weighting).

The Authority considered guaranteeing the security of festival visitors as an important and acceptable purpose, in which the economic interest of the organizer of the event and the safety of citizens, and the public interest are simultaneously present.

In examining the indispensability and appropriateness of the applied practice, the Authority brought up several examples of admittance procedure at European festivals of similar size to demonstrate what other methods can provide a high level of protection by means less damaging to the information self-determination rights of data subjects.

The Authority considers the applied means and method of protecting the safety of visitors inappropriate to achieving the purpose, and regards the scanning of identity cards and the related data processing, as well as the legal restriction it involves as disproportionate thereof.

c) In its decision, the Authority stated that guaranteeing the safety of festival visitors would be in the public interest, and, in this case, taking measures and steps to ensure an adequate level of protection is typically a public task. Consequently, according to the Authority, it would be a solution if the legislator regulated the matter adequately and provided the legal basis for processing the data absolutely necessary to achieve the appropriate level of protection.

In view of the above, the Authority called on the company to review and modify its admittance system and data processing practices, as well as to prepare its data processing notice and rules to provide adequate information to data subjects. The Authority also called the attention of the data controller to the obligation to comply with the GDPR when reviewing its data processing practices.

V.18. The Data Processing of The Church Scientology in Hungary and its Central Organization
(Abbreviated)

Both the Data Protection Commissioner and the Authority have examined the data processing of the Church of Scientology in Hungary on several occasions. Complaints by data subjects made the unlawful processing or personal data look probable. It was also likely that unlawful processing of data affected a very wide range of people and special data as well, and thus the Authority *ex officio* opened administrative proceedings for data protection. In order to clarify the facts of the case, the Authority conducted on-site inspections without prior notification, and seized documents and electronic media. It also appointed a forensic informatics and a forensic clinical psychologist expert.

The reviewed data processing activities are linked to four data processing purposes, namely:

i. The purpose of data processing related to services ministered to believers and to following their spiritual development is primarily linked to PC and Ethics Folders;

ii. The purpose of data processing related to the appointment, aptitude of staff members and the disclosure of information to authorities is primarily linked to Staff Folders;
iii. Direct marketing purposes are primarily linked to Mailing Files;
iv. Persons and property protection purpose is primarily related surveillance cameras.

PC Folders contain notes, records, work sheets, reports made in the course of auditing and detoxification, the major services the Church provides, which include a large amount of personal and special data of believers and third persons.

Auditing is a precisely planned procedure in which the auditor (a Church minister) and his or her patient (a believer, or preclear) participate; the auditor asks questions, and the believer answers, which the auditor acknowledges and takes note of. Auditing is supported by a 'religious artefact', the E-meter. According to the findings of the psychologist expert, most of the methods used in auditing induce altered consciousness (and are virtually hypnotherapy), but the other methods used also result in the narrowing of consciousness and social submission in the subject. Both suggestive, mind-altering methods (hypnotherapy) and biofeedback constitute therapeutic procedures, healthcare activities.

The believers share extraordinarily large amounts of often specially sensitive data during auditing sessions, and the auditor often records the data of other, non-member persons, the personal and special data of third parties.

PC Folders are used to hold several documents containing sensitive data on the PC concerned, such as former diseases, surgeries, bodily and mental conditions, marital status, personal data of family members, etc.

Detoxification, which according to the forensic psychologist expert has nothing to do with the medical science therapy, consists in diets, consumption of defined types and quantities of vitamin, taking saunas and physical exercises, and their aim is—according to the Church of Scientology—to purify and clean the human body of chemical and drug residues that might obstruct reaching the results of Dianetics or Scientology auditing/processing.

Prior to detoxification a medical examination is required and the completion of a form on medical fitness, which is stored by the Church, and includes the personal and special data of the believer (e.g. blood pressure, symptoms of anaemia, heart, liver disease, diabetes, use of drugs, medicines taken, surgery, etc.)

With regard to the PC Folders, the Authority found that the notices required to be signed by the believers before the start of services do not provide appropriate information, because they do not identify the data controller, and the purpose of the date processing is outlined far too briefly. For a data processing involving complex and large amounts of personal data like the one examined, the purpose of data processing should be outlined far more precisely and clearly, and the data to be processed for the given purpose should also be delineated, because it is only on this basis that the data subject can decide whether or not to consent to the data processing. The notices do not identify clearly which church persons, officers, and staff members are entitled to access the data, neither do they provide appropriate information on the rights of data subjects; consent is not obtained for data transfers; moreover, believers are not entitled to access the PC Folders made on them.

The Authority furthermore found in respect of the detoxification programme that, only the examining physician or the medical service provider may process—with consent—the health data collected, the records of the medical check-up, and can transfer the information that the data subject fulfils the conditions of participation in the programme or not, but the full content of the declaration together with the detailed data on the medical check-up and medical reports should not be handed over to a religious organization in the opinion of the Authority.

The particularly grave violation of law the Decision found was the processing of the personal data of third persons, e.g. family members, friends, acquaintances, love relations of the PC. It occurred in several cases that the Church processed in certain documents the special data of third persons in spite of the fact that it had not obtained consent from the data subjects.

By processing data without the provision of information, the data controller, the Church, acquires a 'dominant informational position', which is extremely damaging to the protection of personal data and the right to privacy of these third parties, they cannot enforce their right to informational self-determination, and, moreover, the data processing is qualified as unfair.

Collecting and recording the data of data subjects who qualify as third parties not being in any legal, membership, relation with 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 special 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.

In view of all these, the Authority prohibited, in the operative part of its decision, the processing of medical data, and ordered the provision of appropriate prior information to the believers, obtaining their repeated consent, as well as the erasure the personal data of the believers who did not give their repeated consent and of any third parties, and prohibited the Church's practice of collecting third party personal data.

Ethics Folders include also 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' and other reports in the Ethics Folders contain large amounts of often extremely sensitive data. In these believers write various reports on each other, calling attention to their irregular conduct, lifestyle, work in the Church, and love relations. The reported irregularities range from insignificant 'sins' to others' health, financial or sex life, or even crimes a believer committed.

The folders regularly include information on believers' arrears (to the tax office, services or private persons) and borrowings.

This type of folder is used for keeping the documents of the CSH internal judicial procedures. As it appears in 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. For the examination and sanctioning of ethics and other wrongs, various procedures were developed by the Church.

Documents produced on the internal judicial procedures are typically drafted in, or evidence in Hungarian is translated into, English. These folders contain very detailed procedures, much like 'secular' judicial proceedings, and include all the related 'Knowledge Reports' and other reports, ethics reports with health data, social security numbers, ambulant treatment sheets (e.g. one related to harassment), outpatient medical records, forensic medical opinions, or, for example, the records of interrogations of a party to a suit on sex life and prostitution, and some filled-in Life History Forms known from Staff Member Folders can also be found in these folders.

The Authority found that the infringements of law established in respect of documents presented above can be established in this type of folder, as well, that is, processing of personal and special data without appropriate lawful basis in respect of believers and third persons.

The other important area of the proceedings was the group of data recorded in Staff Member Folders. Prior to employment with the CHS Central Organization, applicants have to undergo a lengthy admission procedure in the course of which they have to complete several application forms, aptitude tests, and questionnaires, providing an extraordinary large amount of personal and special data to the Church.

The forensic psychologist expert emphasized in respect of these tests that their use is unprofessional, questions in many cases cannot be linked to any psychological feature, are too general, or contain elements that cannot be answered clearly, a testee will answer correctly if his worldview is the same as that of Scientology. Presenting this test method without the prior information of the subject that no well-founded conclusion can be drawn from it constitutes deliberate misrepresentation.

Among the applications forms to be filled in, there is the 'Life History Form' containing 130 questions, which requires—in the opinion of the Authority, unlawfully—data on e.g. the data subject's debts, possible secret service activities, participation in the media, military services, government agencies, drug use, former diseases, surgery, etc. But not only is it the personal and special data of the applicant believer that are so processed but also those of third persons, because applicants must provide details of their former love relations, sexual customs, and also the data of their family members and friends.

With regard to Mailing Files (Central File) and direct marketing (Addresso database), the Authority examined the various paper-based forms used by the Church for direct marketing purposes, the notices used for website book selling and online tests, as well as the Addresso electronic database, and found the data processing of the Church for marketing purposes as unlawful in two respects, namely:

- it did not obtain consent by data subjects, and
- the source of the consent of the data subjects cannot be established.

In view of the above, the Authority prohibited the Data Controllers from unlawful data processing, and required them to modify their practice of providing prior information and provide prior information, to request all data subjects to consent or reaffirm their consent to data processing. In the lack of consent, they were required by the Authority to ensure the documented erasure of the data of the data subjects. They were prohibited by the Authority to desist from their practice of collecting the personal data third parties not qualifying as staff members, employment applicants and believers, and were ordered to erase or destroy data processed in this way. They were also required to terminate the transfer of data to other countries.

Simultaneously, the Authority imposed a maximum data-protection fine of HUF 20 million on each of the two Data Controllers. In establishing the amount of the fine, the Authority considered all the circumstances of the case, particularly the number of those concerned, the gravity of the infringement of law and its being a repeated offense. The case is currently under judicial review.

V.19. A Small Key: The Continuation of the NAIH Children's Rights Project

The National Authority for Data Protection and Freedom of Information (NAIH) has laid particular emphasis on the protection of the personal data of children; this was why we published our volume of studies entitled *Key to the World of the Net!* on the Internet habits of children between 10 and 16 (a new edition of which came out in 2016, updated and supplemented with current topics); this was why we launched our awareness campaign with Tamás Vastag's song in 2014; and this was why we joined the ARCADES project of the European Union whereby reference books on data protection were published for teachers (in Hungarian, too).[34]

The aim was always the same: to help children and youths—directly and by way of assistance from adults responsible for their upbringing—live consciously in the world of the Internet, not only be smart but also knowledgeable at using these devices, and also to take responsibility for others in virtual reality, as well.

The 'super-now' generation, those born after 2000, displays features of Internet use that have not been characteristic of those born earlier. The most serious problem is—experts maintain—that children are drawn in a selfish and aggressive direction. Kindergarten has an enormous role, as it is where group or community life begins, which is then given a further 'twist' by schools with their performance pressure. All age groups have their own characteristic learning processes; if these are interiorized in the wrong way, they may result in problems for the individual, family, and even society. Children use the Internet as a sort of 'situation report' ('it's break, I'm out in the garden'; 'I'm havin' my apple pie', etc.), not necessarily conveying genuine feelings. The media and milieu establish the rules of conduct; and the child is either sensitive to this or not. A conscious and natural use of the Internet should be directed toward supplementing personal presence and obtaining genuine knowledge; however, youths use digital equipment for purposes of a much wider range; eventually, a normal practice will develop and crystallize between these limits.

The most powerful model is the parent here as well. It is primarily up to the parent to teach the child the rules of using the Internet, thus the parent has to acquire information beforehand, and set the rules of the immediate environment. The best is when parents discover his world together with their children, and not simply exercise their external control. The safe use of the Internet can only be learned in practice, and all users have a responsibility in this, because they are the ones that shape, and can shape, their culture.[35]

In our experience, education for this purpose cannot be begun early enough, because, on the one hand, everyone, regardless of age, has the right to the protection of personal data when encountering danger, and, on the other hand, the age groups using the Internet is becoming younger and younger. There is no wonder; a baby is born into an environment where mobile phones and computers or other devices are used as everyday tools, and, in some cases and for some people, they are more important than anything else. However, while, in the cases of adolescents, the emphasis falls on preparing them for independent decision making, in the case of children under ten, protection is of primary importance.

In 2017, the NAIH has thus focused on children under 10. This study volume seeks to map those sources of danger that might infringe on the privacy kindergarten and school children, the protection of their personal data, and thereby damage their future healthy development. Our aim is certainly not to deter; rather, it is to call attention to digital-space phenomena that may affect the youngest age groups now and in the future.

[34] https://www.naih.hu/adatvedelemr-l-fi ataloknak--kulcs-a-net-vilagahoz--projekt.html

[35] Mátraházi, Tibor (psychologist) in.: SomogyTv: 'Miért?' (Why?) – Mátraházi Tibor | 27/01/2017. 18:41:00 (http://www.somogytv.hu/videok/miert/118569/)

VI. Data-protection Audits and BCRs

VI.1. Binding Corporate Rules

The NAIH approved of 14 *binding* corporate rules (hereinafter 'BCR'). In each of the approved BCR cases, the NAIH conducted co-operation procedures as per Working Document WP107 of the Article 29 Working Party and the approval of the lead authority before NAIH did so.

The NAIH approved of the following BCRs by data controllers (or groups of data controllers) in 2017, the names of which uploaded on to the website of the authority for informing data subjects (https://www.naih.hu/a-bcr-t-magyarorszagon-alkalmazo-adatkezel-k.html):

Data of approval	Name of Corporate Group	Name of Data Controllers a Applying BCRs in Hungary
2017.11.29	IBM	IBM Magyarországi Kft.
2017.11.29	IBM	IBM Data Storage Systems Információtechnológiai Kft.
2017.11.29	IBM	IBM Hungary International Shared Service Centre Kft.
2017.11.29	IBM	IBM Capital Hungary Kft.
2017.11.29	Schneider Electric	Schneider Electric Hungária Villamossági Zrt.
2017.11.29	Schneider Electric	SE-CEE Kft.
2017.11.29	Schneider Electric	M&C Energia Kft.
2017.11.29	Schneider Electric	Schneider-ElectricEnergy Magyarország Villamos Kapcsolóberendezések Gyártó Kft.
2017.10.30	Cardinal Health	Cardinal Health Polandspółka z organiczonąodpowiendzialnością
2017.10.04	Atos	ATOS Magyarország Kft.
2017.10.04	Atos	Atos International Kft.
2017.10.04	Atos	UnifyCommunications Szolgáltató Kft.
2017.07.11	Merck Sharp &Dohme (MSD)	Intervet Hungária Kft.
2017.07.11	Merck Sharp &Dohme (MSD)	MSD Pharma Hungary Kft.
2017.05.23	Michelin	Michelin Hungária Abroncsgyártó Kft.
2017.05.23	Accenture	Accenture Tanácsadó Kft.
2017.05.23	Accenture	Accenture Industrial Software Solutions Kft.
2017.05.12	SanofiAventis	CHINOIN Zrt.
2017.05.12	SanofiAventis	SANOFI-AVENTIS Zrt.
2017.04.25	Mastercard	Mastercard Europe SA Magyarországi Kereskedelmi Képviselete

2017.03.31	ENGIE	GDF SUEZ Energia Holding Hungary Zrt.
2017.03.31	ENGIE	Égáz-Dégáz Földgázelosztó Zrt.
2017.03.31	ENGIE	COTHEC Energetikai Üzemeltető Kft.
2017.03.31	ENGIE	COFELY Épületgépészeti Kft.
2017.03.31	ENGIE	FABRICOM ELECTRICAL-PVV Villanyszerelő Ipari Kft.
2017.03.13	DSM	DSM Nutritional Products Hungary Kft.
2017.03.08	Legrand	Legrand Magyarország Villamossági Rendszerek Zrt.
2017.03.08	Legrand	Legrand Közép- és Kelet-európai Disztribúciós Kft.
2017.01.25	JACOBS DOUWE EGBERTS	JACOBS DOUWE EGBERTS HU Zrt.
2017.01.17	Siemens	Siemens Zrt.

VI.2. Data-protection Audits

The draft amendment of the Privacy Act (hereinafter: 'the Draft') terminates the institution of data-protection audits, in its stead the GDPR provides for data protection certification. This closes a period beginning in 2013 when data controllers requiring a higher level of data protection compliance could have the data protection authority audit their data processing. According to the feedback from audited data controllers, a successful and useful tool is being terminated, which provided important feedback to the Authority on the issues data controllers regarded important, and thus the experience gained during audits was reflected in the recommendations of the Authority.

VII. Freedom of Information

2017 was fundamentally geared towards the preparation of the General Data Protection Regulation for both public bodies and the Authority. However, compliance with the new data protection rules did not mean that the other informational right, the freedom of information, was relegated to the background. On the contrary, the Authority paid more attention to the right to access and disseminate data of public interest and data public on grounds of public interest, and to raising awareness of obligations related to the freedom of information.

As in previous years, the Authority focused on the publicity of data on the management and use of public funds and national assets. Public funds and national assets must be managed according to the principles of transparency and the purity of public life. For the realization of the values and goals enshrined in the Fundamental Law, the existence and enforcement of the freedom of information is indispensable.

In 2017, the Authority expanded and developed its practice in the application of the rules of the reimbursement of costs regarding requests for data of public interest. 2017 was the first year in which the relevant regulations were already in force throughout the whole year. The public bodies applied the rules of charging fees in ways that led to infringement of law on several occasions. In each case, the Authority not only tried to consider facts and circumstances relevant to the particular case, but also to provide general guidance to the bodies and persons concerned.

Finally, it should be emphasized that the Authority continued to play an active role in fulfilling the state responsibilities in the prevention of corruption. In addition, the Authority actively participated at international and European forums on freedom of information. These conferences were primarily aimed at fostering closer international cooperation and the harmonization of different national practices.

VII.1. Transparency of the Use of National Assets and Public Funds

It is a fundamental social requirement for the community of citizens to control the use of public funds and national assets. The supervision of the management of these assets is also supported by—apart from constitutional control mechanisms, the procedures of the State Audit Office, the Government Control Office and the investigating authorities—the enforcement of the freedom of information. The ability of the press, NGOs, and members of society to access and disseminate data of public interest and data public on grounds of public interest is at all times one of the most important values and goals of the democratic rule of law.

The current legal environment, in the spirit of the Fundamental Law and its National Avowal, provides also for fairness in public life, the control of responsible management of the national assets and as its prerequisite, public scrutiny. Accordingly, the provisions of Act CXCVI of 2011 on National Assets (hereinafter 'National Assets Act'), Act CVI of 2007 CVI on State Assets (hereinafter 'State Assets Act'), and the guiding rules of the Privacy Act are designed to enforce the principles of transparency, accountability and the purity of public life. The publicity of the use of public funds and national assets is supervised first and foremost by the NAIH.

In 2017 also, the Authority examined the transparency of the use of public funds and national assets in a number of cases. In the course of its investigations, the NAIH started out from the often-quoted provision of the Fundamental Law: 'Every organization managing public funds shall be obliged to publicly account for its management of public funds. Public funds and national assets shall be managed according to the principles of transparency and the purity of public life. Data relating to public funds and national assets shall be data of public interest' (Article 39 (2)).

This constitutional requirement also covers the traceability and transparency of public finance management and the public accountability of the transfer of national assets. Article 39 (2) of the Fundamental Law, in fact, constitutes one of the most important limits of the exercise of public authority and the use of public funds. First, it ensures their public control by declaring it the fundamental right of individuals; second, it clarifies and supplements this by declaring information on the use of public funds as data of public interest; and, third, it makes transparency the constitutional obligation of bodies managing public funds.

The essential purpose of national assets is to provide for the performance of public service duties, [36] and national assets are to be managed responsibly and properly. The task of national asset management is primarily to run the state and local governments in order to perform public service duties and meet the prevailing needs of society in a transparent, efficient and cost-saving way that is consistent with the existing potential of the state and local governments and based on unified principles; to protect the value and condition of state and local-government property, to use it to increase its value, to utilize it profitably, enlarge it, and also to sell those elements of it that are rendered superfluous for the performance of the state or local-government duties. National assets, their value and changes, are registered by the exerciser of ownership rights. Registering the value may be dispensed with if the value of the given property cannot be determined by nature.[37] Registration shall also include the designation

[36] Section 7 of the National Assets Act.
[37] Section 10 (1) of the National Assets Act.

of the primary-purpose public service duty of the asset. The data registered, with the exception of classified information, shall be public.

In addition, the NAIH also took into account that the Constitutional Court, in Decision 25/2014 (VII.22.) AB, bindingly confirmed that bodies and persons managing or disposing of public assets qualify as bodies with public service functions under the Privacy Act.[38] Data on the management and disposal of state assets that are not data of public interest shall be deemed as data public on grounds of public interest.[39] The Constitutional Court therefore clearly confirmed that the requirement of transparency generally extends to bodies and persons managing public assets, further strengthening the transparency and controllability of the operation of public funds and state assets.

By way of summary, it can be stated that the current legal environment focuses not only on the fact that a body or person actually fulfils a public service duty as defined by law but also on the fact of disposal and management of national assets. Thus the Fundamental Law and the laws detailing its provisions doubly ensure the transparency of the management of public funds. On the one hand, the Fundamental Law itself provides for standards of data of public interest and data public on grounds of public interest. Since this is the basis of the Hungarian legal system, it can be stated that the transparency of the management of public funds is ensured at the highest, constitutional level. On the other hand, taking also into account the rules of the National Assets Act and State Assets Act, the provisions of the Privacy Act on the accessibility of data of public interest and data public on grounds of public interest must be applied in this regard.

1) In one case, the NAIH received a consultation submission requesting the Authority to deliver its opinion whether the salaries and other benefits of the employees of the Pallas Athéné Foundations and of the company they established are to be considered as public information.[40]
In its opinion, NAIH first of all considered whether the Pallas Athena Foundations and the company it established qualify as entities with public services functions. In this respect, the Authority took into account that, under Article 162 (2) of Act CXXXIX of 2013 on the Magyar Nemzeti Bank (hereinafter 'the National Bank Act'), the Hungarian National Bank, in line with its tasks and primary objective, may establish a business association in which it has a majority holding or may create a foundation. In its Decision no. 8/2016 (IV.6) AB, the Constitutional Court explained in this respect that: 'When the state-owned National Bank creates a business association or a foundation, the sources of the assets it contributes to their establishment or operation (starting capital and support later provided) are necessarily public funds.'[41]

In the reasons of that decision, the Constitutional Court found that 'the companies established by the National Bank, in which it is a majority or exclusive shareholder, i.e. it controls them, as well as the foundations the National Bank establishes, manage public funds, and are consequently—as per Section 39 (2) of the Fundamental Law—obliged to ensure the publicity of data in respect of the data of public interest and data public on grounds of public interest they process in accordance with Article VI (2) of the Fundamental Law and the appropriate prescriptions of applicable laws'.[42] Both the Pallas Athéné Foundations and the company they created qualify as bodies with public services functions under the provisions of the Privacy Act.

As a next step, the NAIH examined whether the wages and other benefits of these employees employed under Act I of 2012 on the Labour Code were data public on grounds of public interest in accordance with the Privacy Act and other legislation. In this respect, the Authority emphasized that there is certain group of data where publicity must be enforced relating to the employees of the foundations and company as persons exercising the duties and powers of a body with public services functions. The employees concerned are those whose activities are among the duties of the body with public services functions as defined by law. In their case, it is primarily the information listed in Section 26 (2) of the Privacy Act that can be accessible to anyone: the name, scope of responsibilities, scope of work, and executive mandate of the employees.

In addition to the range of data mentioned above, other personal data of the employees related to the performance of the public service duty may also be deemed to be data public on grounds of public interest pursuant to Article 26 (2) of the Privacy Act. As the use of public funds is at stake, transparency and controllability—being public interest—is of paramount importance. For this reason, the wages paid to the employees concerned, as well as their regular, ad hoc, cash and in-kind benefits, such as holiday rebates, bonuses, substitution fees, earning allowances, and target bonuses, qualify as personal data arising in connection with the performance of the public service duty, which anyone can access.

At the same time, the freedom of information and the right to informational self-determination must be enforced with mutual respect to each other; thus defining the range of other personal data relating to performing public service duty must take into account whether their publicity does not disproportionately violate privacy rights.

[38] Section 5 (2) of the State Assets Act.
[39] Section 5 (1) of the State Assets Act.
[40] Case no. NAIH/2017/871/V.
[41] Reasons (19) of Decision no. 8/2016 (IV.6) AB.
[42] Reasons (29) of Decision no. 8/2016 (IV.6) AB.

According to the NAIH's practice in this regard, the information under Section 26 (2) of the Privacy Act concerning those employees whose activities are not directly related to the performance public service functions of the authority may not be accessible. This includes, inter alia, employees who do not take part in decision making, neither in the preparatory nor in decision-making stage. Examples include drivers, cleaning staff, etc.

2) In another case, the complainant requested the NAIH to investigate an application for disclosure of data of public interest not fulfilled by Magyar Villamos Művek Zrt (MVM).[43] The purpose of the request was to obtain copies of the documents relating to the granting of assistance to the Civil Összefogás Közhasznú Alapítvány (Civic Union Public Benefit Foundation; CÖKA). MVM refused to fulfil the data request, stating that: 'the support was covered not from public funds but from its own resources', and thus information about it was not subject to Article 26 (1) of the Privacy Act.

In the course of the investigation, the NAIH found—from publicly available company data—that MVM's sole shareholder is the Hungarian State, which exercises its shareholder's rights through the Hungarian National Asset Management Inc. Pursuant to the relevant provisions of the National Assets Act and the State Assets Act, the MVM constitutes national and state assets. Consequently, the MVM qualifies as a body with public service functions, which is obliged to enforce the right of access to data of public interest and data public on grounds of public interest.

The NAIH also stated in its opinion that MVM manages public funds, therefore information on its management, the use of the funds it manages, constitute data of public interest under Article 3 (5) of the Privacy Act and Section 39 (2) of the Fundamental Law. By denying to fulfil the request to access data, MVM therefore violated the fundamental constitutional right of the data requester to access data of public interest.

3) NAIH delivered a similar opinion following an investigation concerning the unlawful denial of a request for disclosing data of public interest by Antenna Hungária Zrt.[44] In this case, the company claimed in response to NAIH's first warning that revenue from its own market activity did not fall within the concept of public funds, and also denied its being a body with public services functions.

In its opinion, therefore, the Authority called the attention of the company to the fact that several factors justify why publicly owned companies qualify as bodies with public service functions. On the one hand, these entities perform a wide range of public or municipal activities and tasks. The laws themselves name the specific companies that carry out prominent public service duties. On the other hand, the financial and other assets available to the companies owned by the state or local government constitute state or national assets.[45] These companies make decisions on them, their management, and use. Now, pursuant to Section 7 (1) of the National Assets Act, the fundamental function of national assets is exclusively to ensure the fulfilment of public service duties. Under Section 5 (2) of State Assets Act, bodies managing public funds qualify as bodies with public service functions. Limiting the group of the entities solely to those defined in the formerly effective annex of the State Assets Act would therefore amount to emptying out the regulation, and consequently lead to an unconstitutional restriction of the fundamental right to freedom of information.

It follows from the foregoing that a company owned by the state or a local government 'is obliged to ensure access to the data of public interest [and data public on grounds of public interest] it processes as a body with public service functions in accordance with provisions of law'.[46] Now, under Section 3 (5) of the Privacy Act, the data of public interest includes all information relating to the activity of the body with public service functions, or arises in relation to the performance of a public service duty, 'in particular data concerning the scope of authority, competence, organizational structure, professional activities and the evaluation of such activities covering various aspects thereof, the type of data held and the regulations governing operations, as well as data concerning financial management and concluded contracts'. However, the relevant legislation does not include any exception for the 'management' of a body with public service functions, and this includes funds from either the state and local governments or market sources. The procedure of Antenna Hungária Zrt thus continued to fail to comply with the fundamental constitutional right of access to data of public interest.

4) In another case, the NAIH investigated the request for data of public interest that was not performed by Bp2017 Nonprofit Kft.[47] In doing so, the Authority emphasized that the company as a body disposing with national assets was not to have denied the request for data on certain contracts it had entered into under Section 27 (3) and (3a) of the Privacy Act, even on grounds that some of the data contained therein cannot be disclosed. According to the so-called data principle, data subject to disclosure restriction in the document must be rendered unrecognizable, while the information that can be disclosed shall be supplied in a readily intelligible form and by way of the

[43] Case no. NAIH/2017/4100/V.
[44] Case no. NAIH/2017/5250/V.
[45] Reason (22) of Constitutional Court Decision no. 8/2016. (IV. 6.) AB.
[46] Reason (46) of Constitutional Court Decision no. 25/2014. (VII. 22.) AB.]
[47] Case no. NAIH/2017/2725/V.

technical means asked for by the requesting party.[48] The NAIH therefore found that Bp2017 Nonprofit Kft. violated the relevant provisions of the Privacy Act.

5) The NAIH also examined the question concerning the publicity of the annex to the contract for modernizing public lighting disclosed on www.gyal.hu. The mayor's office of Gyál only partially fulfilled the request for data provision, because, in its view, the disclosure would have affected business information. During the course of the proceedings, the NAIH reviewed the documents (more than 350 pages) requested to be accessed and the information contained therein in detail. It then found that the disclosure of the data contained in certain parts of the documents—with the exception of (personal) data public on grounds of public interest pursuant to law (chamber and company registration)—may be lawfully restricted on grounds of legitimate business interest under Section 2:47 of Act V of 2013 on the Civil Code and Section 27 (3) of the Privacy Act. However, access to the information not specified in the opinion cannot cause disproportionate damage to business activity, and should therefore have been made available to the requester of the data, which it was made following the investigation.

6) The NAIH also investigated the Heves Megyei Vállalkozás- és Területfejlesztési Alapítvány (Heves County Foundation for Enterprise and Regional Development, hereinafter 'the Foundation') for denying a request for data of public interest that, in its view, would have harmed the personal interests of its clients due to a confidentiality agreement.[49] The Authority found during its proceedings that the founders of the Foundation included the Local Government of Heves County, the Local Government of Eger County, the City of Hatvan, and the Hungarian Foundation for Enterprise Promotion. For this reason—and in view of the rules governing the transparency of national assets management—the NAIH deemed it unacceptable for the body with public service functions to conclude a confidentiality agreement with its clients in order to limit the disclosure of data of public interest and data public on grounds of public interest process. It is thus closely linked to the transparent and accountable operation of the Foundation, a body managing public funds, to disclose the data in all the detail the requester asked for.

7) The NAIH also investigated whether the monthly allowance given to Shane Tusup, Olympic champion Katinka Hosszú's trainer, by the Magyar Edzők Társasága ('Hungarian Coaches Society', MET) in the framework of the Special Coaches Programme qualified as data public on grounds of public interest.

In the course of its proceedings, the Authority found that the financial source for the operation and financing of the Programme was provided by the appropriation for the development of priority sports in the Act on the Central Budget of Hungary. Consequently, the funds managed by the Programme qualify as public funds, and thus constitute data of public interest within the meaning of the Fundamental Law.[50] Under effective legal provisions, on the other hand, a natural person who establishes a financial or business relationship with a person subject to a subsystem of general government finances is obliged to provide information to any person on the data public on grounds of public interest arising from that relationship.[51] This includes, inter alia, Shane Tusup's share of the sum under the subsidy contract concluded between the Ministry of Human Resources and the MET.

Finally, the NAIH took into account the fact that the salary paid to Shane Tusup under the employment contract with MET qualifies as data public on grounds of public interest pursuant to the Privacy Act.[52] If it is not possible to know what kind of benefits the professionals participating in the Programme are entitled to, the control of the use of public funds provided for by the Fundamental Law is not ensured.

VII.2. Rules of the Reimbursement of Costs Regarding Data Requests

Since the amendment of the Privacy Act, which came into effect on 1 October 2015, bodies with public services functions had the opportunity—in certain defined cases—to charge a fee for fulfilling data requests. The Government adopted Decree 301/2016 (IX. 30) on the Costs of Disclosure of Information (hereinafter: 'the Decree'), which came into force on 15 October 2016. The experience gained during its practical implementation in the more than a year-long period after its coming into force and the guidance issued by the Authority can be summarized as follows.

It should be noted first that with regard to the rules of the Privacy Act, charging a fee is not obligatory, but left to the discretion of the body concerned. It is therefore always up to the given body with public service functions to decide whether it wishes to exercise this right or not. If the body wishes to charge a fee, it has the opportunity to do so in the case of those requests that were filed after the Decree had come into force and under its provisions. The NAIH examined several data requests that had been submitted prior to the Decree coming into force. In fulfilling these requests, the bodies with public services functions might charge fees for costs in accordance with the principles and rules laid down by the practice of the NAIH. In several instances, the NAIH called the attention of public duty bodies that they could decide to omit reimbursement.

[48] Section 31 (1)–(2) of the Privacy Act.
[49] Case no. NAIH/2017/1368/V.
[50] Section 39 (2) of the Fundamental Law.
[51] Section 27 (3) and (3a) of the Privacy Act.
[52] Section 26 (2) of the Privacy Act.

Fulfilling a data request does necessarily involve certain amount of workforce allocation—this is an institutional concomitant of the fundamental right of access to data of public interest. The measure that might be established under the Decree also does not mean that the data controller can enforce it in all cases, because the fees must correspond to real costs; thus if the fees are lower than the amount defined by the Decree, the data controller must take the actual cost into account.

On the other hand, it should be noted that, the fulfilment of requests regarding data of public interest is still not subject to VAT, because, according to Section 2 of Act CXXVII of 2007 on Value Added Tax (hereinafter 'the VAT Act'), the scope of the Act covers the supply of goods and services for consideration within the domestic territory by a taxable person acting as such, the intra-Community acquisition of goods for consideration within the domestic territory, and the importation of goods. Under Section 5 (1) of the VAT Act, a 'taxable person' shall mean any person or organization having the capacity to perform legal acts who (that), in its own name, carries out in any place any economic activity, whatever the purpose or results of that activity. According to Section 6 (1) of the VAT Act, 'economic activity' shall mean any business activity carried out independently on a regular or continuing basis for the purposes of obtaining income, or that results in the obtainment of income.

In accordance with the Privacy Act, the Decree provides for three cost elements in determining the fee chargeable. During performance, only the cost of the data storage device, of the delivery, and of the workforce needed may be taken into account. No other cost elements may be charged.

In the course of implementing the Privacy Act, most of the problems arose due to the reimbursement of the workforce necessary for fulfilling requests for data, particularly in the light of the fact that the largest part of the fees to be paid by data requesters was the cost element in most of the cases.

According to the Decree, 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 HUF 4,400). Other contributions, bonuses, rewards and other benefits, such as fringe benefits cannot be taken into account.

According to Section 29 (5) point c) of the Privacy Act, if the fulfilment of a request for data requires a disproportionate use of the workforce needed for the ordinary operation of the body, the additional work costs needed may be taken into account in determining the fee chargeable. In other words, additional work costs may be taken into account when the public body:

I. the workforce needed for its ordinary operation,
II. is required disproportionately, and
III. the period of using the workforce exceeds four working hours.

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

In 2017, the NAIH developed the criteria and methodological principles that were used to examine what constitutes disproportionate use of the workforce when determining the rate of reimbursement. The NAIH considered information such as the number of people working in the public body, the position of the staff participating in fulfilling the data request, and relationship of the position of the staff involved in fulfilling the data request to the ordinary operation of the body, and which basic activity the body could or could not perform due to fulfilling data request. During the investigations, the NAIH asked why the bodies thought the workforce required to fulfil the data request was disproportionate, and that the data the requester wanted to access was of substantial size. The NAIH also took into account the technical conditions at the disposal of the public body (for example, the number of printers and scanners available in the institution, and how long they were used to fulfil the data request). Naturally, it was also necessary to examine whether the data requested was available in the desired format. The NAIH investigation also covered whether the requested data was included the Standard Disclosure List in Annex 1 of the Privacy Act, i.e. data the public body should have already made electronically accessible.

Section 29 (4) of the Privacy Act states that, if the fulfilment of the data request means a disproportionate use of the workforce of the public body needed for its ordinary operation, or the document or part of a document of which the copy had been requested is substantial in size and/or volume, and the reimbursement amount exceeds the amount defined by the Decree, the copy shall be provided within fifteen days from the date of payment of the fee. The requesting party shall be informed within fifteen days of filing the request that the fulfilment of the data request means a disproportionate use of the workforce of the public body needed for its ordinary operation, that the document or part of a document of which the copy was requested is substantial in size and/or volume, and also of the reimbursement amount and the alternate solution available instead of making a copy.

In the opinion of the Authority, the cost of data requests may be advanced in two cases:

I. If the fulfilment of the request for information entails a disproportionate use of the workforce necessary to perform the basic tasks of the public body, and the reimbursement amount exceeds the amount specified in the Decree;

II. If the document or part of the document of which a copy was requested is substantial in size, and the amount of reimbursement exceeds the amount specified in the Decree (HUF 5,000).

Consequently, the two conditions mentioned must be met together. An additional condition for the advance payment of the costs of data requests is that the data controller informs the requesting party about the fact, reason and the amount of the reimbursement fee within 15 days of receiving the request. In this regard, the NAIH is of the opinion that, if a public body wishes to apply Section 29 (4), i.e. to make the fulfilling of the data request subject to prior payment of the fee, it is obliged to notify the requesting party within 15 days of receipt of the request. In all cases where the body exceeded the above deadline, the NAIH ordered the data controller to fulfil the data request without charging a fee.

In order to orient the relevant practice, it is also important to note that Section 29 (2) of the Privacy Act provides also for extending the deadline for fulfilling data requests. The legislator regulated the extension of the deadline for fulfilment and the payment of the fee so that the public bodies can, at their discretion, rely on one or another law, or both at the same time. The conditions for the cases under Section 29 (2) and (4) of the Privacy Act essentially correspond to each other. It can therefore be concluded that the fifteen-day deadline for providing information under Section 29 (4) of the Privacy Act must be complied with, regardless of whether or not the body extended the deadline for fulfilment or not. In this case, the obligation to provide information is not linked to the extension of time for fulfilment.

If the data request is fulfilled electronically, the time required for making a copy in accordance with the Decree 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 provide the electronically available data. That is, in the case of data required in electronic form, the duration of using the workforce may only be taken into account if:

– the data is not available in electronic form (it must be scanned), or

– scanning/copying would be faster than searching for an electronic file.

The NAIH continues to hold that the bodies with public services functions do not provide services when fulfilling requests for information of public interest, but comply with their obligations arising from the fundamental right enshrined in the Fundamental Law. Moreover, it is not on a commercial basis that these bodies sell copies of documents, but they have the opportunity to request the data requester to reimburse material costs.

Finally, the NAIH emphasizes that the proper enforcement of the freedom of information requires the transparency of the procedure for determining reimbursement. Transparency is best served by the institution of providing information on reimbursement for the fulfilment of requests for data public interest. Under the Privacy Act, the bodies with public services functions must communicate the amount of reimbursement to the requesting party in advance. Section 29 (3) of the Privacy Act uses the term ‘amount’, while Section 29 (4) provides for the ‘measure’ of reimbursement. However, simply communicating the amount can give rise to abuse. For a communication on the amount does not in itself enable the determination of whether the fee was charged lawfully. The Authority therefore set down additional minimum requirements for providing information. In the interest of the freedom of information as a fundamental right, information on fees charged for costs of fulfilling a request for data must be sufficiently detailed; the bodies with public services functions must therein state any reason or cost element that justifies the amount charged. Appropriate information greatly contributes to making the requesting party truly understand and be aware of why he or she should pay for receiving the data requested. Based on the information, the requesting party will also be able to make the appropriate decision regarding the remedies available. According to the NAIH, the provision of information is sufficiently detailed if it contains the factual and legal justification of the fees charged. If additional workforce is used, the number of employees and the number of hours accounted, as well as the sum broken down to hourly work per employee must be shown. Both recourse to legal remedies and the NAIH proceedings are made easier if the data controller describes the work processes that were/would be necessitated for fulfilling a data request. When a copy of significant size is required, the provision of information must give details, such as the amount of paper the data request involves. Lastly, the data requester must be informed of alternate solutions available instead of making copies.

Determining costs requires preliminary calculations. This means that the entity with public services functions may request the data requester to reimburse the costs established on the basis of an estimate made prior to fulfilment, who is obliged to pay it if he or she continues to request the data after being informed thereof. However, cost reimbursement must always be limited to the cost directly and actually incurred in providing the data. Thus, it must be borne in mind that there may be a difference between the costs actually incurred and those previously calculated. In the light of the above, the public body must also carry out a subsequent cost calculation in order to

determine the exact amount of the costs actually incurred. The requester must be informed of the result, the supporting calculations, certificates, working time statements, and other documents. No provision of the Privacy Act or the Decree allows the charging of additional costs incurred above the costs calculated previously. In other words, the data requester may not be subsequently charged with the difference due to an underestimation of costs. However, pursuant to the Decree, if the pre-paid reimbursement exceeds the sum of costs actually incurred, the difference is to be refunded to the data requester. It is important to substantiate the costs incurred in connection with the data request by means of documents also because, in a possible dispute, the data controller is responsible for demonstrating the exact cost elements.

The NAIH is confident that the time passed since the entry into force of the Decree has proved sufficient for law enforcement bodies to acquire sufficient experience in fulfilling requests for data of public interest, and to establish a well-defined procedural framework for fully complying with the rules of the Privacy Act and the Decree.

VII.3. The NAIH's Activities Related to the Prevention of Corruption

The NAIH represented itself at several home and international professional or scientific conferences, lectures, and workshops. At these, it highlighted the importance of the freedom of information and transparency in the prevention, suppression, prosecution of corruption. In addition, the NAIH called the attention of the professional and lay public to the outstanding role and context of the issue.

In close cooperation with a member of National Protective Service, the NAIH organized a conference for the local governments of towns with a population over 15,000 on 26 February on the freedom of information. The lectures delivered here focussed on access to data of public interest and data public on grounds of public interest, as well as the practical issues of electronic disclosure. The two organizations continue to shape the programme and topics of discussion of future conferences on the basis experiences gained during prior cooperation.

VII.3.1. Participation at International Forums on the Promotion of the Freedom of Information

During 2017, the NAIH represented itself at two international forums aiming to approximate and coordinate national and international institutions specialized in overseeing the freedom of information.

The NAIH, attended the conference of European Commissioners for Freedom of Information held in Berlin between 23 and 24 February 2017. The participants at the event organized by the German Federal Data Protection and Information Commissioner presented their national experiences of the fundamental right to freedom of information, and gained insights into the relevant practices of other states. In addition to the exchange of experiences, specific issues were also discussed. At the close of the conference, the European Data Protection Supervisors adopted a resolution calling on national parliaments and governments to strengthen the role of the freedom of information and of the national institutions supervising it.[53] Freedom of information and transparency are an essential element of a freely and democratically functioning legal system.

NAIH also actively participated at the 10th International Conference on Freedom of Information Commissioners in Manchester between the 20 and 21 September 2017. More than a hundred participants from different parts of the world were able to discuss national and international experiences of the freedom of information. In the resolution of the conference, the participants emphasized and considered the strengthening of the transparency of performance of public and local government services provided by outsourced contractors and public procurement in the future.[54]

The participants at these forums repeatedly expressed the need to deepen cooperation at European and international level, with the aim, first and foremost, of establishing common standards. The NAIH therefore expresses the hope that such future events will expand the opportunities of cooperation. These may ultimately lead to the creation of regional or global standards, as in the regulation of data protection, in the field of the freedom of information.

[53] http://naih.hu/files/EU_Infoszab_bizt_nyil_2017-02-24.pdf.
[54] http://naih.hu/files/2017-09-28-Infoszab_biztosok_hatarozata.pdf.

VIII. The NAIH Activities Related to Legislation

VIII.1. Statistics on Legislation-related Activities

In 2017, the number of draft legal proposals to be commented on by the Authority did not change significantly compared to the previous year. However, the number of substantive objections and suggestions we made increased by a good fifth. The difference is even more marked if we examine the statistics of the proposals in terms of substance: the number of comments on data protection doubled compared to 2016, while those on freedom of information dropped to roughly a quarter. This does not mean that the Authority paid less attention to the enforcement of the freedom of information, but rather the reason for the change is that 2017 saw the preparation for the renewal of the data protection framework, and that the number of draft proposals touching on the freedom of information also decreased. Therefore, with regard to 2017, data protection is in the focus of our report.

The Number of Legislation-related Cases by Year and Legal Source			
Legal Source/Year	**2015**	**2016**	**2017**
Law	79	85	82
Government decree	133	98	89
Ministerial decree	126	83	94
Government regulation	61	29	33
Public-law regulatory instruments	27	20	23
Total	**426**	**315**	**321**

The Number of Substantive Comments on Draft Legal Proposals			
Comment subject matter	**Number of comments/year**		
	2015	**2016**	**2017**
Data protection	298	222	461
Freedom of information	53	101	28
Other	137	127	92
Total	**488**	**450**	**581**

VIII.2. Changes in the Regulatory Framework for Data Protection Legislation

Before addressing the main NAIH cases relating legislation on the processing of personal data and freedom of information, it must be mentioned that the legal framework for the protection of personal data will change with the coming into effect of the GDPR (General Data Protection Regulation) in 2018. The activities of the Authority related to the preparations for the GDPR were discussed in last year's report, so it is not necessary to repeat it or to describe its standards. It is enough to point out here that the protection of personal data is a fundamental right as defined in the Fundamental Law (formerly the Constitution), the content and principles of which were and are interpreted by the decisions of the Constitutional Court, and its basic rules are laid down by the Privacy Act. The data protection rules for data processing subject to the GDPR data shall be covered not by law but the GDPR. The scope of the GDPR does include all personal data processing, an obligation to regulate the basic rules of data protection not falling within the scope of the GDPR therefore continues to arise from the Fundamental Law, i.e. the Privacy Act need not be repealed, it is only necessary to change its scope in order to delimit it from the GDPR. It should also be noted that the legal framework is becoming more complex with further EU legal standards currently under preparation or already adopted, which set forth specific requirements of data protection for given regulatory fields (e.g. law enforcement, on-line space). From 2018, a legal framework is coming into existence that is going to make strong adaptation claims on Hungarian legislation, the Authority as regulator, and the data controllers themselves. As far as our report is concerned, we do not think that the GDPR will contradict

the content of the protection of personal data laid down by the decisions of the Constitutional Court and thus lead to any a constitutional conflict, because the GDPR aims at creating a high level of data protection, and it is therefore expected to make overall progress, the level of protection of personal data attained is thus going to be sustainable at least. Moreover, the GDPR is sufficiently flexible to leave room for the legislators of the Member States even with regard to the data processing under its scope, and to allow for smaller differences in the constitutional perception and traditions of the various Member States to be enforced within the framework of the GDPR.

Accordingly, the Authority's continuing role in 2017 was (and is in 2018) to support the maintenance of the legal environment facilitating the protection of personal data by delivering comments and suggestions on the amendment of the Privacy Act required by the GDPR and the adaptation of sectoral data control law to the GDPR. This task was also given in the case legislation on data processing not subject to the GDPR, due partly to the amendment of the Privacy Act may give rise to purely technical adjustment needs at sectoral level and partly to the EU data protection legal standards already mentioned.

VIII.3. The Amendment of the Privacy Act

Adopted in 2011, the Privacy Act, in our opinion, is an advanced data protection law that has met the requirements of European legal development to a great extent so that the transition to the rules of the GDPR is not going to increase severity. In the fields of data protection regulation remaining under national legislative competences, it is advisable to develop a data protection regulatory environment by the amendment of the Privacy Act that approximates the GDPR in terms of its conceptual framework, principles, and legal institutions, since it is beneficial to both data subjects and data controllers if the general rules of data protection provide for a more unified and transparent system of legal requirements. Compliance with the new data protection rules is not only a priority for the NAIH, but data controllers and data processors also need to start reviewing their data processing practices in a time.

Under the agreement between the Ministry of Justice and the NAIH, the NAIH had the opportunity to take part in the preparatory work for the Amendment of the Privacy Act from the outset, January 2017. By way of official meetings and delivery of comments, there has been a regular direct working relationship between the two bodies at administrator level to develop the concrete content of the rules and to clarify the issues.

In identifying legislative tasks, the NAIH took the view that there is no likelihood of a need arising to modify the parts concerning the freedom of information, since the relevant EU acts only govern the processing of personal data and the flow of personal data. In order to comply with the EU obligation, it seemed therefore sufficient and appropriate to amend only the provisions concerning the same subject in the Privacy Act.

The independent status of the NAIH is based on the Fundamental Law, and it can be stated on the basis of the examination of the Hungarian laws on its powers, management, and organization that they are in accordance with the EU legislation prescribing the independence of the supervisory authorities of the Member States and its specific conditions, so we argued that the current provisions of the Privacy Act are also suitable for the enforcement of EU rules.

In terms of substantive rules, we represented the expectation that there should be no stepping down from the high level of protection already provided by the Privacy Act.

In shaping the new procedural rules for the Privacy Act, we kept in mind that the NAIH should be able to exercise its obligations under EU law, and to exercise its new powers in accordance with constitutional requirements, and that the new procedural order can be integrated seamlessly into (the now more direct) international cooperation between the supervisory authorities of the Member States. Another factor to be taken into account is that Act CL of 2016 on General Public Administration Procedures, effective as of 1 January 2018, applies to several procedures falling within the competence of the NAIH. Thus, concord has to be achieved with these rules likewise.

Drafted in close cooperation between the Ministry of Justice and the NAIH, the bill underwent social and administrative consultation until September 2017; all competent organizations had delivered their comments on the draft. At the time of writing this report, the bill was not put on the agenda of Parliament.

The review of sectoral laws in accordance with the GDPR and the amendment of the Privacy Act was begun in 2018, and this will therefore be discussed next year's report.

VIII.4. The Reform of Gathering of Intelligence Subject to Outside Authorization

The Act CXXV of 1995 on National Security Services (hereinafter ‘the Security Act’) is to be amended due to the judgment of the European Court of Human Rights in Strasbourg (ECHR) in 2016 (hereinafter 'the Judgment'). Last year's report discussed the suggestions of the Authority on the Judgment and its action to amend the law.

The preparation of the amendment of the Security Act went over into 2017, so what follows is an account of developments in 2017.

The Chairman of the National Security Committee of Parliament invited the NAIH President to comment on the outside authorization reform. This request was an opportunity to outline the data protection aspects of the outside authorization system.

The reasoning of Decision 2/2007 (I.24.) AB of the Constitutional Court analyzing the case law of the ECHR found that, in the case of gathering of intelligence, 'the application must be subject to a three-stage check: when the intervention is ordered, while the intervention is being carried out, and after the completion of the intervention'. The decision primarily interpreted the Constitution in relation to gathering intelligence for law enforcement purposes, but its general findings are, in our opinion, also valid for gathering intelligence for national security purposes. In accordance with the Judgment, the re-regulation of the ordering the application was primarily the focus of the attention, however, under the Hungarian constitutional requirements, the guarantee system of gathering intelligence must be equally solid in its entirety, i.e. at the time of ordering, during application and the follow-up check.

In the case of using special means and methods for the deepest exploration of privacy, the prior authorization of gathering intelligence is a key element of the control system. However, given that only a short period of time is available for decision making in the authorization procedure—which is necessarily closed from public control, is basically based on the data and allegations made by the applicant authority, and omits the institutional representation of the data subject—full compliance with the conditions of 'law enforcement quality assurance' that would otherwise apply as a main rule in any civil or criminal court proceedings is unattainable. In the case of the procedure of outside authorization of special means and methods, the decision of both the judge and the minister lacks the following: adversarial procedure, unrestricted evidence, public hearing, flexibility of time frame depending on the complexity of the case, and remedy. In the opinion of the Authority, therefore, so as the application of the special means and methods is subject to control in accordance with the Judgment and the intentions of the Constitutional Court, the regulation of the simultaneous and subsequent control of gathering intelligence should also considered alongside the procedural law reform of prior authorization in the process of drafting legislation in.

VIII.4.1. The Simultaneous Control of Gathering Intelligence

Special means are deployed in a fixed time frame, typically under special circumstances (strict conspiracy, covert performance, etc.), which usually do not allow simultaneous, outside control of the intervention. Therefore, the organization that carries out tasks related to deploying special means is the key player in ensuring the lawfulness of gathering intelligence. During the data protection audit of the service provision activity National Security Special Service (NSSS) related to deploying special means, it was found in the division of labour and duty fulfilment order under the Security Act, it is a duty of the NSSS deriving from law to ensure the professionalism and lawfulness of deploying the special means. The Authority supports the strengthening of this role controlling lawfulness by the NSSS.

VIII.4.2. The Subsequent Control of Gathering Intelligence

The most important independent, general control body of the national security services is the Committee on National Security of Parliament, which is given the appropriate examination competence by the law to control the proper functioning of national security services. Gathering intelligence by the national security services is primarily to be controlled from the point of view of the protection of personal data. Under Article VI (3) of Fundamental Law, the application of the right to the protection of personal data shall be supervised by the National Data Protection and Information Authority in accordance with the provisions of the Privacy Act. The Authority shall also be entitled to the (subsequent) control of gathering intelligence. The information gathering activities of the national security services constitute particularly sensitive data processing in terms of data protection, and therefore deserves the special attention of our Authority, but there are only limited means at our disposal for the subsequent control of the lawfulness of gathering intelligence.

Currently constraints are as follows:

- Naturally, to the Authority receives little information about the potentially unlawful gathering of intelligence;

- In the framework of the Privacy Act, we can only initiate a proceedings to control the lawfulness of gathering intelligence under conditions (such as submissions from target persons, information on the content of gathering intelligence) that seldom occur in the case of gathering intelligence.

For several problems mentioned above, a draft amendment to the Security and the Privacy Act prepared by the Ministry of Interior Affairs could lead to a solution, as it provides the Authority, in the case of gathering intelligence authorized by the minister, with competence for prior control the protection of personal data and, in the event of

perceiving breach of law, effective means of intervention for the protection of the privacy of the data subjects. The administrative consultation on the draft amendment took place in 2017. In its course, the proposer took into account the Authority's observations and suggestions. The bill has not been submitted to Parliament yet.

VIII.4.3. The Regulation of Gathering Intelligence for National Security in the Light of the Data Protection Audit of the National Security Special Service (NSSS)

The data protection audit of the NSSS service provision related to the deployment of special means was completed in 2017. During the audit, the Authority examined primarily the compliance of the service activity with legal requirements, but we also gained experience on how far the legal provisions on the deployment of special means accord with the constitutional requirements set out in the Fundamental Law, the Privacy Act, and the decisions of the Constitutional Court. We found the examination of the latter issue important because, as stated in the reasons of the 2007 decision of Constitutional Court mentioned above, the use of secret means requires strict guarantees covering all the details of interference in fundamental rights. The precise and detailed regulation of gathering intelligence guarantees the protection of the rights of the data subjects and assessing whether the guarantees meet the requirements arising from the principles of legal certainty and security, predictability and foreseeability, and whether they meet the requirements of necessity and proportionality, and whether stricter standards are enforced than in open procedures. From the point of view of the protection of personal data and the enforcement of state interests that require the gathering of intelligence, the lawfulness and professionalism of the activities of the NSSS, it is essential to identify possible errors or shortcomings of the legal regulations concerned. The data protection audit focused on the following aspects and relations of the legal regulation.

VIII.4.3.1 The System of Regulating the Means and Methods of Gathering Intelligence in the Security Act—the Relationship and Delimitation of Each of the Special Means and Methods

This is important because the Security Act lists the means and methods of gathering intelligence, but does not detail their nature, so it may be questionable in cases whether each of them can be defined and delimited from one another in the system of legal regulation, or uncertainties and inconsistencies may be experienced in the application of the law in this respect. In connection with this, several tests were carried out, for example, when we examined whether the grounds of outside authorization could be properly distinguished in the investigation of postal mail containing computing devices (see Section 56 (c) and (e) of the Security Act).

Regulations of law must delimit with equal precision the specific means and methods that are and are not subject to outside authorization (as otherwise obligation to obtain outside authorization could be avoided). According to the audit experience, the legal regulation and the enforcement practice are in line with this aspect.

VIII.4.3.2 The Legal Definition of Each of the Special Means and Methods

The Security Act it does not define the content of the special means and methods beyond naming them; we therefore examined whether the legal regulation, as it is, is sufficient to meet data protection requirements. In connection with this, we tested, for example, whether the covert control of electronic communications devices clearly distinguishes the content of communications transmitted via the electronic communications service from the meta-information attached to the communication. This is important because the control of the content of communication is subject to outside authorization under Section 56 (d) of Security Act, but not to metadata. According to the relevant audit test concept, the question to be examined in deployment of special means was which category do signals transferred before call setup and ringing fit in. (In addition, further audit tests that cannot be covered in this report were also relevant to the issues of legal certainty of certain special means and methods and to the possible deficiencies in the legal definition.)

The tests demonstrated that the effective Security Act does not define the details of several special means and methods relevant to data protection, but the detailed, internal rules for deploying special means laid down by the NSSS and its interpretation of law are in line with the requirements of data protection; in other words, the good practice in terms of data protection makes up for the want of detail in the law.

VIII.4.3.3 Procedural Rules of Gathering Intelligence

This is an important issue in terms of data protection, because it is a constitutional requirement that the procedural order of deploying special means must guarantee the rights of the individual. Applicable rules must be precise, detailed, and transparent, and must also be clear about the scope of the organ deploying the means, the essence and the methods of the measures exercised. According to the audit tests, the regulation meets the requirements less minor flaws. For instance, under Section 57 (2) c) of the Security Act, the application for outside authorization of gathering intelligence shall include the beginning and end of the activity in days, but Section 58 (4) thereof fails to clarify how precisely the authorizing party is to define the commencement time and the termination of the permit, and the law does not include exact deadline calculation method establishing that the outside authorization shall define the duration in days, meaning the day of commencement at 00:00 hours and the day of termination at 23:59 hours.

VIII.4.4. The Regulation of Gathering Intelligence for Law Enforcement Purposes

The problem of outside authorization for gathering intelligence arose also in the context of regulating criminal proceedings in 2017. The draft bill to amend the rules of gathering intelligence in connection to the new law on criminal proceedings envisaged the enactment of a number of new rules that are in line with the constitutional requirements laid down by Decision 2/2007 (I.24) AB of the Constitutional Court, and are therefore to be supported from the perspective of data protection. The Authority considered, for example, as an important step forward the amendment—making good a legislative debt of many years—whereby a target person shall be provided subsequent information on the fact that intelligence was gathered on him provided that this does not prejudice the interest of gathering intelligence or the effectiveness of ongoing criminal proceedings. We also agreed that the draft detailed the control of deploying means. According to the draft bill, the power of control will be granted to the courts. In this respect, the Authority pointed out that independent courts may obviously be able to supervise the lawfulness of deploying special means, but the intended rules were in many respects defective. The draft only referred to the possibility that the courts may review the lawfulness of deploying special means subject to judicial authorization during deployment. It was not clear who—under what conditions and on what criteria—is to decide on starting the review of the lawfulness of deploying special means is mandatory. The draft also did not answer the question as to how the courts should find out which gathering of intelligence was suspect to be in breach of law and was thus to be reviewed. In this regard, we considered it appropriate to point out that, due to the confidentiality of gathering intelligence, information about the deployment of special means cannot be returned to the courts, so it may be assumed that the courts will not receive information justifying the necessity of reviewing the legality of a given deployment of special means. On these grounds, we deemed it questionable whether the overloaded courts will be able to exercise the power of review when the regulation enters into force.

VIII.4.5. The Criminal-law Sanctioning of Illicit Data Collection

A regrettable event in 2017 highlighted the wants in the criminal law regulation of illicit data collection. According to press reports, a hidden camera had been found in one of the offices of the headquarters of the public Hungarian Television (MTVA), but there was no way to find and prosecute the perpetrator, because, under the effective Criminal Code, the office did not qualify as a private home, so it could not be the scene of illicit data collection. Unlawful covert surveillance and data collection can result in extremely serious violation of basic information rights, because it can uncover the most inner areas of the private sphere of the individual that are to be protected most, but because of the covertness of this activity, the data subject has no opportunity to protect his or her rights. In order to protect the right to informational self-determination and to the respect of privacy, the law sanctions all similar violations by the means of criminal law.

For the purposes of rules of procedure and criminal-law cases related to similar, covert data gathering, ‘residence’ and ‘private home’ is to be construed so as to mean all other places or areas, including non-public transport vehicles, that are beyond ‘residence’ or ‘private home’ in the everyday sense and not open to the general public. In the view of the Authority, there is no reasonable justification for deviating from this in a criminal-law case of illicit data collection, and referring to the notion of home used in the criminal-law case ‘home violation’ as governing, because it may result in impunity for such serious violations as the MTVA surveillance case. Therefore, the NAIH agreed that the Prosecution Service initiated the amendment of the fact of illicit collection of data in the Criminal Code, furthermore it also initiated this in a letter to the Deputy Secretary of State for Public Law Legislation of the Ministry of Justice.

VIII.5. Major Public IT Development Projects Affecting Big Public Data Processing Systems

When examining submissions on the protection of personal data, it is usually the question of whether a particular data controller processed the personal data of the submitter lawfully, or whether data subject was able to enforce his or her data rights under the Privacy Act. In these cases, the data-protection law issue appears in the context of the enforcement of rights.

In addition, there is an aspect of data protection law that is less related to a particular person, namely when the question arises in the course of an investigation by the Authority whether the records or other data processing activity of a particular data controller as a whole is in compliance with data protection requirements in their entirety. It is in this respect that it is necessary to examine, for example, whether the internal data processing instructions of the data controller are adequate, or whether the IT system for processing personal data is appropriately protected against cyber attacks.

Finally, it is also possible to define a section of data protection law that determines legal requirements in the sphere of the hierarchy of data beyond concrete data-processing activities and data controllers (for example, the principle of divided information systems, the requirement of data portability, and any other data protection rules that apply to the connections between information systems, i.e. to data processing systems as a whole). This area of data protection is becoming increasingly important, as technological developments in the age of the Internet enables the interconnection of data processing systems, which is becoming more and more inevitable in an advanced information society. However, this area of data-protection law, including its normative content and principles, is less clarified at the level of theory than the rights of the data subject. It is worth reflecting on the fact

that international conventions with broad consistency laid down the conditions under which the right to information of the data subject could be restricted in a democratic society decades ago, yet there is still no unified European response to the question whether a state may oblige its citizens to use a single and universal identification mark.

Currently, it seems to us that the data protection of the data processing systems is more difficult to describe as a formal list of specific data-protection requirements, such as the relationship between the *data subject and controller* or between the *data controller and processor*. In our opinion, the main reason for this is that, in the data processing systems, any aspect of possible data connections may have complex technical and IT content, and, in principle, any minor detail of this may be relevant from a data protection point of view. Yet, of course, not only minor details but also major relationships may be significant in this sphere. For example, the question arises whether any legal requirement can be deduced from the constitutional principles of state organization, for example the separation of powers, on who (what body) is to exercise control over an information system of a given branch of power or public organization, and where should these systems be placed within the state organization? If such informatics requirements of state organization can be deduced, then it would be necessary to clarify how these relate to data protection requirements of the system of data processing. Raising the problem like this might seem to be abstract, but the Authority often faces similar issues when examining draft legislation or the large interconnected systems of data processing. This is thus a very complex subject matter, but it would be a major mistake if the Authority, which the Fundamental Law confers the power of data protection control on, harked back from difficulties of delivering theoretically sound legal responses to the complicated problems of the data protection occurring in data processing systems. Therefore, our aim is to make progress in shaping the data protection requirements of the big data processing systems based on earlier guidelines delivered by the Constitutional Court.

In Hungary, in the sphere of the big data processing systems, an important milestone was the act on electronic administration and the interoperability of public data processing systems, the essential rules of which enter into force as of 2018, but this area is not unknown to the Authority, as it had delivered its opinion on both the act and its implementing regulations, its staff had been invited to participate in government discussions on data processing and protection issues of electronic administration. Electronic administration is deemed to include the National Unified Card System, the applicable rules of Act XX of 1996 on the methods of identification and using of identification codes which replace the personal identification mark, as well as the ASP system of the local governments. In 2017, we delivered our opinion on several related draft bills, of which the proposal for the creation of a Government Data Repository should be highlighted.

VIII.5.1. Government Data Repository

According to the draft Government Decree on a Government Data Repository, the organs obliged to carry out electronic administration are required to systematically backup data from their IT systems, which they shall hereafter have to transfer to the Government Data Repository. The Government Repository is to provide storage for saved data files, that is, the retention and restoration of the data necessary for the proper operation of the data-source organs should a natural disaster, a terrorist attack or any other reason damage or destroy the data of the organs concerned. The Authority believes that the creation of a Government Data Repository is a reasonable, legitimate purpose, but it involves serious data-protection risks if all the data-file backups of the entire public administration, the health care system, the courts, and public service companies go into the possession of a single organ. The question arises whether it is compatible with the constitutional principle of the separation of information systems that, beyond all the data assets of the public sector and public service providers, even those of the courts are concentrated in the Government Data Repository; whether it is in line with the principle of separation of powers under democratic rule of law if all the data possessed by public administration, including the data processed in the operation of the court system, will be transferred to the same body. Moreover, any data loss or unauthorized access to data may be a risk to data protection.

Risks may be eliminated by establishing an order for the centralized retention of archived data that enables access to data only by the body that placed them in the Central Repository. The Authority also recommended that all data processing organizations be provided with their own custom keys. A key should not be used more than once and should not be disclosed to a third body or person. In addition, key management (secure storage) tasks of data processing organizations, including procedures for key compromise, should be defined. It is also necessary to clarify the data processing status of the Repository.

VIII.5.2. Integrating Public Surveillance Systems Into a Single IT System

For administrative consultation, the Ministry of Interior Affairs tabled a proposal which would involve the amendment of several laws and is intended to ensure that voice and video recordings made by the police, public safety departments, passenger transport services, public road services, toll collectors, and financial service providers, would in the future be transferred to a central public service body subordinated to the Ministry of Interior Affairs. According to the bill, data control organizations would provide IT access to the organizations authorized by the act, which would thus enable the ‘omission of one-by-one requests’. According to the submission, it is a question of changing the location of storing the recordings and unifying the duration of data retention. In the opinion of the Authority, the central storage of image sequences would multiply the possibilities of

observing, data collecting and linking, and would therefore create a new situation from a data-protection point of view. Furthermore, organizations operating surveillance cameras would have much less chance of checking the lawfulness of using image recordings, as the recorded files would no longer be in their possession. The organization into a single data storage system would, by facilitating easy access to data, result in a video surveillance system that operates continuously, collects data on a stockpiling basis, can be used for collecting secret information, and covers a large geographic area (areas of Budapest and the country's most important public roads with surveillance cameras).

The planned central system may only be established if the regulation contains adequate safeguards against the unlawful use of the data. Particularly important is the documentation of data access and the creation of a control system that has a proper deterrent against unlawful surveillance involving disproportionate limitation and infringements of rights. Furthermore, the possibility of the centralized, hidden, data-recording surveillance of public places (such as environments of churches) or events (such as political demonstrations) is in no way desirable.

VIII.5.3. Regulation of Data Processing by Drones

Regarding the regulation of pilotless aircraft by way of implementing rules, the Authority, reporting its opinion, agreed on the necessity of drafting the regulation and proposed supplementing the regulation of data processing by drones, as pilotless aircraft are primarily used for surveillance and aerial photography. The Authority's proposals were as follows:

- suitable distinction of the minimum distance drones are to keep from those persons and their homes who have not consented to their observation by drones;

- the use of light drones should also be regulated when they are equipped with cameras capable of taking high resolution pictures and can be flown far from the remote operator;

- the legal framework of data processing by drones in the public sector should also be outlined;

- consideration should be given to the press obtaining easier terms for the use of drones with regard to state leaders and events;

- drone flights are permitted from dawn to sunset, and drones should be made clearly visible by being painted or otherwise;

- drone pilots while flying drones must wear a clearly visible pictogram on their clothes to indicate that they control the drones;

- pilots' training syllabus and state-required pilot examination requirements should be supplemented with knowledge of data processing and protection law.

IX. Control of Classified Data—Classified-data Cases

So-called classified-data cases make up a heterogeneous part of the Authority's duty portfolio. The cases belonging here may be related to both the protection of personal data and access to public data. Neither can they be considered as uniform from the point of view of procedural law, because, from among the proceedings under the Privacy Act, not only may administrative proceedings for the control of classified data touch classified data but also investigation proceedings, administrative proceedings for data protection, and data protection audits; moreover delivering opinion on draft legislation may concern basic information rights related to classified information. The Authority may, in the case of national security data, examine whether its classification is lawful, or whether its classification violates the right to the protection of personal data or to the access and disclosure of data of public interest. In the case of foreign classified data, the review of its classification falls outside the competence of the Authority.

In spite of their diversity outlined above, classified-data cases have common features whereby it is reasonable to treat them as a separate case group. First of all because the protection of state interest—designated by the Act CLV of 2009 on the Protection of Classified Information (hereinafter 'the Classification Act') as state interest and representing public interest—requires particular principles, legal institutions and strictly kept prescriptions in order to protect classified information, which significantly differ from rules applicable to classified information protected by other laws (e.g. banking secrets, business secrets, etc.). What follows is an incomplete list of these characteristics:

• Classification is a procedure regulated in detail by Classification Act, in which full compliance with formal and procedural requirements have a significant role; otherwise the data does not become classified.

• The principle of 'necessary knowledge' limits access to classified information to certain persons.

• While classification is valid, i.e. until the termination of the classification or the deletion of the classified data, the classifier (in the case of succession the successor of the classifier) is entitled to the most extensive right of disposal with respect to the classified information whether or not he or she possesses or transferred the data.

There is another pragmatic reason for dealing with classified-data cases as a separate group, namely that we have to comply with personal, administrative, and technical security requirements for classified information that do not apply to other cases. The data and documents classified as 'confidential' and above may only be used in the security area meeting the security requirements defined by the implementing regulation of the Classification Act. Documents containing classified information must be administratively completely separated from the processing of the other documents. The so-called TEMPEST information system for the production and use of classified information must be protected against compromising electromagnetic radiation. Classified data can only be processed by employees whose national security clearance identified no risk factor. In order to ensure a high level of compliance with the security requirements, the Authority expanded its security area in 2017, took steps to acquire NATO TEMPEST Level A IT equipment, and initiated its connection to the Government Encrypted Backbone Network. Hereafter, we highlight the following classified-data cases among those of 2017.

IX.1. The Classification of the Data of the Spy Trial

On the basis of a submission by a journalist, the Authority examined the classification of the data of the so-called Spy Trial. The press had widely reported on the fact that the Budapest Court of Appeal, in its final decision, found former leaders of the national security agency, former minister of the secret services, and a private person not guilty of the charges of espionage and complicity. The case had aroused public interest, but little could be known on the subject of the lawsuit, because the court dealt with classified information. However, newspapers leaked information from unknown sources with doubtful reliability on the actual or assumed details of the trial. In the opinion of the Authority, the acquittal called into doubt the necessity of classification of at least some of the data, and agreed with the submitter that some of the accused were charged with actions related to their exercising public office, and thus the public has an emphatic constitutional interest in being acquainted with the events. The Authority found that the National Protective Service (hereinafter 'the NPS') had investigated the case before the open criminal proceedings, and was the one where the classification had been carried out. Thereon, the Authority requested detailed justification of the classification by the classifier, and also examined the documents classified on site. As a result, the Authority found that the several volumes of documents on the complicated intelligence activity included many data whose classification remained a state interest, these included the following:

- The disclosure of certain data would enable the identification of the source of intelligence. In this case, the person providing the intelligence would have had to face adverse consequences. If Hungarian law enforcement authorities had not been able to keep the identity of their intelligence sources secret, that would harmed law enforcement interests, because no one would cooperate with law enforcement agencies if he could not be sure that his identity would remain a secret.
- Some details of the case were not to be disclosed because it could have adversely affected the external relations of Hungary.

– Had data been disclosed, it would have been possible to reconstruct the specific procedural rules, methodology, and the limits of the criminal intelligence gathering activity. If this came to the attention of potential target persons, it would jeopardize the success of subsequent intelligence gathering, that is violate law enforcement interests.

According to the Authority, however, it was in the public interest to disclose the essence of the happenings which had been the object of intelligence gathering and the subsequent criminal proceedings, and this was more powerful than the factors requiring the limitation of publicity. In addition to the circumstances mentioned (the acquittal and that the accused had formerly held public office), the following factors supported publicity:

– Some of the facts of the case had been leaked earlier and publicized through the press. Maintaining the classification of data already known to the public is obviously superfluous.
– During the proceedings, what arose was the foreign influencing of the Hungarian National Security Service. This is a matter of a kind and weight a democratic public must be informed of.

In order to resolve the contradiction, the Authority selected from the documentation a summary report on the intelligence gathering activity, which sufficiently detailed the facts of the case the NPS had gathered intelligence on, but did not contain classified information, therefore maintaining its classification was no longer justified, and the Authority, in its decision made in administrative proceedings for the control of classified data, called on the classifier to terminate the classification of the data in the report mentioned. The classifier did not appeal to the court within the statutory deadline, and therefore the classification of the data was terminated.

In the course of the administrative proceedings for the control of the said classified data, it came to our notice that there are classified data in the documents of the case tried by the Budapest Court of Appeal that had been classified not by the National Security Service. We will review the lawfulness of classifying these data in another administrative proceedings for the control of classified data.

IX.2. Data Collected on the NGOs Supported by György Soros

Public opinion and political opinion makers are strongly polarized in judging the activity of expatriate György Soros. Some say that the organizations he supports seek covert control and to influence public decision-making, while others believe that these assumptions are unfounded. In these circumstances, it is no wonder that several proceedings were initiated at the Authority on the data related György Soros and the NGOs he supports.

In March 2017, Szilárd Németh, vice-president of the National Security Committee of Parliament, stated to a news blog that he had turned to the secret services, 'having gathered the names of organizations cooperating with the Soros network, to request the full screening of their activities'. As Act CXXV of 1995 on National Security Services (hereinafter 'the Security Act') does not authorize the Vice-President of the National Security Committee of Parliament to define any specific task or intelligence requirement for the National Security Services, the Authority *ex officio* requested information from Mr Szilárd Németh whether what appeared on the blog actually occurred or no. In response, the Vice-President of the National Security Committee clarified the statements made on the blog that, knowing and complying with the relevant legal provisions, he had never issued direct instructions for action to the national security services.

In the course of administrative proceedings for the control of classified data, the Authority reviewed whether the data concerning Soros György and the organizations he supports, which were discussed by the National Security Committee of the Parliament, were lawfully classified a 'Strictly Confidential!' or not. During the proceedings, the Authority examined the minutes of the closed session, and clarified that the data were classified by the Information Office (hereinafter 'the IO'), as the National Security Committee used data from the IO.

Having recognized the facts of the case, the Authority held that there was a strong public interest in the publicity of the discussion at the closed session in order that the public may realistically weigh whether the activities of György Soros and the civil organizations he supported were harmful for national security or not. However, there were two very important reasons for maintaining the classification of the data:

1) The National Security Committee discussed intelligence gathered by the IO, that is, the National Security Service performing foreign intelligence tasks, at the closed meeting. In agreement with the detailed justification by the Director-General of the IO, the Authority found that, in the event of disclosure of the data discussed at a closed session, it could be inferred what intelligence sources the IO had among top state, political, and economic decision-makers in other countries. This would have paralyzed Hungarian intelligence activities, and foreign law enforcement agencies would have been able to identify Hungarian intelligence sources, and thus the foreigners concerned would have had to face serious criminal reprisals in their country.

2) During the closed session, opinions and statements were made about the leadership and politics of other states that lacked the criteria of diplomatic courtesy, and thus their disclosure would have caused inconvenience in Hungary's diplomatic and foreign relations.

On the basis of the above, the Authority found that, although it would have been desirable to terminate the classification of the data subjected to the administrative proceedings, national security and foreign policy the

interests were weightier and in favour of maintaining the classification, and thus it ended the administrative proceedings.

IX.3. The Problem of Subsequent Classification

The review of a classified-data case revealed that the classifier had classified data several years after its generation, and the question arose whether this classification practice was lawful or not. The Authority found the following:

1) If the statutory conditions of classifying data are met, classification must not be procrastinated. A delay in the classification procedure would be detrimental to the freedom of information, because, ultimately, it would prolong the period of time between data generation and the disclosure of the data of public interest (until the termination of classification). If the classifier delays the classification procedure, and goes on to determine a validity period that is within the maximum period from the date of classification, but far exceeds the period beginning with the generation of the data for the given classification level under the Classification Act, it is to be considered a circumvention of the legal prescription to limit the validity of classification, which violates the enforcement of the right of access to data of public interest by extending the period of withdrawal of data from the public. (In our experience in applying law in other cases, it has also happened that a classifier waited with classification until receiving a request to access data of public interest. In such cases, the abuse of classification power could clearly be established.)

2.) Stricter personal, physical, administrative, and electronic security standards apply in processing classified data than in general document processing. Access to media containing classified data and use (transferring, reproduction, etc.) thereof are subject to conditions and precise documentation. Compliance with the classified-data regime can only be guaranteed if the data is classified without delay after its generation (recording, entry, etc.). (According to Article 6 (6) of the Classification Act, during classification procedure, until the classification decision is made, data shall be processed according to the personal, physical, administrative, and electronic security regulations applicable to the initiated classification level.)

If classification is delayed, the question arises who could actually access the data between its generation and the start of the classification procedure. If classified information is accessed by someone without authorization, it can scarcely be proved that the data was accessed before or after classification. No legal uncertainty can be accepted in establishing a possible confidentiality breach, because the abuse of classified data is a category in criminal law.

IX.4. Publicity of the Data on the Paks Nuclear Power Plant Construction

A number of submissions were and are being received by the Authority regarding the publicity of the data on the construction of the Paks II Nuclear Plant. The submissions relate to a wide range of data, including, for example, implementation agreements, consultancy contracts, and the accessibility of documents relating to the preparation of the construction. In connection with these submissions, the Authority several parallel proceedings—investigations or proceedings for the control of classified data—of which the following were concluded in 2017:

1) Regarding the implementation agreements, several discussions were held with the representative of the classifier to clarify which data should be protected by classification, and which classification should be terminated. During the proceedings, the classifier first reduced the classification to the lowest level, 'Restricted', and then terminated the classification of most of the documents. Maintaining the classification of the remaining data, mostly technical and security information, was justified, and therefore the Authority terminated the proceedings in this case.

2) In the context of several hundreds of contracts containing partly classified data, partly business secrets, the Authority provided, during consultations and on-site investigations, methodological assistance to the data processor to review the contracts in accordance with the right of access to data of public interest and render them accessible to data requesters. To do this, the following had to be clarified for each contract:

- identification of data content of public interest;
- definition of business secrecy; identification of legal requirements for specific data groups, such as environmental data or plant security data; the issue of data to be protected in the interests of national security. In addition, the Authority highlighted to the following:

- Classification must always apply to specific data, not to full documents. The parts of contracts with classified data that need not be protected by classification must be made accessible; It is also not necessary to maintain classification where parts include classified information. If the interest in the protection of classified data ceases, classification must be reviewed and terminated; In the case of document parts to be blacked out, only the information to be really protected must be blacked out, not the entire paragraph or sentence, on the anonymized copy. Following the technical consultations, first about 170, then about 90 documents were made accessible. Thus, a part of the documents became fully accessible; some documents, however, contained data related to decision-making, as well as technical and

security issues which were to be protected, and so data requesters were provided these documents in extracted form. The data controller rendered the data under investigation accessible, and the Authority accordingly closed the proceedings in this case.

IX.5. The Data Connection between the Counter-terrorism Information and Criminal Analysis Centre and the Prosecution Service

It was in connection with a consultation question that the Authority interpreted the entitlement of the Counter-terrorism Information and Criminal Analysis Centre (hereinafter 'the TIBEK') under the Security Act to request data processed by the Prosecution Service.

The TIBEK is one of the national security services of Hungary. Its data processing regulated by the Security Act differs in two respects from those of other national security services. On the one hand, it is not entitled to gather intelligence for obtaining the data it processes, and, on the other hand, it acquires the data necessary for the performance of its activity by means of a direct electronic data connection with the group of cooperating bodies defined by the law. According to current legislation, TIBEK acquires the data that cannot be obtained through direct electronic connection or the data controllers of which are bodies not belonging to the group of cooperating bodies defined by the law, such as the Prosecution Service, by way of a request under the general data processing requirements of the Security Act.

In view of the above, under Article 40 (1) of the Security Act, the transfer of data is possible according to general rules from the Prosecution Service if TIBEK indicates the purpose of the request for data. This lacking, TIBEK's request for information would not be lawful. However, under Act CLXIII 32 (6) of 2011 on the Prosecution Service (hereinafter 'the Prosecution Act'), there still is a possibility for the Prosecution Service to transfer data as long as the body requesting the data may process the data under law. Regarding the content of the regulation, it can be stated that it is not the statutory designation of the criminal offense concerned that is required for the transfer of data but the indication of the purpose of the request for data.

The Authority found that the conclusion of the cooperation agreement between the Prosecutor Service and the TIBEK and the transfer of data based on it cannot be objected to provided that legal provisions are complied with; that is the regulation of data transfer by way of the cooperation agreement may be implemented if the Privacy Act and cogent rules mentioned above are complied with.

It is important to note that provisions on the processing of personal data of the Privacy Act (the necessity and proportionality of limiting the right to the protection of personal data, the purpose limitation of processing personal data, the lawfulness and fairness of data processing) may not be validly departed from; authorization of requests in a general framework would therefore not be in accordance with the purpose of the legal institution, and would constitute abuse of law. The fact that it is to the transferer of the data to consider the circumstances justifying data disclosure may give rise to uncertainty as to when the transmission of the data is necessary and when not. It is important to emphasize that consideration must be defined clearly, in exclusives terms, so as to point out what circumstances justify the necessity of data requests and their transfer.

IX.6. The Entitlement of the Counter-terrorism Centre to Request Data

In a case somewhat similar to the one described above, an investigation initiated by Commissioner for Fundamental Rights gave rise to the question what data protection requirements the Counter-terrorism Centre (hereinafter 'the TEK') is to meet when requesting data. According to the facts of the case established during the investigation, a permanent officer acting on behalf of the TEK communicated a data request of the TEK verbally on the scene, at the premises of the data controller (a business entity). In this respect, the Authority made the following proposals to the Director-General of the TEK:

- A data request must always be made in writing (in order to be able to control the lawfulness of data processing and to document the data transfer);
- The data request must designate the purpose and legal basis of using the data;
- The written request must precisely specify the range of data requested. This is justified by the fact that the data transferer has the right and obligation to satisfy himself about the existence of the purpose and legal basis mentioned above before he fulfils the data request. This, of course, does not mean that the data controller is entitled to know the specific activity for which the TEK requests the data. In the case of requests for data by law enforcement agencies and national security services—in view of the nature of the activities of these bodies—instead of describing the specific purpose of the request for data, the purpose may be indicated by referring to the law defining the given activities and duties of the body. The designation of the legal basis—in order to perform the specified task—should refer to the law authorizing data requests and to the concrete reference number;
- It was also pointed out that a data request must also include information on remedy (i.e. complaints may be filed with the minister responsible for the control of the body and with the NAIH, both options being available independently of each other).

As regards remedy, the Director-General of the TEK disputed the opinion of the Authority mentioned above, and held that the minister responsible for law enforcement agencies is entitled to investigate a complaint against a data request made in the framework of gathering intelligence by the TEK, and therefore brought the matter to the Minister of Interior Affairs. The Ministry of Interior Affairs agreed with the opinion of the NAIH on both issues, the order of remedy (acknowledging that both the Minister responsible for law enforcement agencies and the NAIH are entitled to investigate the complaint, the two competences can be exercised independently of each other and in parallel) and the data protection requirements to be fulfilled by data requests made in the framework of gathering intelligence.

As a result of the proceedings, the TEK informed the Authority that, although the data request in question became void, a procedure would be established to meet the data protection requirements according to the information provided by the NAIH, and data requests would be drawn up in accordance with the requirements of content and form specified by the Authority.

IX.7. The Publicity of the Information Necessitating the Maintenance of the Crisis Situation Caused by Mass Immigration

One complainant asked the Authority to examine whether it was necessary to maintain the confidentiality of the justification of maintaining the crisis situation due to mass immigration.

Section 80/A (2) of Act LXXX 2007 on Asylum states that a crisis situation caused by mass immigration can be declared in a Government Decree on the proposal by the minister responsible for alien police authority and asylum matters as initiated by the National Commander of the Police and the head of the refugee authority. This was done by Government Decree 41/2016 (III.9). Section 80/A (3) prescribes that the existence of the preconditions of a crisis situation caused by mass immigration shall be monitored on a continuous basis by the National Commander of the Police and the head of the asylum authority, and Section 4 of the Government Decree mentioned above obligates them to regularly inform the minister responsible for alien policing and asylum of the existence of the preconditions of a crisis situation caused by mass immigration.

The Authority started investigation proceedings, and, having regard to the above, sought the Minister of Interior Affairs. In its reply to the Authority, the Ministry of Interior Affairs stated that the report submitted by the National Commander of the Police and the head of the asylum authority did not qualify as classified data under the Classification Act, and the Ministry of Interior Affairs rendered it accessible on the basis of a request for data of public interest. Although this made the further examination of the case devoid of purpose, and Authority therefore terminated it, it is worth mentioning that, during administrative consultations on extending the effect of Government Decree 41/2016. (III 9), the Authority drew the attention of the Ministry of Interior Affairs to the fact that the decision to extend the crisis situation was going to command a high level of public interest, and therefore the information justifying it must be disclosed.

IX.8. Protection of Data Processed During National Security Screening

A private person turned to our Authority because he had received an anonymous defamatory letter, containing details of his private life and family that he believed had been obtained by gathering intelligence. He had previously held an important and confidential position, and so he took into consideration the possibility that the author of the anonymous letter might have had access to information that had been obtained on him and his family during his previous national security screening. He therefore requested an investigation to find out whether a person without authorization could have had access to his national security screening documents containing classified information. The Authority started an investigation, and, during an on-site inspection of the premises of the data controller, reviewed the circumstances of data processing, including the scope of the data processed, and whether an unauthorized person could have accessed the personal data indicated in the submission. In order to clarify the facts of the case, the Authority requested written and oral information from the data controller, examined the documents that could be related to the case, entered the room where processing had taken place, and studied the data processing related to the case. As a result, it was found that data collected during the national security screening may only be accessed under controlled and documented conditions. During the investigation, no circumstance emerged pointing to unauthorized access to data. It could not be ruled out however that the information written in the defamatory letter came from a different source, such as the circle of acquaintances of the complainant. There was no evidence of an infringement of law regarding the processing of the security screening data, and the Authority thus terminated the proceedings in this case.

X. International Relations

All EU data protection authorities focused on preparing for the new regulatory system of the GDPR and the Police Directive in 2017.

With regard to Brexit, the data protection authority of the UK confirmed that it wishes to closely cooperate with the data protection working groups of the EU, and that the competent UK Minister (for digital economy) is committed to the full-scale application of the GDPR as of May 2018. However, the Commission called the attention of the public to the fact that, as of 30 March 2019, the UK would qualify as third country within the meaning of the GDPR and from a data protection point of view with all its consequences.[55]

Numerous bilateral, regional and international conferences were held on the problems of the practical elaboration of general or partial regulations. From among these the following stand out: the V4 meeting of data protection authorities held at Visegrád in October 2017 stands pout, where strategic and organizational issues were discussed by the leaders of the authorities; a training course of several sessions solving GDPR cases organized by the Austrian data protection authority, where the Hungarian NAIH staff were privileged to attend; and a study trip to the Netherlands where we could study on-site the Data Protection Breach Reporting System, which has been in operation since 1 January 2016. (In 2016, more than 6,000 breaches were reported, of which 28% had to do with health, 20% finances, 19% public sector, and 8% telecommunications.)[56]

One of members of the EU delegation conducting the first annual review of the functioning of the new EU-U.S. Privacy Shield Framework adopted on 12 July 2016 and replacing the repealed Safe Harbour Convention, was a staff member of the NAIH. The review report acknowledges the importance of the Framework (more than 2,400 US companies have undergone the certification procedure and become trusted data controllers), but the ombudsperson for investigating data protection complaints for EU Citizens has still not yet been appointed, the Privacy and Civil Liberties Oversight Board, also conducting government control in terms of privacy, also has only one commissioner in office out of five, and, furthermore, there is still no reassuring guarantee system for national security data processing—mass observations—concerning EU nationals.[57]

The Council of Europe has been updating its Personal Data Protection Convention, 'Convention 108', for several years. In this field, only lesser progress was made in 2017, but there were further discussions on the Council of Europe recommendations on the processing of health data and on police data processing; however, the Handbook on Data Protection in Humanitarian Action was brought out, which addresses literally vital issues such as how to protect personal information of vulnerable beneficiaries in war zones, or how encryption of data is possible for messaging applications.[58]

It is also of the highly important that the Digital Rights Expert Group of the Committee for the Rights of the Child of the Council of Europe (CAHENF-IT), an invited member of which was a NAIH staff member, drew up a draft recommendation to the Member States to promote and protect children's rights in a digital environment in 2016–17. The adoption of the material with strict standards of child protection is expected in 2018.

Finally, out of the number of international complaints in 2017, it is worth mentioning the case when a Pakistani citizen informed the Authority that, during registration at the Client Site ('Ügyfélkapu'), his data were not entered in the personal register of foreign nationals using electronic administration (3.NYT). During the investigation of the case, it was found that the foreign representations of Hungary could not offer a way to register in the 3.NYT system, because the equipment they have for the mandatory recording of facial images and signatures were not the same as the ones used in the Offices of Government Issued Documents; thus data transfer between the equipment for collecting biometric data (G3) at foreign representations and the 3.NYT did not function. Regarding the 3.NYT registration, the Deputy State Secretariat for Records Management of the Ministry of Interior Affairs informed the Authority that the IT developments needed for 3.NYT and Client Site registration at the foreign representations of Hungary were completed by the end of 2017.[59]

X.1. Participation in the Article 29 Working Party

2017 was the last full year of the Article 29 Working Party, which primarily carries out consultancy tasks under Article 29 of the EU Data Protection Directive. According to the new data protection regulation, GDPR, its place will be taken over by the European Data Protection Board from May 2018. In 2017, the Working Party focused primarily on the preparation for the GDPR, and set out guidelines to assist data controllers and law enforcement authorities in the practical application of the Regulation.

[55] http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=611943.
[56] The Dutch data protection authority revealed several data-breaching practices in the Microsoft Windows 10 operation system. For details see: https://autoriteitpersoonsgegevens.nl/en/news/dutch-dpa-microsoft-breaches-data-protection-law-windows-10
[57] https://iapp.org/media/pdf/resource_center/Privacy_Shield_Report-WP29pdf.pdf
[58] https://www.icrc.org/en/publication/handbook-data-protection-humanitarian-action
[59] Case no. NAIH/2017/2692/I.

Guidelines were issued the following areas:

• The right of data portability;
• The Data Protection Officer;
• The Lead Supervisory Authority;
• Data protection impact assessment;
• Data protection (administrative) fines;
• Data breach notification;
• Automated individual decision-making and profiling;
• Consent by data subjects;
• Transparency in data processing;
• Several issues related to the transfer of data to third countries.

The guidelines are in English, and are gradually becoming available in all the official languages of the Union.

In 2018, the Working Party also issues new guidelines and finalizes the ones issued for public consultations, thereby completing the information provided to and opinions on the Regulation by the joint bodies of data protection authorities, as well as on its internal activities, it has also issued guidelines on cooperation between the data protection authorities of the Member States, practically the documents of the internal working order. These guidelines were referred to in chapter III as well.

In preparation for the GDPR, the French chairman of the Working Party, Isabelle Falque-Pierrotin, visited Hungary to get acquainted with the country's preparatory work and consult with the staff of the Authority.

X.2. The Subgroups of Article 29 Working Party

X.2.1. The Cooperation Subgroup

The task of the Cooperation Subgroup is to prepare documents for the Working Party that promote cooperation between the authorities, but it should be noted that, for example, documents describing of some procedures between Member States are not disclosed. The task of the subgroup was to elaborate in detail the procedures for one-stop government, mutual assistance and joint operations, and to establish a common position in this regard. It was also the Cooperation Subgroup that prepared guidelines on administrative fines.

In the context of the enforcement of GDPR, it also develops parts of documents, and has also participated in the preparation of a form for notifying data breaches. The task of the subgroup is therefore to prepare the practical tools, forms, and guidelines that assist the smooth and coordinated enforcement of GDPR. This activity will continue, in parallel with the other subgroups, during the application of GDPR, and thus earlier documents will need to be amended and supplemented in the light of practical experience.

X.2.2. The GDPR Enforcement Subgroup

The main purpose of the subgroup in 2017 was to test the three cooperative systems of the GDPR by using the tools developed by the Article 29 Working Party, through various real/generated case studies:

• Mutual assistance (‘cooperation mechanism’);

• Joint operations of the supervisory authorities (consistency mechanism, in particular where the purpose of a supervisory authority is to adopt a measure producing legal effects on the processing of the data of a large number of data subjects in several Member States);

• One-stop government in cross-border data processing.

The subgroup initiated consultations with the data protection authorities, and carried out a European survey of the number of complaints that will be subject to the GDPR consistency mechanism in the future. The European data protection authorities handled approximately 65,000 complaints, 9,000–11,000 of which shall be subject to the consistency mechanism, and these cases are mostly related to the data processing of international IT companies.

In order to ensure its consistent enforcement throughout the Union, the GDPR confers the same tasks and actual powers to the supervisory authorities in each Member State, including powers of investigation, corrective powers and sanctions, and authorization and advisory powers, in particular in cases of complaints from natural persons, and without prejudice to the powers of prosecutorial authorities under Member State law, to bring infringements of this Regulation to the attention of the judicial authorities and engage in legal proceedings.

The subgroup, together with the Cooperation Subgroup, develops guidelines to make enforcement as consistent as possible, thus contributing to the development of a single system of GDPR-based criteria.

X.2.3. The International Transfers Subgroup (ITS)

A priority topic of this subgroup in 2017 was the examination of trade-related issues in the framework of the annual review of the Privacy Shield; work, however, focused on the preparation for the GDPR:

• Adapting previous WP 29 documents (working documents WP153 and WP195) to a tabular format, providing data controllers and data processors with the compulsory content elements of BCRs when drafting and approving them.

• Delivering an opinion on examining the adequacy of the level of data protection in a given third country, providing guidance to the Article 29 Working Party and the Commission on which basic data protection rules and principles are indispensable on the basis of the GDPR for the adoption of an adequacy decision.

• Guidelines on transfer of data to a third country, the legal basis applicable in specific situations under Article 49 of the GDPR.

The above opinions will be finalized and published by Article 29 Working Party in 2018 on its website.

With the help of the subgroup experts, a number of cooperation procedures under working document WP 107 were carried out on specific issues. As a result, the list of approved BCRs can be found on the Article 29 Working Party website.

X.2.4. The Borders, Travels and Law Enforcement Subgroup (BTLE)

This subgroup finalized a document package containing recommendations on the interpretation and analysis of the most important provisions of the Police Directive. From the point of view of transposition and application of the Directive, the most important question is whether or not the procedure has a punitive character and purpose. The meeting agreed that, in practice, the data processing of international criminal justice cooperation and the Financial Intelligence Units (FIUs) providing analysis on preventing money laundering in the Member States are subject to the Directive—alongside the data processing involved in classical law enforcement activities, such as conducting criminal and law-infringement procedures, enforcing penalties, and protecting public order and public security.

The subgroup agreed to develop a common methodology for controlling large-scale IT systems in the area of freedom, security and justice (SIS II, VIS, Eurodac, CIS, Europol IS), as there is relatively much overlap between these systems and their control mechanisms in terms of data protection.

The European Court of Justice in its opinion of 26 July 2017 found that there was a lack of necessity and proportionality in relation to the PNR data transfer to Canada. Due to the opinion, the renegotiation of the EU-CAN PNR Convention became necessary. The subgroup started to analyse and process the opinion.

In addition, the subgroup developed standard forms for the exercise of the right of access of the data subjects in respect of data transfers under the Privacy Shield. These forms were published on the websites of national data protection authorities in the national language concerned. The criminal/ national security data form is available on the Authority's website in Hungarian.[60]

X.2.5. The Technology Subgroup (TS)

This subgroup was designated to prepare guidelines for data portability, data protection impact assessment, data breach notification, and data protection certification. Of these, the most urgent issue was the subject of data portability, as it provides the greatest help for data controllers in the interpretation of this new right of data subjects. The document was submitted for public consultation by the Article 29 Working Party, and the final text of the guidelines was prepared by taking into account more than 600 pages of comments.

Given the fact that several data protection authorities have developed their own methodology for the conduction of data protection impact assessments, the guidance includes no specific methodological description, only general requirements of data protection impact assessment methodology, and refers to the existing standardization of impact assessment methodologies in Member States and internationally. The submissions received after the public debate were incorporated by the subgroup in the final text of the guidelines.

Public consultation on personal data breach notification is in progress in 2018.

[60] https://www.naih.hu/kuelfoeldi-adattovabbitas.html

The guidelines on certification divided by the sub-group into two separate topics—accreditation and the basic requirements for data protection certification mechanisms—resulting in two separate documents. The guidelines are being drafted.

In addition, the subgroup issued an opinion on basic data protection issues of controlling employees and the proposal for a new ePrivacy Regulation, and commented in a letter on the concepts of regulating intelligent transport systems and the data protection aspects of the public registration database of the ICANN domain. The consistent approach of the Article29 Working Party as formulated in its correspondence has achieved significant progress in both of the above mentioned issues.

X.3. Participation in the Joint Data Protection Supervisory Bodies of the European Union

X.3.1. The Schengen Information System Supervision Coordination Group (SIS II SCG) and the Schengen Affairs of the NAIH

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 2017.

On 2 May 2017, the European Data Protection Supervisor (hereinafter 'the EDPS') issued an opinion on the future operation of the SIS II system, as the system could handle several new biometric identifiers in the future, such as: facial images, finger and palm prints, as well as DNS profiles. According to the EDPS's criticism, the necessity for data processing (for example, in recording facial images, decreasing the age limit for taking fingerprints to 6 years of age, the prescription of 5 years' storage) is often questionable.

The meetings discussed the European Search Portal, an ongoing development aiming to provide interoperability to the large EU IT systems. The essence of the development is that it can simultaneously be used to search almost all databases through a single interface (SIS, VIS, Eurodac, ECRIS, ETIAS, EES). The system would separate access privileges in such a way that, with regard to the data stored in the database for which the user does not have direct access, it would only give one match/no match signal, and so the user can turn later on directly to the data controller. The system will also be able to compare data contained in each database and list similar data (on the basis of biometric data).

The implementation of the Automated Fingerprint Identification System (AFIS) project started with 8 Member States participating in the first phase (Hungary is not among them). As of 4 July 2018, Member States will have to apply new standards for fingerprints and convert existing NIST files to new standards. Conversion has already been completed by some Member States, and the process is well under way.

In addition to the above, the European Commission conducted Schengen data protection inspections (SCHEVAL) in seven Member States (DK, IS, SE, NO, ES, HR, UK) in 2017.

In 2017, 16 review requests were filed with the NAIH with regard to the processing of personal data in the SIS II. A total of 18 persons—7 Kosovar, 3 Hungarian, 2 Serbian, 2 Algerian, 1 Albanian, 1 Nigerian, 1 Macedonian, and 1 American citizens—were concerned (one of the submissions concerned 3 persons). The Authority conducted 5 review proceedings; in the other cases, it provided general information to the petitioners on the right to petition the National SIRENE Bureau and the procedure thereof. In one of the review proceedings, NAIH found that the SIS alert issued against the complainant had already been removed from the system, but the national entry and residence ban imposed by the Immigration and Asylum Office (BMH) was in force. The petitioner was informed of the possibility of petitioning the BMH.

In the other case, the complainant requested the cancellation of the SIS alert against him, but the SIRENE Bureau informed him that his right to reside in Hungary had ceased and that his residence card was also withdrawn, and, pending the final closing of the proceedings before the BMH, cancelling his Norwegian SIS alert was not warranted. The investigation revealed that the foreign complainant had not abandoned to exercise his right of residence in Hungary, and had a valid residence card, as a result of which the BMH initiated the cancellation of the Norwegian SIS alert.

The starting point in another review case was that the complainant had bought a car in Italy at a wholesale car dealer, and upon its registration in Hungary, it turned out that the Italian authorities had issued a search warrant for its previous registration number. The Hungarian police seized the documents of the car—whereby the Hungarian owner could not register it—and sent them to the Italian Embassy in Budapest. According to the information provided by the Italian Embassy, the Schengen warrant was for the registration number stolen in Italy, not the car itself. On the basis of the NAIH's intervention, the Office of International Cooperation on Crime (NEBEK) made a further check on the warrant for the Italian registration number, and found that it had been revoked in the meantime by the competent Italian authority. The competent Hungarian police captaincy also

issued the documents terminating the seizure, and then informed the Embassy thereof. After the above, the bona fide Hungarian owner was able register the car in Hungary.

In April 2017, the NAIH conducted an on-site inspection of the N.SIS II Office at the Deputy State Secretariat for Records Management of the Ministry of Internal Affairs, the domestic operator of the SIS. The legal basis for the inspection was based on Section 34 of Act CLXXXI of 2012 (the SIS II Act) and Article 60 of Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II).

In the course of the inspection and by way the questionnaire sent in advance, NAIH staff checked the fulfilment of the conditions for the lawfulness of data processing, the method and legal basis of data entry, the logging of the data processing operations, the questions of purpose limitation and proportionality of the data processing, the definition and implementation of tasks, and they also visited the server room to ascertain its physical security as well. For a general examination of system logging, three searches were made in connection to SIS II specific complaints. No unlawful data processing was found on the basis of the range of data processed and the log data.

Overall, it can be stated that N.SIS II Office fulfils its legal requirements and operates in accordance with the data protection framework. However, the application providing access to SIS II needs to be improved, and a fault that causes the previous user's query data to 'get stuck' in the system and be visible to a person logging in later from the same workstation must be corrected.

X.3.2. The Customs Information System Supervision Coordination Group (JSA Customs and CIS SCG)

On 1 May 2017, JSA Customs, the authority that had supervised the customs information system of the 'old third pillar' of the EU, was integrated into the Customs Information System Supervision Coordination Group (CIS SCG). The JSA Customs Authority was therefore formally terminated, but its duties and the cases within its competence were taken over by CIS SCG.

Representatives of the European Anti-Fraud Office (OLAF) delivered a presentation to the CIS SCG on the information security settings and rules of the so-called the Anti-Fraud Information System (abbreviated as AFIS, not to be confused with the Eurodac-related Automated Fingerprint Identification System, also abbreviated as AFIS). OLAF's internal data protection officer had also been involved in the development of the rules. Personal data breaches are reported via the internal data protection officer. OLAF reviews its security policy every two years, and updates the system when new threats emerge. They also have automatic tools to control logs. An e-learning module was also developed to help users learn to use the system.

The Coordination Group also prepared a document for the common audit framework for the national supervision of the CIS.

X.3.3. The Eurodac Supervision Coordination Group (Eurodac SCG)

The Eurodac Supervision Coordination Group is responsible for the data protection supervision of Eurodac, the system containing fingerprints, heard a report by an eu-LISA[61] representative on the latest developments in the Central System. Currently, there are about 7 million records in the system, but the aim is to ensure that storing 10 million entries will cause no problem in the future. The most common faults in the system arise from the poor quality of fingerprints. The eu-LISA is conducting an impact assessment in connection with the amendments of the Eurodac Regulation and related future developments.

The Coordination Group compiled a questionnaire for Member States on the exercise of the rights of data subjects. The questionnaire will be forwarded by the national data protection authorities to the national authorities concerned. After the aggregation of the responses, a report containing recommendations will also be compiled.

X.3.4. The Visa Information Supervision Coordination Group (VIS SCG)

The representative of eu-LISA reported on latest developments in the central system. With regard to the quality of fingerprints, statistics showed that Hungary takes them with one of the best error rates (only 3.5% are unacceptable). The European Commission is currently conducting an impact assessment on the need to take the fingerprints of children above 6 years of age (this is currently technically possible). It will also be an important new development when copies of passports can be uploaded to the system in the future.

In the context of the uploading long-stay visas and residence documents to the Visa Information System (VIS), a public consultation was held until 9 February 2018; participation in it was enabled by filling in an online

[61] European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice.

questionnaire.[62] The consultation launched on decreasing minimum age for taking fingerprints from 12 to 6 years ended on 9 November 2017.

X.3.5. The Europol Cooperation Board

The Europol Cooperation Board held a total of three meetings in 2017, at which the NAIH represented Hungary. Its first meeting took place in April still within the framework of the Joint Supervisory Body (JSB) Europol, the body with a mandate for the independent supervision of Europol. The most important change in the operation of the body responsible for the independent supervision of Europol's activity is that, with the entry into force of the new Europol regulation as of 1 May 2017, the Cooperation Board took over the responsibilities of JSB Europol previously entrusted with these tasks, and, at the same time, JSB Europol ceased its operation. For the new Body, the European Data Protection Supervisor shall carry out the administrative and secretarial tasks, and shall be represented by a permanent representative at the meetings. The files and knowledge base relating to JSB Europol's operation was transferred to the EDPS; the internal procedural order was finalized and accepted by the first meeting of the Cooperation Board.

At the end of January 2017, JSB delegates attended an inspection at Europol, which examined how far they had met the recommendations of JSB (more than 80). In most cases, the recommendations had been implemented, 38 were still in progress, but in four cases no significant progress had been made. In general, Europol has developed a clear culture of data protection, it is serious about data protection compliance and JSB recommendations. It is a drawback that, due of their huge amounts, data were not filtered, and appropriate analyses were not made.

On the basis of its opt-out right, Denmark rejected to apply the new Europol Regulation at a referendum, and will thus be considered a third state for Europol data transfers. Irrespective of this, Denmark will continue to participate in the work of Europol in the same way and maintain its national unit, but cooperation will be based not on the Regulation but a bilateral agreement between Denmark and Europol.

Furthermore, the EDPS formulated a recommendation to Europol, because individual data processing purposes were not clear enough. On 15 December 2017, the EDPS carried out an inspection at Europol with the assistance of the Italian data protection authority, focusing mainly on compliance with the new Europol Regulation, information security, data security, and data retention.

X.3.6. The International Working Group on Data Protection in Telecommunications (IWGDPT)

In 2017, the Working Group adopted an opinion on personal data processed by e-learning platforms; the data protection issues of the domain-register ICANN whois database; the international principles of gathering intelligence; the issues of updating firmware and software and the principle of data protection for accountability; on issues related to cross-border data requests for law enforcement.

The 2018 spring meeting of the Working Group will be hosted by the NAIH in Budapest on 9–10 April.

X.3.7. The Police Cooperation Convention for Southeast Europe (PCC SEE)

Hungary acceded the Convention by the entry into force Act XCII of 2012 on 11 December 2012. The objective of the Convention is to increase security in the region and prepare the Western Balkans for membership in the European Union. The Contracting Parties shall step up their cooperation in the prevention of threats to public security, and in the prevention, detection, and police investigation of criminal offenses. The NAIH is a member of the Data Protection Working Group of the Committee of Ministers, the main decision-making body for the implementation of the Convention. The Data Protection Working Group prepared a draft data protection implementation agreement for its December 2016 meeting, which was finalized on the basis of opinions and comments received from the data protection and law enforcement authorities of the Contracting States in Belgrade in late May 2017. There is currently no further information regarding the promulgation of the Implementation Agreement and its implementation in the national laws of the Contracting States.

X.3.8. The TFTP Agreement

On 28 June 2010, the European Union and the United States of America concluded the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program (TFTP Agreement). Within the framework of the agreement, which entered into force on 1 August 2010, the parties process and transmit millions of financial data annually. The TFTP Agreement also includes data protection guarantees in accordance with EU and national rules to protect the personal data of EU citizens. Such is the right

[62] https://ec.europa.eu/home-affairs/content/consultation-extending-scope-visa-information-system-vis-include-data-long-stay-visas-and_en.

of access pursuant to Article 15 of the TFTP Agreement and to the rectification, erasure or blocking under Article 16 thereof.

A Hungarian citizen initiated proceedings by the NAIH for access to his personal data processed in the TFTP system. The Department of Treasury of the United States informed the NAIH that the complaint had been examined, and no infringement was experienced regarding the processing of personal data. However, specific information on processing of the complainant's personal data was denied, because disclosure is subject to the restrictions set out in Article 15 (2) of the TFTP Agreement[63] and would be contrary to Section 522. § (b) (1) and (b) (7) (E) of Freedom of Information Act. Based on the above provisions of law, disclosure of information to the data subject about the processing of his or her personal data by US bodies can be lawfully denied by reference to law enforcement, combating terrorism, and eliminating national security risks. Disclosure of information may also be denied if the bodies concerned do not otherwise process the data of the person requesting information. With regard to the denial of disclosing information to the data subject, the body has no further obligation to state reasons under either US law or the TFTP Agreement. The Hungarian complainant appealed against the decision. In his appeal, he argued that he had never been to the USA, and that it was not clear from the information provided whether his data were processed by foreign authorities. He assumed that his personal data were processed, because otherwise the denial would not make sense. The US Deputy Assistant Secretary for Privacy, Transparency and Records judged the appeal and upheld the decision, pointing out that both US and EU citizens were entitled to the same rights, the content of the answer did not depend on whether the applicant was an American or a European citizen. The complainant had the right to appeal against the decision before the Federal Court of the District of Columbia.

X.4. International Projects

X.4.1. Macedonian project

In the framework of the tender called „*Support to access to right on protection of personal data in Macedonia",* in which the NAIH is a consortium partner, and which is financed by EUROPAID, study visits in the Republic of Macedonia continued in 2017. The three topics the NAIH experts focused on were: international cooperation in data protection, harmonization of the two informational laws and data protection cases of the courts, prosecution and the ombudsman's data processing. As part of the project, staff members of the Macedonian Data Protection Authority visited the NAIH in Budapest, and got acquainted with its internal operation and procedures, visited Magyar Telekom Nyrt, and consulted with data protection officer of the company.

X.4.2. The STAR Project

In November 2017, the start of our new EU data protection project—STAR (Support Training Activities on the Data Protection Reform)—began with the kick-off meeting in Budapest. The 24-month project is co-funded by the European Union, and alongside NAIH, partners are the Vrije Universiteit (VUB) in Brussels and the British Trilateral Research Ltd (TRI), and the objective is the compilation and testing of training material on the GDPR for data protection authorities and data protection officers. For further details about the project, visit https://projectstareu.wordpress.com/.

[63] Article 15 (2) of the TFTP Agreement states: 'Disclosure to a person of his or her personal data processed under this Agreement may be subject to reasonable legal limitations applicable under national law to safeguard the prevention, detection, investigation, or prosecution of criminal offences, and to protect public or national security, with due regard for the legitimate interest of the person concerned.'

XI. Annexes

XI.1. The Awardees of the NAIH Medal in 2017

I. The NAIH awarded its 2017 medal to Zoltán Pokorni, teacher, Mayor of Budapest District XII, for the developing and implementing of the Buda Hills Area ONProtection Programme.
Zoltán Pokorni, as the head of the Buda Hills Area Local Government, together with his colleagues, created and maintained a complex legal awareness-raising, sensitizing local programme designed to prepare children, their parents, and teachers for the digital world, its potential dangers and threats, future challenges.

The digital world offers a variety of benefits for children both in learning and in communication, but there are also many potential hazards that can have negative effects on their emotional and mental development. That is why all activities of teaching and training children to use the Internet consciously are very important. NAIH has its own initiatives, but also pays attention to and supports those of other organizations, and, in this respect, found the awareness-raising programme of a local government in Budapest to be of special importance.

The Buda Hills Area ONProtection Programme of the local government of Budapest District XII applies a complex approach, engages dedicated professionals, defines children, teachers, and parents as its target group in order to achieve its goal in the long term. It implements it programme efficiently and creatively by enabling (and funding) infographic short films, posters, leaflets, parent academies, peer mentoring programmes, and accredited teacher training programmes, and thereby sets an example to other public actors.

It is important to note that this is not a campaign, although it does have elements of campaign; instead, the programme tries to create a routine in district schools, linked to a fixed time, that involves all those concerned at once. The initiative annually invites teachers to a special training course, secondary school students for a so-called peer-to-peer training, which ends with a mentor-training programme, and parents to an academy-type of dialogue.

The preparation for the 2016 programme started with a scientific survey, in which self-assessment questionnaires helped to map the problems, which revealed parents' misconceptions about the Internet use of their children. For example, only 6% of the parents think that their child communicated with a stranger on the Internet, while in reality this figure is 21%.

The programme includes: awareness-raising, a 60-hour accredited teacher training course, panel-discussion academies for parents, and peer-to-peer training, as it is obvious that a somewhat older 'smart guy' will have a more open and receptive target group in his younger peers.

The films and information material on the website and the organization of the programme have serious work and considerable resources behind. The programme focuses on the future of the local community in dealing with the digital security and education of future generations. It is our hope that this enterprise will set an example not only for other communities but also at national level.

On the basis of its Rules 19/2012 NAIH, the National Authority for Data Protection and Freedom of Information awarded the silver medal to Zoltán Pokorni, the mayor of the Buda Hills Area Local Government (representing the staff members of the programme) for outstanding activity in Internet data protection and the promotion of safe and legally conscious use of the Internet by young people.

Zoltán Pokorni and Attila Péterfalvi

II On the occasion of the Freedom of Information Day, NAIH awarded its medal to the head of the Office of the Chief Clerk of the Office of the Mayor of Budapest, its internal data protection officer, in 2017.

Molnár Katalin has been working at the Office of the Mayor of the Municipality of Budapest since October 2003, initially as a data protection administrator, and since May 2006 as an internal data protection officer. In 2011 she was appointed acting head of office and then head of Office of the Chief Clerk in 2014. In 2010 she received a professional counsellor title. Her tasks include not only supervising the enforcement of data protection rules but also fulfilling requests for data of public interest and ensuring the freedom of information.

Like all public bodies, the Mayor's Office also has a duty—even more emphatic due its status under public law—to ensure that the public is informed of the substantial content of the data it processes, to disclose a substantial part of them, as well as to fulfil requests for data of public interest on a daily basis and within the deadline prescribed by law.

Administering and coordinating daily affairs and internal trainings, Katalin Molnár has worked to raise employees' awareness of the importance of the freedom of information and to ensure the appropriate enforcement of the rules of data protection and freedom of information at the 1000-strong office.

In addition to ensuring the opportunity to request data of public interest, the legal institution of the obligation of publication is another legal pillar of publicity. The desirable practice for bodies with public service functions is to publish accurate and updated data on their activities and management on their websites—data to be made public under law. It is to the merit of the awardee that the Office's financial system is linked to the e-Information Freedom system, whereby not only are the data of contracts over HUF 5 million disclosed but also those below this limit; a much larger proportion of the contracts can therefore be accessed without actively requesting data. This forward-looking initiative sets an example to other bodies with public service functions.

Katalin Molnár and Attila Péterfalvi

XI.2. The Conference of Internal Data Protection Officers

In 2017 also, the Authority organized the Conference on Internal Data Protection Officers, the theme of which was, of course, preparing for the new data protection regulation. In the first part of the Conference, issues related to GDPR, such as the rights of data subjects, personal data breach notification, the issue of legal bases, and the changes in sanctions system, were on the agenda.

With regard to the Police Directive, the second part of the Conference discussed the rights of data subjects, the scope of the Authority, personal data breach, impact assessment, and cooperation between the authorities and jointly supervised data processing.

Interest in the Conference was high, with more than two hundred internal data protection officers registering. Given that the Conference is a good form of communication and cooperation between the Authority and data controllers, it is expected to be regularly organized by the Authority during the application of the GDPR after May 2018.

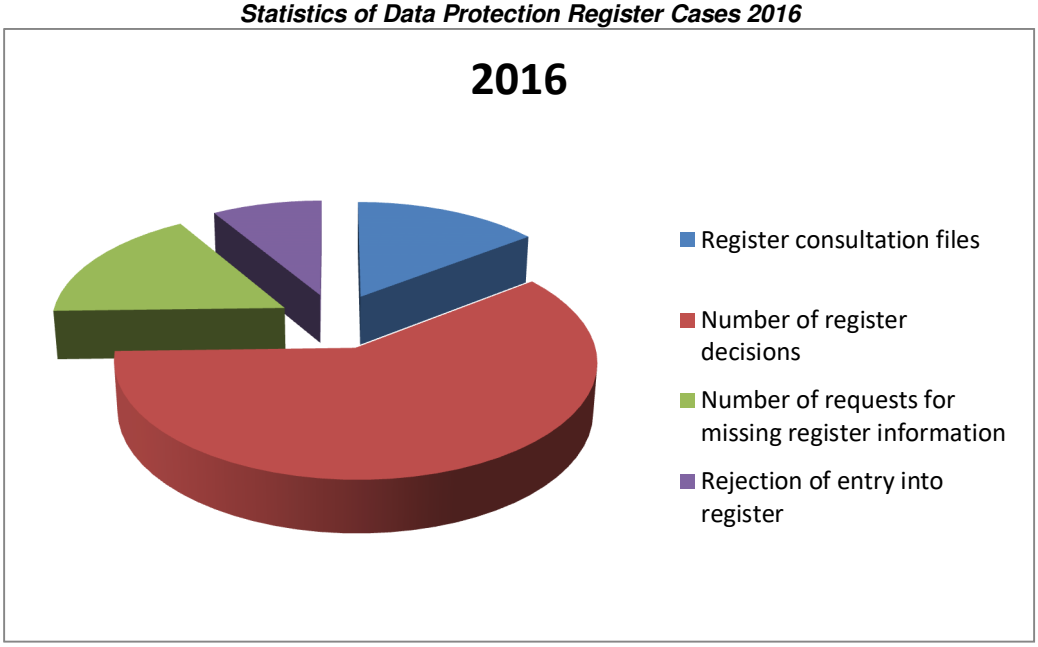
XI.3. The Data Protection Register and IT

In 2017, Data Protection Register tasks were fulfilled by the Department of Information Technology, Administration and Registration. The processing of submissions and related operational tasks were carried out by two persons in 2017.

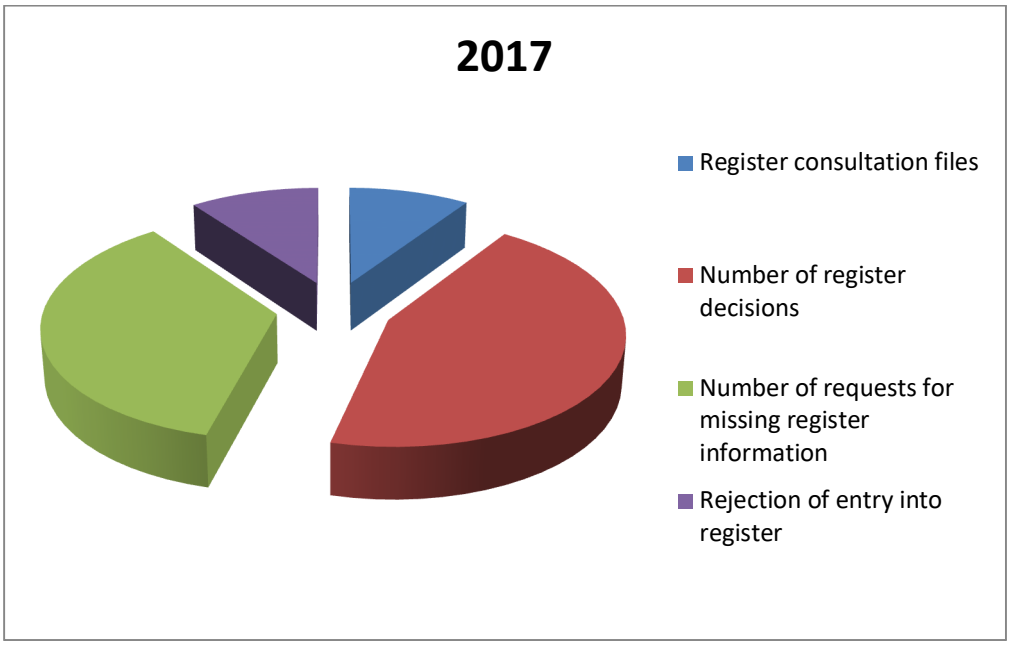
Statistics of Data Protection Register Cases

	2016	**2017**
Register consultation files	2,983	2,522
Number of register decisions	12,275	11,890
Number of requests for missing register information	3,437	9,614
Rejection of entry into register	1,766	2,702
Register files total:	**20,461**	**26,728**

Statistics of Data Protection Register Cases 2016



Statistics of Data Protection Register Cases 2017



The number of submissions received on paper has further decreased compared to previous years, which is only 6% of all submissions. There was no change compared to previous years in the procedure of requesting entry to the Data Protection Register, in the way registered data processing is modified, deleted, and missing information is provided.

As mentioned in the previous chapters of the report, the GDPR does not provide for a national data protection register to be maintained by the data protection authorities of the Member States as the Privacy Act the does. Article 30 of the GDPR obligates data controllers and data processors to maintain a record of processing activities under their responsibility. This will mean that data controllers and processors will keep their own records of their activities, and shall not have to report thereof to the Authority. The obligation to report to the current registry will cease as of 25 May 2018.

XI.3.1. The NAIH Project to Support the Preparation for Applying the GDPR

The Integrated Legislation System (ILS) is being set up under Government Decision 1004/2016 (I.18) and the framework of Priority Government Project KOPOP 1.0.0 –VEKOP-15, among projects aimed at reducing the administrative burden on the budget.

The project involves the administrative and procedural harmonization, as well as IT modernization of the NAIH's EU obligations to track changes in law.

After several months of preparation, we signed the first amendment of the ILS Project Grant Contract under Government Decision 1585/2016 (X.25) in April 2017, which designates the Authority among the consortium partners and the tasks supported by the project and provided for by the GDPR. The NAIH joined the I ILS Project as a consortium partner, taking into account its essential goals and means.

As a result of the project, the full development of an integrated, multilingual intelligent administration and decision preparation module is being set up for the NAIH, moreover the full-scale development of the personal data breach notification systems is also being carried out, including the implementation of the system in terms of IT, IT security, and organization.

Within the framework of the project, we are setting up a system that meets both EU and home requirements, is capable of professionally handling more complex administrative burdens greater in magnitude than before, as well as preparing drafts of Authority decisions at a high level of quality in both legal and linguistic (professional language) terms

It is important to note that the logical approach to the proposed decision preparation module fits in with the GovLex Law-drafting Module. At the same time it differs from it in both structure and components: separately developed, it simultaneously constitutes an integral yet different subsystem from other applications of the ILS.

A client system for the notification of personal data breaches is also being set up, as the GDPR makes it mandatory for data breaches involving data loss and unauthorized access to be notified as of 25 May 2018. The competent national data protection authority, i.e. NAIH, not only receives but also evaluates notifications. Based on the content of the notification and the information available, it may require the data controller to take further action or inform the data subjects. When assessing a data breach, the NAIH may decide to initiate administrative proceedings on the matter.

Parallel to the IT system developments mentioned, it is necessary to enlarge IT, mainly data security and organizational infrastructure (comprehensive organization development), and information security quality assurance.

During the build-up of its subsystems in the project, the Authority provides hardware infrastructure from its own source. Due to the legal status of the NAIH, the project aims to create an independent service system and infrastructure.

Only that part of the functions of the NAIH ILS subsystems can run on the KAK (Government Data Centre) infrastructure, which is functionally located in the ILS base system. These functions are completely separate from the other service-system modules of the NAIH ILS subsystem.

The NAIH ILS subsystem is a service system under development that will perform the law enforcement tasks of the NAIH exclusively. Separated from the ILS base system for security and legal purposes, it will still have integrated features at some points when completed in the near future.

XI.4. Rejected Data and Information Requests

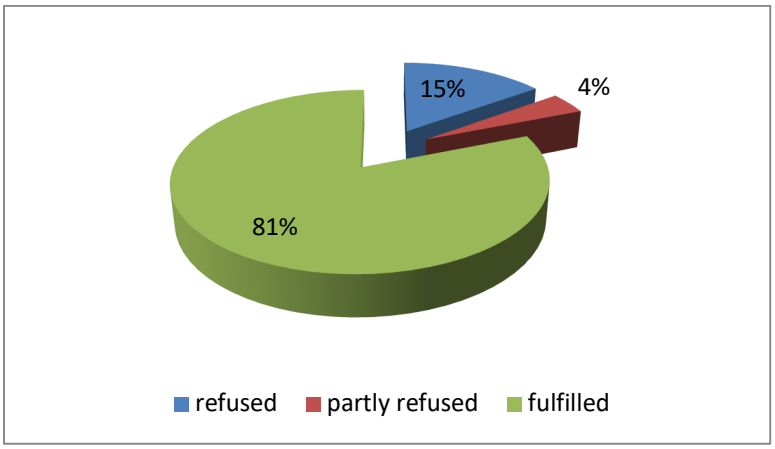
XI.4.1. The Fulfilment of Information Provision Requirements on Refused and Fulfilled Requests and Reasons of Refusal

Under Section 30 (3) of the Privacy Act, the data controller shall keep records of refused requests for information of public interest and of the reasons of refusal and shall inform the Authority thereof by 31 January of each year.

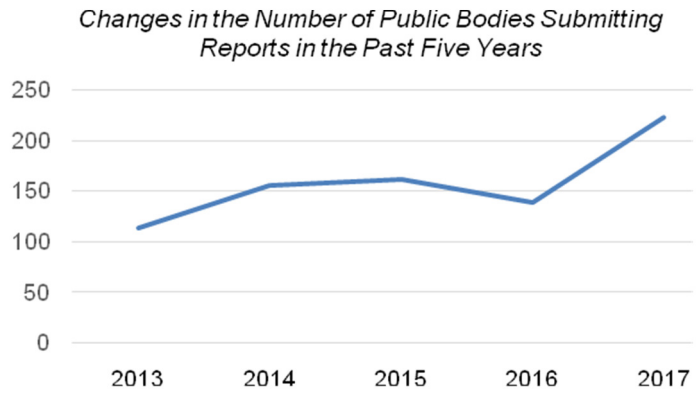
By 21 February 2018, 223 data controllers met the obligation to inform the Authority pursuant to Section 30 (3) of the Privacy Act.

Data requests for data of public interest and data public on grounds of public interest				
Refused (no.)	Partly refused (no.)	Fulfilled (no.)	Total (db)	Number of data controllers
552	150	3016	3718	223

Statistics on data requests for data of public interest and data public on grounds of public interest in 2017



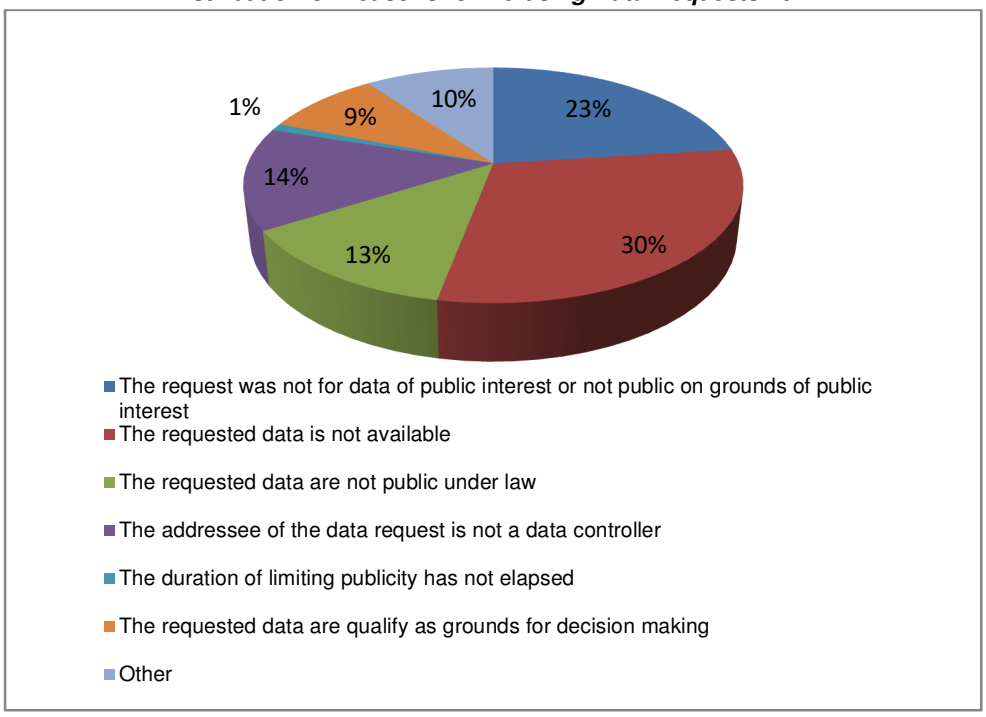
Compared to the statistics for 2016, the tendency fulfilling requests for data public interest by public bodies has improved, as the proportion of refused requests declined by 5%, and the proportion of fulfilled data requests increased by 5%.



The graph shows the fulfilment of reporting obligations by public bodies in the past five years.

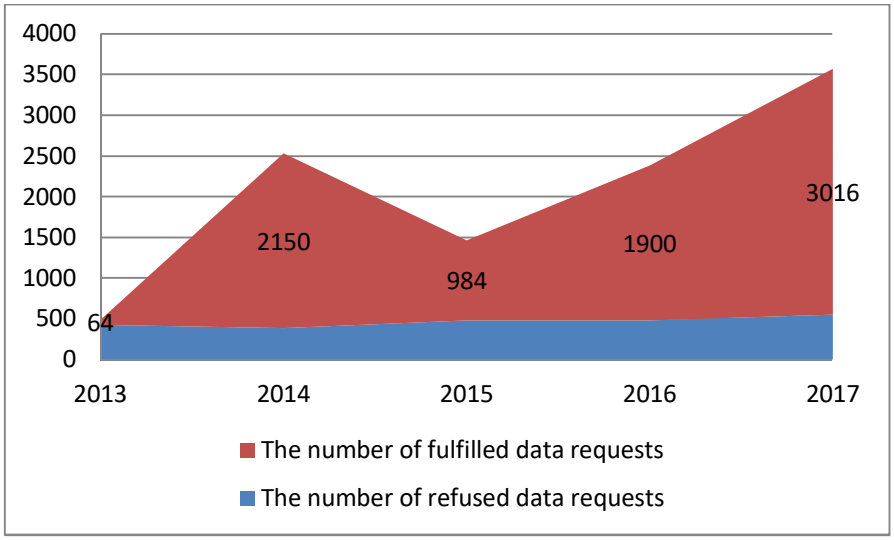
Reasons of Refusal	**Number of References**
The request was not for data of public interest or not public on grounds of public interest	128
The requested data is not available	166
The requested data are not public under law	74
The addressee of the data request is not a data controller	78
The duration of limiting publicity has not elapsed	6
The requested data are qualify as grounds for decision making	50
Other reason	53

Distribution of Reasons for Refusing Data Requests 2017



In contrast to the decline in 2015, the number of submitted and fulfilled data requests increased, suggesting that the activity of data requesters heightened.

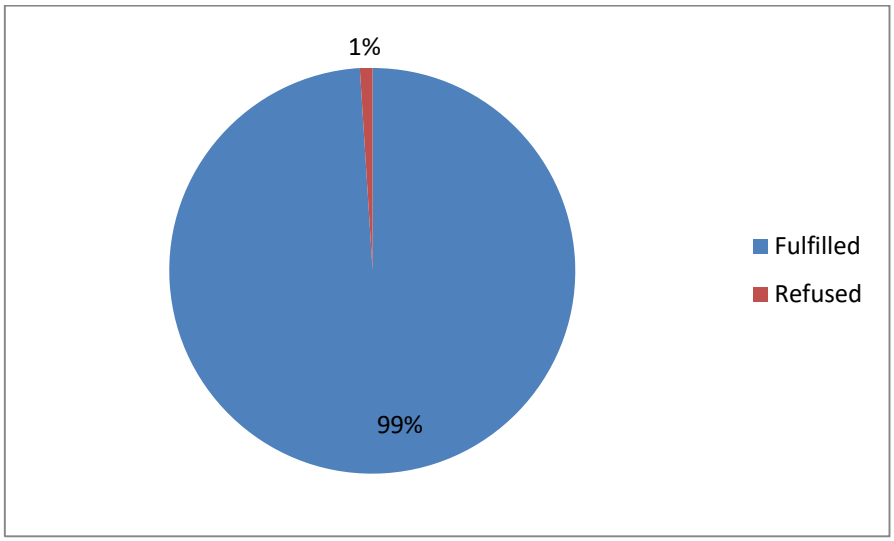
Changes in the Refusal and Fulfilment of Data Requests in the Past Five Years



XI.4.2. The Enforcement of the Right of Access by Data Subjects

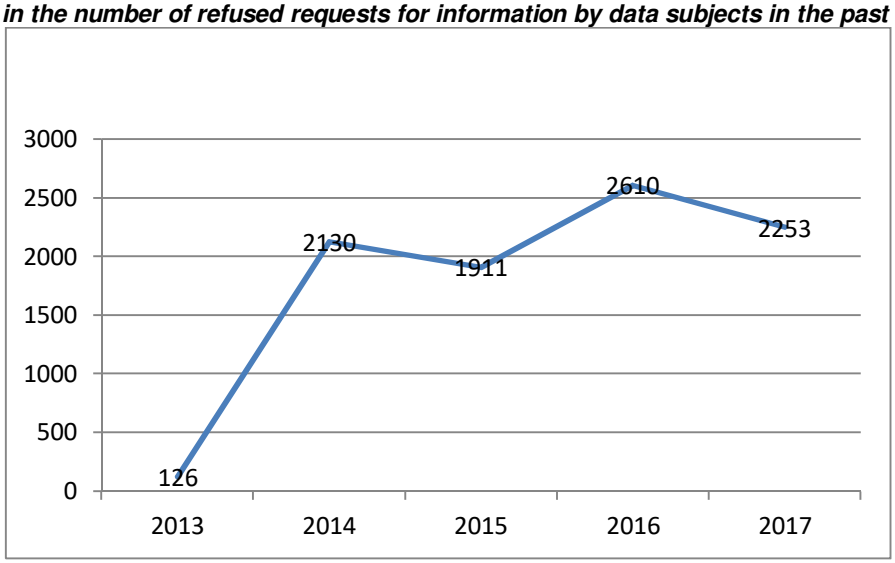
Under Section 14 of the Privacy Act, data subjects may apply to the data controller for information on the processing of his or her personal data or request the rectification, erasure, or blocking thereof. Pursuant to Article 16 (3), data controllers shall notify the Authority of refused requests once a year, by 31 January of the following year.

Data subjects receipt of information on their personal data in 2017



The diagram above shows that data controllers fulfilled data requests at a rate of 99%.

Changes in the number of refused requests for information by data subjects in the past five years



XI.5. The Financial Management of the NAIH in 2017

2017 saw the sixth year of operation and management of the National Authority for Data Protection and Freedom of Information.

XI.5.1. Revenue Appropriations and Performance Data in 2017

The NAIH budget, initial appropriation, was HUF 642,300,000 for 2017, of which the special staff appropriation was HUF 411,800,000, health and pension levies EUR 103,000,000, supplies expenses HUF 105,900,000, and the accumulation-purpose appropriation HUF 21,600,000.

The adjusted appropriation for 2017 was HUF 739,482,000, including the original appropriation, the balance of 2016 including commitments of HUF 50,319,000, and the others revenue of HUF 25,000,000 from the COMFOP-1.0.0-VEKOP-15-2016-00029 tender. Additional revenues included the operation-purpose revenue of HUF 10,268,000, other services revenue of HUF 4,080,000, the invoiced revenue of HUF 1,414,000, and the settled revenue of HUF 2,550,000 from the Arcades project. The wage compensation amounted to 930,000 HUF. The figures are shown in the following table:

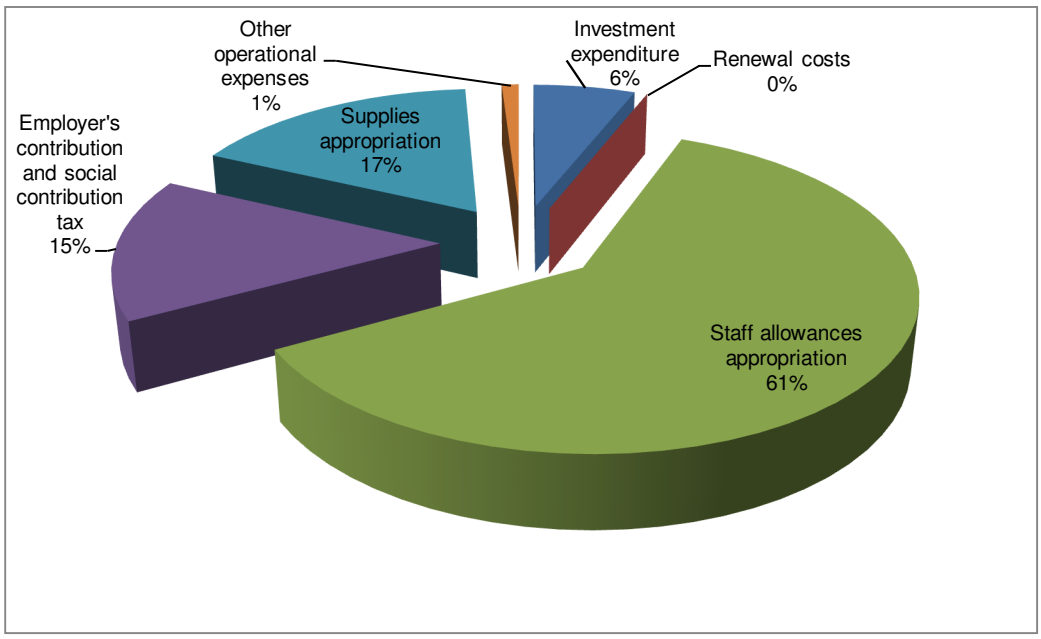
Denomination	Initial appropriation	Adjusted appropriation	Performance	2017 Balance including Commitments
Initial appropriation	642 300			
Other operation-purpose subsidies (KÖFOP)		25 000	25 000	
Revenue related to the power of the state		2 926	2 926	
Services revenues		4 080	4 080	
Invoiced turnover tax		1 114	1 114	
Exchange rate profit		40	40	
Other operation-purpose revenue		10 268	10 268	
Other operation-purpose funds (ARCADES)		2 505	2 505	
2016 balance		50 319	50 319	
Central, governing agency subsidy	*642 300*	*643 230*	*643 230*	
From this: wage compensation, guaranteed wage minimum		*930*	*930*	
Total revenue appropriation:	***642 300***	***739 482***	***739 482***	-
Staff allowances appropriation	411 800	428 970	407 762	21 208
Employer's contribution and social contribution tax	103 000	104 159	98 615	5 544
Supplies expenses appropriation	105 900	130 722	114 749	15 973
Other operation-purpose expenses	-	10 629	10 629	-
Investment-purpose expenses	19 100	63 484	40 169	23 315
Renewal-purpose expense	2 500	1 518	-	
Expenses appropriation	***642 300***	***739 482***	***671 924***	***67 558***

XI.5.2. Expenditure Appropriations and Performance Details

The original budget for 2017 budget was HUF 642,300,000. The adjusted revenue appropriation was HUF 737,482,000, of which the staff allowances appropriations were HUF 428,970,000. The settled employer's contribution and social contribution tax were HUF 98,615,000. Expenditure on supplies totalled HUF 114,749,000. Investment expenditures amounted to HUF 40,169,000, and other operating expenses amounted to HUF 10,629,000.

The following graph shows the distribution of the performance of adjusted appropriations in 2017

The distribution of the performance of adjusted appropriations in 2017



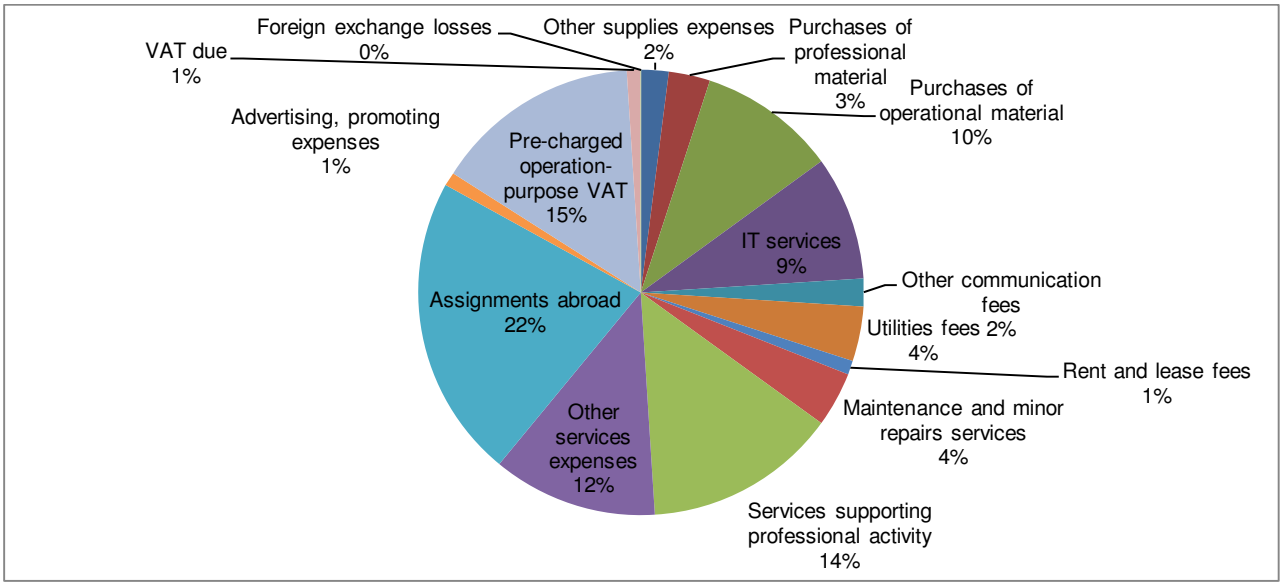
61% of the adjusted appropriations was performed as staff allowances expenditure 2017. The employer's contribution and social contribution tax was 15% in proportion to the total expenditure. Priority supplies appropriations amounted to 17% of the total budget. Investment expenditure accounted for 6% of the total budget. Other operational expenditure was 1%.

The 2017 balance was HUF 67,558,000 including commitments. This included the HUF 25,000,000 from the KÖFOP-1.0.0-VEKOP-15-2016-00029 tender, from which no payments were made in 2017, because its financial performance was subject to the amendment of the contract with the Authority. Due to the delay of the public procurement procedure, a balance of HUF 23,315,000 was generated.

XI.5.3. Distribution of Supplies Expenses

The following diagram shows supplies expenses performed according to the order of headings

Distribution of Supplies Expenses 2017



The bulk of the expenditure on supplies, HUF 24,686,000, i.e. 22%, was made up of those of assignments abroad. Due to the introduction of GDPR in 2018, the number of EU trips increased considerably.

The Authority not being entitled to reclaim, pre-charged VAT for operational purposes made up for 15% of the total supplies expenditure, i.e. HUF 17,153,000. Services supporting professional activity amounted to HUF16,439,000.

Operation materials cost HUF 11,483,000, while IT services HUF 10,880,000. For public utility fees, the Authority paid a total of HUF 4,970,000.

XI.5.4. Revenues from Fines

The fine the Authority imposed and received amounted to HUF 68,010,000, which was entirely the proceeds of the central budget.

XI.5.5. Changes in the Authority Staff

The number of employees of the Authority was 77 on 31 December 2017. The increase in staffing began at the of the year due to the entry into force of the General Adoption of Data Protection Regulation in 2018. Major admissions of personnel are expected from the beginning of 2018.

XI.6. Photos of NAIH Events

The press conference on the 2016 NAIH Report at Parliament

E-commerce Expo 2017, the NAIH stand

XI.7. Participation of the President of the Authority at Professional Conferences And Events in 2017

13January 2017—Paris—International Workshop on Post-Mortem Data Protection—Fate of our personal Data after Decease

19–20 January 2017—Florence—Ch@rterClick! Workshop—roundtable discussion

22–24 February 2017—Berlin—Meeting of FOI Commissioners and Ombudsmen—roundtable discussion

28 February 2017—Budapest, Stefania Palace—Security Market 2017 Conference and Exhibition—Security Development in the Light IT Information Security and Data Protection Rules / Panel discussion

8 March 2017—Budapest—Ernst & Young Conference—Data Protection Regulation in the Light of Technological Progress

23–24 March 2017—Krakow—V4 DPA's meeting—Roundtable conversations

31 March 2017—Budapest, Müpa—CIO Forum 2017—Data Protection Regulation in the Light of Technological Progress

4 April 2017—Budapest, Ernst & Young Conference—Data Protection Regulation in the Light of Technological Progress

10 April 2017—Full meeting of Kaposvár South Trans-Danubian Regional Council for Public Administration and Employment—Data Protection Challenges of the Time

27–28 April 2017—Cyprus, Limassol—Spring Conference of European Data Protection Commissioners—Roundtable discussions

2 May 2017—Budapest, Telekom Headquarters—Conference for the leaders of Telekom's key German clients—New Data Protection Era—Challenges and Duties for the Hungarian DPA

3 May 2017—Budapest—mySec GDPR Conference—Data Protection Regulation in the Light of Technological Progress

4–5 May 2017—Brussels—European University Association Expert Group meeting—Open Access / roundtable discussion

9 May 2017—Budapest—Conference of the Hungarian National Section of AIDA—Current Issues, Challenges of New Data Protection Regulations and Insurance

17-18 May 2017—Tbilisi, Georgia—19th Meeting of the Central and Eastern European Data Protection Authorities—Data Processing by Law Enforcement Sector / roundtable discussion

24 May 2017—Budapest—KPMG Privacy Conference—The New European Data Protection Regulation and Hungarian Aspects

25-26 May 2017—Budapest, Ludovika Campus—Procedural Law in the European Union?—The Review of the ReNEUAL Model Rules, or the European Union Law of Administrative Procedure from the Perspective of

Hungarian Researchers—Scientific and Professional Conference—Procedures of Hungarian Data Protection Authorities Based on GDPR

26–28 May 2017—Bratislava—GLOBSEC 2017 Forum—Roundtable discussion

29 May 29 2017—Budapest, Pázmány Péter Catholic University, Faculty of Law and Political Sciences, 'Gathering Intelligence and Privacy Protection'—The Role of the National Authority for Data Protection and Freedom of Information in Controlling the Gathering of Intelligence

6 June 6 2017—Budapest—The General Data Protection Regulation (GDPR), Changing Regulation, New Challenges—Technological development and Data Protection

13 June 2017—Budapest—ISACA Conference— Data Protection Regulation in the Light of Technological Progress

16 June 2017—Budapest—Taxation in Europe—XIth International Tax Conference—Digitalization and Security: Data Protection Limits

29 June 2017—Budapest—MNV Zrt. Forum—GDPR

4 July 2017—Kecskemét—'Big Data' IVth Public Relations Academy—The Importance and Social Functions of Freedom of Information

5 July 2017—Budapest—Freedom of Information Conference— The Importance and Social Functions of Freedom of Information

6 July 2017—Miskolc—Association of Hungarian Librarians, Meeting 49—Processing Personal Data in Library Life—Current Issues

7-8 September 2017.—Estonia, Tartu—E-Volution of Data Protection—roundtable discussion

11 September 2017—Budapest—ITOSZ Professional Conference / The Application of the EU General Data Protection Regulation in Practice—The General Aspects of the Application of GDPR in Hungary / Keynote Speech

20-21 September 2017—Manchester—International Conference for Information Commissioners in Manchester—Roundtable discussion

September 25-29, 2017—Hong Kong—39th International Conference on Data Protection and Privacy Commissioners—Hungary's first-hand Experiences of how Profound Change to the Political System Affected the Establishment of the New Fundamental Rights

2 October 2017—Tatabánya—Association of Hungarian Librarians Professional Days—Processing Personal Data in Library Life From 2018

5 October 2017—Balatonföldvár—Ministry of Interior Affairs National Office for Disaster Protection Directorate: Data Protection Conference—The New Data Protection Regulation

5–6 October 2017—Eger—Conference of the Association Judicial Counsellors on European Law—The Impact of the EU's New Data Protection Reform on Hungarian law

8–10 October 2017—Visegrád—Visegrad V4 Meeting—DPA's—roundtable discussions

10 October 2017—Budapest—Ministry of Interior Affairs Data Protection Lecture Series—Actualities in the Freedom of Information, Preparation for the Application of the General Data Protection Regulation (GDPR)

16 October 2017—Budapest—Mansion Full Seat—The New European Data Protection Regulation and its Hungarian Aspects

16-17 October 2017—Warsaw—20th Anniversary of the Personal Data Protection Law in Poland—Effectiveness of Privacy Regulations—Hungarian Experiences

19 October 2017—Budapest—GDPR—Conference on New Data Protection Regulation of the European Union in the Light of the Practice—New European Data Protection Regulation and its Hungarian Aspects

24 October 2017—Budapest—Hungarian Army 4th Data Protection Training— New European Data Protection Regulation and its Hungarian Aspects

25 October 2017—Budapest—IVSZ Conference— New European Data Protection Regulation and its Hungarian Aspects

25 October 2017—Budapest—Pázmány Péter Catholic University—Enforcing Article IV of the Fundamental Law in the Legal System—Personality Rights Issues in the NAIH Practice

26 October 2017—Budapest—Conference on the Application in Hungary of the New Data Protection Regulation—The New European Data Protection Regulation and its Hungarian Aspects

November 6–9 2017—Portugal, Lisbon—Web Summit—roundtable discussions

27 November 2017—Balatonföldvár—Further training of Heads of National Secret Services: Data Protection and Information Security—Assessment of the National Security Service Audit

30 November 2017—Budapest—16th National Conference on Honouring the Deceased—The Culture Honouring the Deceased in the Age of Digitalization, in the Mirror of Data Protection and Freedom of Information

5 December 2017—Budapest—Budapest Police Captaincy Conference—The New European Data Protection Regulation and its Hungarian Aspects

X.8. References to Law (Hungarian—English)

- 108-as egyezmény, az Európa Tanács Adatvédelmi Egyezménye: az egyének védelméről a személyes adatok gépi feldolgozása során Strasbourgban, 1981. január 28-án kelt Egyezmény, Magyarországon kihirdette az 1998. évi VI. törvény—*Treaty No.108: The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981, promulgated in Hungary by Act VI of 1998*;
- Adatvédelmi Irányelv, a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló 95/46/EK európai parlamenti és tanácsi irányelv– *Directive 95/46/EC Of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;*
- A Délkelet-európai Rendőri Együttműködési Egyezmény kihirdetéséről szóló 2012. évi XCII. törvény, 2012. december 11-től hatályos—*The Police Cooperation Convention for Southeast Europe, the promulgated in Hungary by Act XCII of 2012*;
- A jogalkotásról szóló 2010. évi CXXX. törvény—*Act CXXX* of *2010* on Legislation;
- A jogszabályok előkészítésében való társadalmi részvételről szóló 2010. évi CXXXI. törvény—*Act CXXXI* of *2010*. On Public Participation in Developing Legislation;
- A menedékjogról szóló 2007. évi LXXX. törvény— *Act LXXX 2007 on Asylum*

- A pedagógiai szakszolgálati intézmények működéséről szóló 15/2013. (II.26.) EMMI rendelet—*Decree 15/2013 (II.26) of the Ministry of Human Resources on the Operation of Pedagogical Agencies.*
- A tömeges bevándorlás okozta válsághelyzet Magyarország egész területére történő elrendeléséről, valamint a válsághelyzet elrendelésével, fennállásával és megszüntetésével összefüggő szabályokról szóló 41/2016. (III.9.) Korm. rendelet—*Government Decree 41/2016 (III.9.) on ordering a nationwide crisis situation due to mass immigration and on the rules related to ordering, maintaining and terminating a critical situation*;
- ÁFA tv., az általános forgalmi adóról szóló 2007. évi CXXVII. törvény—*Act CXXVII of 2007 on Value Added Tax*;
- Alaptörvény, alkotmány: Magyarország Alaptörvénye (2011. április 25.)—*Fundamental Law, Constitution: the Fundamental Law of Hungary (25 April 2011)*;
- Avtv., a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény— *Act LXIII of 1992 on Personal Data Protection and the Publicity of Data of Public Interest*;
- Ávtv., az állami vagyonról szóló 2007. évi CVI. törvény—*Act CVI of 2007 CVI on State Assets ('State Assets Act')*.
- Az Európai Parlament és a Tanács 765/2008/EK rendelete (2008. július 9.) a termékek forgalmazása tekintetében az akkreditálás és piacfelügyelet előírásainak megállapításáról és a 339/93/EGK rendelet hatályon kívül helyezéséről—*Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93;*
- Bit., a biztosítási tevékenységről szóló 2014. évi LXXXVIII. törvény—*Act LXXXVIII of 2014 on the Business of Insurance;*
- Btk., a Büntető Törvénykönyvről szóló 2012. évi C. törvény—*Act C of 2013 on the Criminal Code*;
- Bűnügyi Irányelv, a bűnüldözési célból kezelt személyes adatok védelmére vonatkozó irányelv, az Európai Parlament és a Tanács (EU) 2016/680 irányelve (2016. április 27.) a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről—*Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA*;
- Eurodac rendelet, (EUROpean DActylographic Comparisonsystem) az Eurodac létrehozásáról szóló 2725/2000/EK Tanácsi Rendelet, és 2015. július 20-ával az azt felváltó, jelenleg is hatályos 603/2013/EU Parlamenti és Tanácsi Rendelet—*Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention;*
- Europol rendelet, az Európai Parlament és Tanács (EU) 2016/794 rendelete (2016. május 11.) a Bűnüldözési Együttműködés Európai Uniós Ügynökségéről (Europol), valamint a 2009/371/IB, a 2009/934/IB, a 2009/935/IB, a 2009/936/IB és a 2009/968/IB tanácsi határozat felváltásáról és hatályon kívül helyezéséről—*Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA;*
- Eüak., az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény—*Act XLVII of 1997 on the Protection and Processing of Medical and Other Related Personal Data ('Health Data Act')*;
- Eütv., az egészségügyről szóló 1997. évi CLIV. törvény—*Act CLIV of 1997 on Health ('Health Act')*;
- GDPR, Általános adatvédelmi rendelet, az Európai Parlament és a Tanács (EU) által elfogadott, a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló 2016/679 Rendelet. 2018. május 25-től alkalmazandó—*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, GDPR);*
- Gyvt., a gyermekek védelméről és a gyámügyi igazgatásról szóló 1997. évi XXXI. törvény—*Act XXXI of 1997 on the Protection of Children and Guardianship Administration ('Child Protection Act')*;
- Infotv.Infotörvény, az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény—*Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information ('Privacy Act');*
- Kkvtv., a kis- és középvállalkozásokról, fejlődésük támogatásáról szóló 2004. évi XXXIV. törvény— *Act XXXIV of 2004 on the Definition of, and Aids to, Small and Medium-sized Enterprises*;
- Költségtérítési rendelet, a közérdekű adat iránti igény teljesítéséért megállapítható költségtérítés mértékéről szóló 301/2016. (IX. 30.) Korm. rendeletet—*Government Decree 301/2016 (IX. 30) on the Costs of Disclosure of Data Public Interest*;

- Mavtv., a minősített adat védelméről szóló 2009. évi CLV. törvény—*Act CLV of 2009 on the Protection of Classified Information ('Classification Act')*;
- MNBtv., a Magyar Nemzeti Bankról szóló 2013. évi CXXXIX. törvény—*Act CXXXIX of 2013 on the Magyar Nemzeti Bank ('National Bank Act')*;
- Mt., a Munka Törvénykönyvéről szóló 2012. évi I. törvény—*Act I of 2012 on the Labour Code*.
- Nbtv., a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény—*Act CXXV of 1995 on National Security Services ('Security Act')*;
- Nvtv., a nemzeti vagyonról szóló 2011. évi CXCVI. törvény—*Act CXCVI of* 2011 *on National Assets ('National Assets Act')*;
- Pmt., régi, 2017. június 26. napjáig hatályos, a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról szóló 2007. évi CXXXVI. törvény—*Act CXXXVI of 2007 on the Prevention and Combating of Money Laundering and Terrorist Financing (in effect until 26 June 2017, 'Former Act on Money-laundering')*;
- Pmt., új, a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról szóló 2017. évi LIII. törvény (2017. június 26. napjától hatályos)—*Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing (in effect as of 26 June 2017, 'New Act on Money-laundering').*
- Ptk. új, a Polgári Törvénykönyvről szóló 2013. évi V. törvény—*Act V of 2013 on the Civil Code ('New Civil Code')*;
- SIS II törvény, a 2012. évi CLXXXI. törvény, a Schengeni Információs Rendszer második generációja keretében történő információcseréről, továbbá egyes rendészeti tárgyú törvények ezzel, valamint a Magyary Egyszerűsítési Programmal összefüggő módosításáról—*Act CLXXXI of 2012 on the Exchange of Information Framework of the Second Generation Schengen Information System, as well as the Amendment of Certain Policing Acts and thereby the Magyary Simplification Programme (SIS II Act)*;
- SIS II, a Schengeni Információs Rendszer második generációjának létrehozásáról, működtetéséről és használatáról szóló 1987/2006/EK számú európai parlamenti és tanácsi rendelet—*Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II)*;
- Szaztv., a személyazonosító jel helyébe lépő azonosítási módokról és a kódok használatáról szóló 1996. évi XX. törvény—*Act XX of 1996 on the methods of identification and using of identification codes which replace the personal identification mark, as well as the ASP system of the local governments*;
- Szvtv., a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvény—*Act CXXXIII of 2005 on Persons and Property Protection and on the Activity of Private Detectives (hereinafter 'the Property Protection Act')*;
- Thtv., a társasházakról szóló 2003. évi CXXXIII. törvény—*Act CXXXIII of 2003 on Condominiums (the Condominiums Act)*;
- Ütv., az ügyészségről szóló 2011. évi CLXIII. törvény—*Act CLXIII 32 (6) of 2011 on the Prosecution Service (hereinafter 'the Prosecution Act').*

Contents