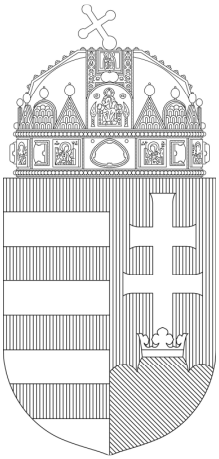
Annual report of the

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

2015

National Authority for Data Protection and Freedom of Information
Budapest, 2016



Preface

Welcome to The Reader,

Year 2015 cannot be defined as a peaceful year, as – including European capital cities - many suffering and restless events took place in the world.

Terrorism and the consequences of the migration, increased security risks and needs, the protection of privacy can all be felt on the field of data protection. Let us think about the identification of the migrants at the Schengen border, or facing the problematic nature of the special legal order which might temporary suspend some constitutional rights.

Data controllers and data protection authorities are facing a big challenge when it comes to the EU Data Protection Reform in 2016, in particular 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.

We hope that - after the two-year preparation period - the case-law concerning this Reform will answer the newest phenomenon and problems both on EU and national levels. Regulation and Directive texts are now available and a study about our competency relating to this acquis will be issued shortly. The additional human resources and extra budget needs relating to these regulations will be examined in the future as well.

These questions will be on focus on the 2016 Budapest “Spring” conference of the data protection authorities of Member States of the EU, which will be organised by our authority. Also this event gives a perfect opportunity to remember the 60th anniversary of the 1956 Hungarian Revolution.

Let us not forget about the small successes of the weekdays. The 2014 Annual Report of the Hungarian National Authority for Data Protection and Freedom of Information was assumed by the dedicated committee of the Hungarian Parliament without any veto. The first specialized legal training year in the history of

our Authority had been also very successful, and the 5th conference of the data protection officers took place as well.

There is a cause for optimism, too regarding the children's and teachers' interest in the protection of privacy which we met during the Arcades-project seminars held for about 200 teachers, introducing teaching materials and the competition of the best privacy lesson in Hungary. Since 2013, one of the NAIH's main priority is to promote the data-protection knowledge of the younger generations and to raise the awareness of the internet-usage ("Key to the Internet!" project). Ten years ago this field was a "terra incognita" occupied by only few data protection authorities, including the Canadian Privacy Commissioner. Today, there are many good practices worldwide which are also available in English language and by taking advantage of these sources, our Authority has also caught up with the best practices. Several Balkan countries are reluctant to take over our experiences and we hope, that through international cooperation in 2016 we will have the opportunity to work on this field.

The Honourable Reader may notice that this year's annual report treats the topic of the application of advanced IT technologies from basic right' approach at least as important as in the last year's report. The main reason is that we are facing more and more legal problems related the usage of advanced IT technologies both when dealing with data-protection complaints and also in the cooperation with the foreign authorities. Here we are facing such high speed changes which can be described revolutionary. Tools, services and concepts are present in our everyday life of which we have never heard before. "Smart" digital devices are surrounding us every day, we use them for our work or just to get connected with each other. We might have a plastic ID card with digital information in our cash money might turn into virtual cash on an online payment system, also Bitcoin is getting more popular every day. We store our data in 'clouds' and a drone is now a common device above our heads. Our life is getting filled with internet related content and services. Objects in our environment – household items, vehicles etc. –are capable of connecting to the internet automatically. The Virtual Reality devices allow people to step into an extended virtual world created by bits.

Behind this phenomenon the progress of information and communication technologies and its influence on the society is getting vigorous. This can be described at one point as a progress which aims to extend the human possibilities, but also as the dependency on technologies. This double-faced status can also be caught in the predictions of the future as well. Optimistic opinions say that the progress of info-communication helps to solve global problems, but pessimistic opinions sug-

gest such an artificial intelligence may get out of human control with unpredictable consequences.

We cannot predict the future, but in the light of basic rights we can determine that the progress of info-communication technologies help to concentrate more information to less information holder ever before, so to say, relieve the major escalation of information inequalities. It is a cliché that information concentration leads to concentration of power. The question is whether states are capable of protecting their citizen's privacy against global firms and other states who are eager to get to know everything. We also need to ask, who is going to protect the citizen's privacy against their own state's hunger for information?

Answers or recipes are not available yet. At the same time, it is reassuring that the protection of privacy in Europe is stepping out of the range of government-related legal control and a unitary EU regulation is expected in this matter which will set the objective of a high level legal protection.
Budapest, 4th March 2016

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

I. Statistical figures and remarkable activities of the Authority

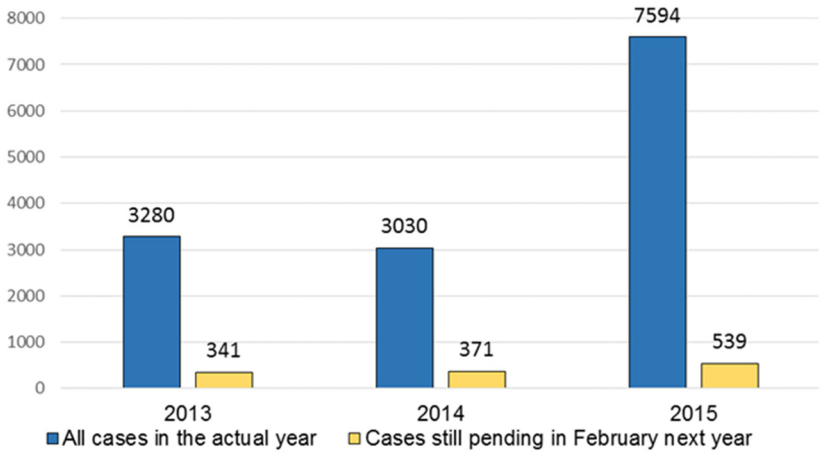
I.1. A statistical summary of our cases

In the year 2015 we had altogether 7594 registered cases which is two and a half more than in year 2014 with 3030 cases. This particular growth is due to the combined change of several factors. On the one hand, the Authority's document managing system has changed, which caused the previous year's ongoing cases to receive new numbers in 2016. Furthermore the number of cases related to data protection register has grown signifi , with 3680 registered cases in 2015, while in 2014 these cases had a number of 588 only, so the growth is more than sixfold. There are also 350 auditing-related cases in the single records managing system. In addition to the above data, the data protection register electronically received 9965 cases which are not presented in the electronic document registration book, so it does not have effect on the case statistic data.

Out of the total 7594 registered cases, 67 cases were affected with the launch of data protection administrative procedure. In some of these procedures multiple data controllers were involved, i.e., in certain single cases numerous organizations became subject to these procedures. 2655 cases out of all incoming submissions were handled as investigation cases which means 800 more cases in 2015. The other cases are associated to other competences of the NAIH such as consultations and enquiries concerning data protection registry, of draft bills, cases of international relevance, conference of internal data protection officers, data protection audit etc. A detailed presentation of data protection administrative procedures can be found in the chapter "Administrative Cases".

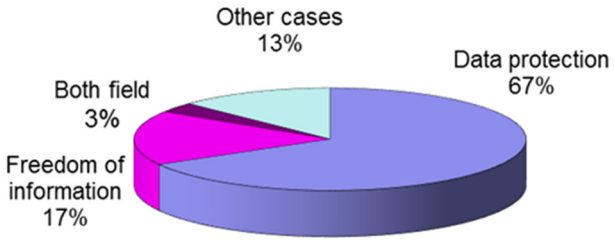
A number of 539 cases from 2015 were in progress on the 1th of February 2016, which is more than in the previous year, although this amount is only 7% of the total cases.

Registered and pending cases of NAIH 2013-2015

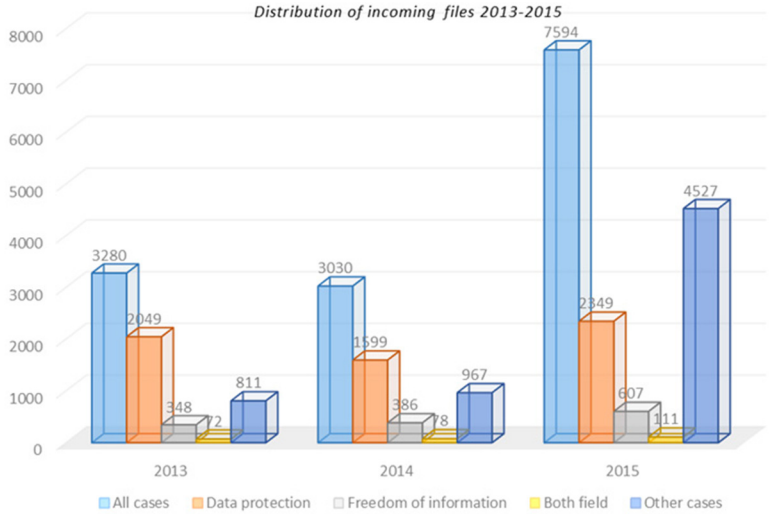


According to Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (hereinafter referred to as *Privacy Act*), NAIH shall be responsible, among others, to supervise and promote the enforcement of the rights to the protection of personal data and access to public information and information of public interest.

Distribution of cases by informational rights in 2015

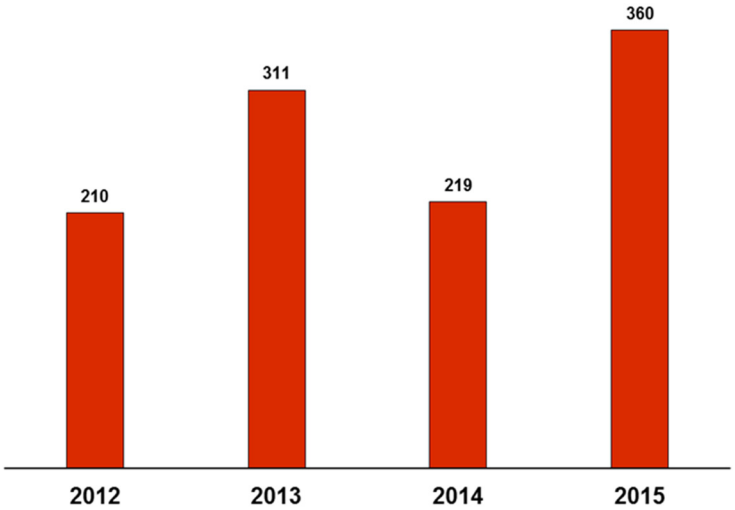


Compared to last year's figure we see that in year 2015, both cases related to basic rights have significantly increased (14% on data protection and 4% on freedom of information).



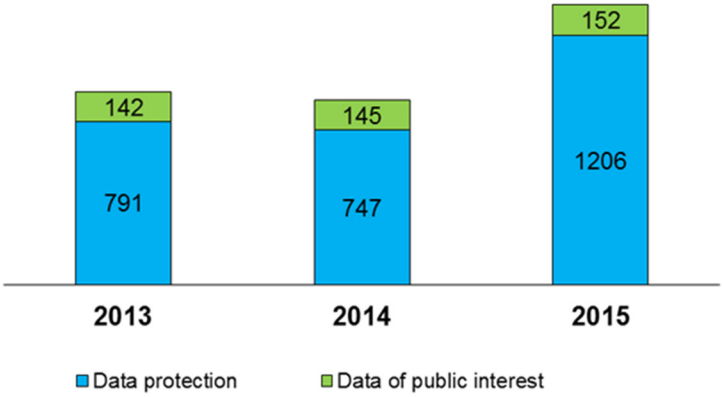
In 2015 we reviewed 360 draft bills, a 64% increase compared to the previous year.

Providing opinion on draft regulations 2012-2015



In 2015 we initiated the amendment of 36 regulations, 26 on data protection and 10 on freedom of information. Out of all cases, investigations in 226 data protection files and 65 freedom of information files were rejected.

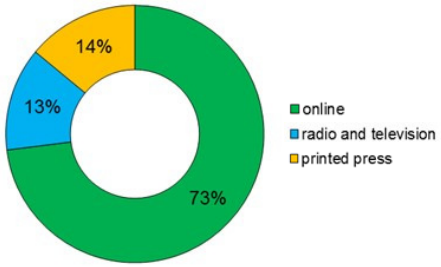
Number of consultation cases 2013-2015



In 2015 we dealt with altogether 144 international cases, additionally, 54 investigation cases had cross-border relevance (EU or third country data controllers or processors were involved). A total of 23 files included data processing of classified personal data or data of public interest. These sets of cases are outlined in different chapters of the present report. In 2015 we received 46 data requests of public interest; all of them were fulfilled. The number of data requests increased slightly in contrast to the previous year. Cases related to Binding Corporate Rules after 1th October 2015 had a number of three.

I.2. The presence of NAIH in the media

Between 1th January and 31th December 2015 the Authority appeared totally 4856 times in the media. The appearance was highest on the internet with 3536 times, in the press 708 times, in other electronic media 612 times.



II. Protection of privacy: new framework – old principles

II.1. The new European Data Protection Regulation

In the past years, the most important endeavour of the European data protection was defining the European data protection legislation package – the new data protection Regulation and Directive – by the European Commission, the European Parliament and the European Council. On 17th December 2015 a compromised proposal was born, and its adoption in 2016 is most likely guaranteed. By the adoption of this proposal a new data protection regime will start, which – after the two -year preparatory phase – will aim to provide a closer cooperation and unified action among Member States, while the privacy principles, the platform of data protection will remain unchanged. The Regulation and the Directive fundamentally organize the data controllers' and public authorities' duties, re-shape the relationship between the authorities and the rules of their cooperation. By the time of its entry into force the authorities will need to be prepared for future application of the new legislation. We will talk about these preparations in the following years' reports.

II.2. New General Data Protection Regulation

The Data Protection Regulation will regulate activities related to the protection and processing of personal data. The directly applicable nature of the legal instrument will result in significant changes in Hungary as well.

The scope of the regulation is expanding: it should be used in all cases when goods or services are offered to persons in the Union, or when the data processing is realized to monitor their behavior. This will be remarkable especially among online data processing and the protection of the market participants' equal opportunity.

The new regulation confirms the users' rights of "to be forgotten" (total deletion) and the portability of the data, latter will help the migration of data between online services. The new legal instruments, such as the mandatory reporting of the data

protection incidents is not only a task for the data controllers but for the Authority as well. For some particular risky data processing, the data controller must prepare a preliminary privacy impact assessment (PIA), in which the risks and risk-limitation need to be dealt with.

There is a higher level of cooperation between national data protection authorities and there will be more opportunities (sometimes compulsorily) for joint investigations. The new forum for the cooperation and dispute resolution is the Brussels-based European Data Protection Board.

The national data protection authorities may impose severe sanctions. When violating the rules, the data controllers may be fined for up to €10 million, or in certain circumstances, up to the two percent of their global sales. In other cases, such as illegal transfer of personal data to a third country, the penalty can go up to €20 million or up to 4 per cent of their global sales.

The additional obligation of data controllers is to present justified data processing in a transparent manner. The appointment of internal data protection officers are supported by the new data protection package.

II.3. New Data Protection Directive

The draft of the Directive on "protection of the individuals' personal data processed by authorities in crime prevention, law enforcement and correctional purposes and the free movement of such data" aims to promote the respect of principles of data protection and to ensure a faster and more efficient data sharing between EU law enforcement agencies.

The scope of the Directive broadly covers personal information held by all public bodies and non-governmental organizations, companies processing personal data for crime prevention, intelligence, law enforcement and correctional purposes, thus personal data processed on that score receives protection in any phase regardless of the controller's identity and status. In the case of transferring data to a third-country, the provisions of the Directive shall continue to apply even when the personal data has already left the territory of the European Union.

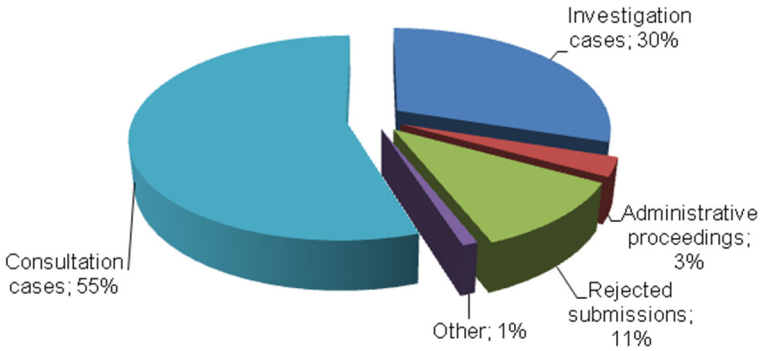
Innovation in the Directive is the distinction between the different categories of data subjects - ensuring greater protection of certain objects of data (witnesses, victims, etc.) – and the prohibition of creating profiles based on special data.

Within the obligations of data controllers “privacy by design”, “privacy by default” principles appear as basic principles, detailed regulations were made in subject of logging operations and it will be mandatory to make a preliminary impact study for cases which have a stronger impact on the private sector

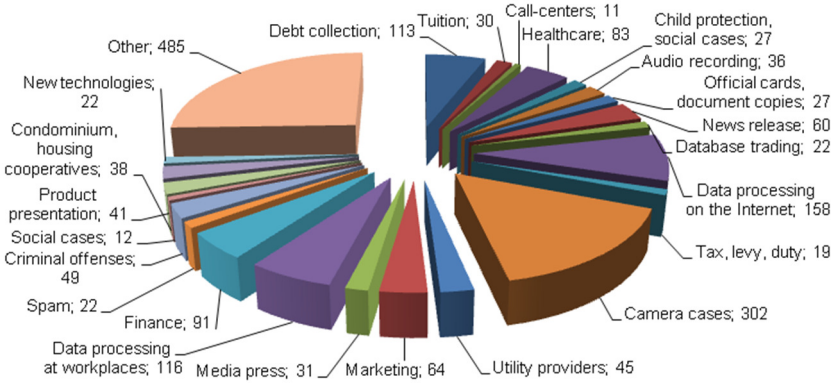
III. Data protection

III.1. Statistical data

In the middle of the year 2015, a transformation in the organization took place at the Authority. As a result of these changes the Data Protection Department's duties have increased significantly. The following diagram shows the types of cases of the Data Protection Department

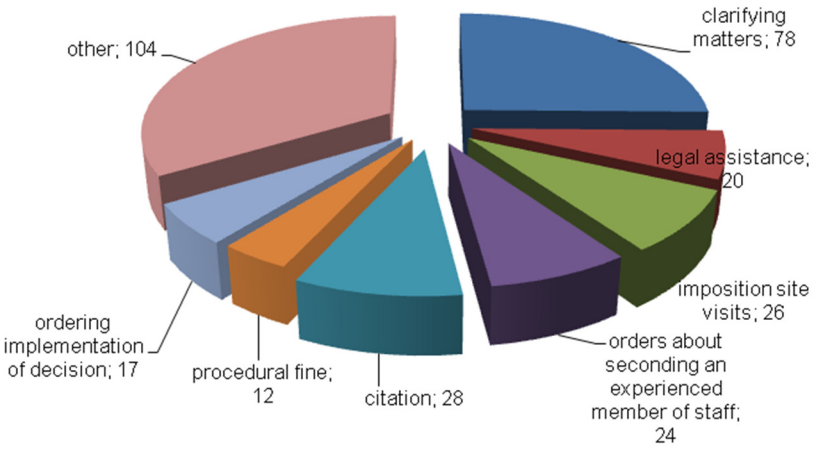


In the year 2015 the Authority had 1902 investigational cases. The area of expertise are presented on the diagram below. It can be said, that proceedings started because of handling personal data had been affected areas of both public administration and private sector as well. The Authority received large number of submissions, complaints, and letters requesting resolution from a wide scale of area of expertise.



In the year 2015, 30 administrative procedures have started, which is approximately equals to the number of administrative cases started in 2014. In 2015 the Authority (along with the postponed cases from 2014) closed a total of 22 procedures, 20 of which an infringement was found and imposed fines in 19 cases. The total amount of fine imposed in 2015 was 94 million HUF.

The expectations from the official procedure requires the Authority to deal with the cases within a reasonable time. During its official proceedings, the Authority makes more intermediate steps in the decision-making process, furthermore takes procedural actions. The purpose and reason of the wide range of procedural comportment is to properly examine the conclusion of facts, under which the Authority can make an informed decision.



The examined organization is able to start a judicial review against the Authority's decision. In the year 2015, 11 lawsuit was in progress which were postponed from the previous years and 1 lawsuit started in the same year.

Lawsuits

	2012	2013	2014	2015	Total
Official procedure	33	40	30	30	133
Judicial review	11	11	8	1	31
Pending lawsuit	0	2	6	1	9

Favorable result of the lawsuit	8	7	1	0	16
Partial favorable result	0	1	0	0	1
Failure of a lawsuit	3	1	1	0	5
All court decisions	**11**	**9**	**2**	**0**	**22**

In connection with litigations, the „Weltimmo affair" is a case worth to take a look at. The Weltimmo s.r.o. (Weltimmo) is a company registered in Slovakia which operates online real estate advertising surfaces. It processed personal information of advertisers and real estate ads. The company's data processing outside the formal Slovakian Deposit Company in all respects relating to Hungary was considered.

In the Authority's decision from 2012, the company was condemned and was required to pay privacy fine. The company called for a conducting review by the Budapest-Capital Administrative and Labor Court. The case was later submitted to the Hungarian Curia. The Curia, in case of the proper analyzation of the applicable law and jurisdiction issues initiated preliminary ruling procedure before the Court of Justice of the European Union, in order to comply with Directive 95/46/EC.

The preliminary ruling procedure has been completed on 1th October 2015. The Luxembourg Court ordered of determining the possible aspects of the company's establishment in relation to the applicable law and jurisdiction. The Court has set the actual location of the activity before the formal establishment and emphasized the protection of individuals' privacy as the primary value to be protected. Accordingly, the Court has ruled the Hungarian data protection provisions applicability, and of the Hungarian data protection authority's jurisdiction.
As a result of a preliminary ruling, the Curia ruled that NAIH has the jurisdiction in this matter and upheld the judgment of the Budapest-Capital Administrative and Labor Court.

The Authority has completed its second proceeding as required by the Budapest-Capital Administrative and Labor Court judgement. In the second proceeding, according to the court's guidelines, the Authority has revealed the facts in a greater detail and repeatedly condemned the data controller. Weltimmo has called for a judicial review again, which will take place in 2016.

III.2. Regulatory procedures

In year 2015, within the framework of data protection proceedings, the Authority gave attention to the following topics:

1. data processing of companies dealing with outstanding, debt processing and debt recovery
2. examination of the data processing of sales demonstrations
3. database-marketing.

III.2.1. Data processing by companies dealing with outstanding, debt management and debt recovery

In the framework of data protection, the inspection of the data processing of debt recovery companies' proceedings had begun in 2013. In 2014 the Authority issued a recommendation with a legislative proposal for companies dealing with outstanding, debt management and debt recovery. According to this legislative proposal, the prevalence of violations justifies the legislation and it is important that the law defines the conditions of handling of personal data during credit management processes and also the conditions of processing personal data of third parties who are not affected in the legal relation.

In the reflection to this legislative proposal, the Minister of Justice informed us that legislative constraints did not arise in the matter of debt collection activities and the recommendation issued by the Authority in connection with unlawful practices in data processing, these practices can be suppressed with consistent sanctioning of violations.

Respecting this ministerial decision, the Authority continued its investigation in the area of debt management.

In 2015 the number of public complaints, notifications which are object to the legality of the various asset management companies data controlling activity has not decreased, which has greatly contributed to the raise of privacy problems in the settlement of the exchange process of currency loans. A variety of companies, credit institutions as data controllers often perform their own debt collections. Occasionally they enter into an agency contract with asset management companies as well as selling their demands to factoring companies through cessions.

Four data protection authority proceedings started in 2013 were closed by court decisions in 2015. Each of the four claims were rejected by the Budapest-Capital Administrative and Labor Court.

In the litigation started in the review of the decrees the Budapest-Capital Administrative and Labor Court ruled the following:

- During the data protection proceedings, the Authority shall not examine if the examined data processing can be justified by the legal ground of considering interest, when the data controller has not established its data processing on this interest.
- The decisions of the Authority rightly pointed out that the examination of the solvency and financial position of the debtors, along with the collection of data associated to this is not the credit management's statutory duty.
- The plaintiffs clearly need to be aware of the small and medium-sized enterprises' quality and providing relevant data for the Authority and for the Court. (Moreover, the applicability of the Act on Small and medium-sized enterprises' within the Authority's work will be ruled by the Curia subsequently.)

The Authority's investigations revealed a widespread condemnable practice in the debt collection sector, according to which the principal and the agent agree over the debtors' heads that they debit recovery costs on the debtors with non-predetermined amount and terms, which will typically be a credit management revenue. However, in this case, the data's of the debtors are being used for other than the original purpose which is the recovery of their own revenue. This practice has no proper legal basis and the debtors are not informed as well.

Three data controllers turned to the Curia against the ruling. The judgment of the Curia on 27th October 2015 rejected the review request and upheld the judgement of the Budapest-Capital Administrative and Labor Court.

The Curia's standpoint is:

- the Court rightly cited that the judicial examination of the possibility of considering interest by the plaintiffs was unnecessary,
- it was right not to rate the – not sufficiently proven – presentation which cited the small and medium-sized enterprises legal status and legal consequences arising from this status,

– NAIH has sufficiently reviled the conclusion of facts and complied with the procedural rules, the considerations of the fines imposed were stated and the grounds of the decisions are reasonable.

In two cases the data controllers did not fully comply with the decisions thus the order of the execution took place. One factoring company's obligation to erase data has created the need for a new data protection authority proceeding, because the company had its receivables and the related data transferred to a new data controller before the judicial review of the decision about data cancellation.

Other aspects of the Authority's data protection proceedings in this matter (like the debtor's relatives data processing, decent data processing requirements, legal basis of data processing etc.) remained unchanged.

Compared to previous years, new types of violations had been experienced.

One of the investigated data controller has been providing loans for purchases of durable goods (products) or services. The Authority has found that under the period of the review various communication problems occurred and therefore the data processing conditions weren't transparent (contradictory, misleading) for customers. Correct interpretation of the Privacy Act reveals that data controller must provide the relevant information on the actual circumstances of the data handling. Thus, it is also illegal where the controller provides information on data processing which is not actually performed, as in this case, those affected may not be able to track the fate of their data properly. The company lodged a claim against the decree and the judicial review of the decision is still pending.

In another case, two data controllers are part of an international group of companies, both of them dealing with debt recovery (via assignment and delegation).
The Authority found that without any appropriate legal ground, sensitive data (data on the debtors' health and criminal record) was processed unlawful by both of the companies. If the companies are going to change their information management practices in the future in a way that there will be a reasonable target assigned to the data processing and will comply with legal requirements for literacy, it is theoretically conceivable that these plaintiffs can legally process sensitive data in the future. Nevertheless the theoretical possibility of this was unable to be taken into account.

During the examination of these companies NAIH has found that the data are deleted logically, but not physically. The logical deletion of data does not prevent

the achievement of the data, they are faintly but clearly legible on the surface of the database. With this deleting technique, Section 4 of Privacy Act about finality and the compliance with the principle of necessity cannot be met. According to Section 4 of the Privacy Act, only such personal data can be processed that is essential for the realization of the objective and appropriate to achieving the goal, but only to the extent and duration necessary to achieve that purpose.

With the logical data deletion technique, while making the „redundant data" paler, data processing is not resolved, the data remains visible, it exist in a recognizable form in the database, and data processing persists in spite of the logical deletion. The company argued that with this technique they can avoid the reuse of false number belonging to another person. However, this goal does not justify the processing of the data belonging to a third party, as there is no significant effect on the purpose of credit management, it does not fulfill the criterion of necessity. NAIH found that this is in contravention of Section 4 of Privacy Act and urged the data controllers to make sure that the data is unrecognizable by deleting inactive data. The companies have lodged a claim against the decree and the judicial review of the decision is still pending.

In a third case, the Authority investigated data processing in connection with debt collection, whether the factoring company's agent is a data controller or a data processor.

Based on publicly available company data, the Authority concluded that the principal (assignee) is the exclusive owner of the commissioned (assignor) company, which deals with the assignment of the claimed debt. The decision of the Authority ruled that because the principal's ownership structure – under Section 10(4) of the Privacy Act – the assignor cannot perform data processing activities legally. The companies have lodged a claim against the decree and the judicial review of the decision is still pending.

III.2.2. Sales demonstrations

Product sales with displaying the actual products, in the course of a sales demonstration are such activities where customers, given the nature of the transaction, need greater protection, also in terms of data protection. It brings up mostly consumer protection issues, as the main targets of these events are senior citizens who are more vulnerable and sensitive to products and services which could improve their health conditions. People are more willing to spend money and disclose their personal data with a view to improve or keep their health conditions

even more than they can afford. Frequently these sales activities using unfair methods, promising gifts and free health assessment for the participants which are actually non-medical services. This practice raises a number of privacy issues, both with the collection and treatment of these people's data, in relation to contacting and contracting.

Since 2014 the NAIH has given high priority to the examination of data processing activities relating to sales demonstrations and has sought to eliminate the unlawful practice in this field and to force data controllers to comply with law. In 2015 the Authority started 11 administrative proceedings which affected data processing in the scope of sales demonstrations and adopted 5 decisions.

In the 2014 Annual Report of NAIH has dealt with the data processing in the scope of sales demonstrations in detail. Here we focus on cases we experienced in 2015.

In the framework of the proceedings, the Authority performs site visits and questions witnesses as well. However, the facts which have occurred in these cases require an extremely difficult and lengthy, often „detective work", as the companies concerned are not cooperative, or trying to „hide" themselves from the authorities. These moves are caught in relocating their headquarters via different agencies or using such offices where they do not take formal letters or any kind of post, and they also try to conceal their „events" from the authorities. Also, typically they no longer operate under the same work but 1-2 years, they sell or liquidated companies (and, of course, continue to pursue the activity under a different company name), thus trying to evade liability. There was a case where the sales demonstrator company's headquarters was registered at an abandoned house in a village and the managing director was a homeless person. In another case the manager was a completely inaccessible foreign national and the delivery agent was a person who has never heard of the manager before.

The site visits were impeded in many cases, malicious server downtime or unintended power outage occurred. Some companies tried to influence the effectiveness of the official investigation by changing the database between inspections. When these actions were proven by a forensic expert, the Authority imposed a fine in the procedure. The appealed decision was dismissed by the Court. In several cases the cited person did not appear, and the absence was not excused in any way. In these cases, procedural fine was imposed. Overall, we can say that without exception each of these procedures have stretches for months, and it is difficult to establish the facts required for the decision.

These businesses using unfair methods against the concerned parties and authorities. It is not uncommon that companies are trying to present their activities to give them a health scientific character with misleading methods. Some company put the logo of the Hungarian Society of Internal Medicine on its leaflets illegitimately or collected data in terms of the so-called „Elixor Research and Development Program". Health data was collected on health status questionnaires According to the Privacy Act, data on health status should be treated within stricter conditions. When the purpose of the event is product sales only, collecting sensitive data is not acceptable. In these procedures, unlawful treatment of medical data was an aggravating circumstance when determining the penalty. The Authority has ordered the deletion of sensitive data.

The main violations related to sales demonstrations are:

- the companies are usually obtaining the invited person's name, phone number, address from illegitimate sources,
- they provide false information to the guests, participants, customers, especially with regard to the purpose of providing "screening tests" and "health-days",
- unlike the contract they record and store too many personal data,
- their operation is contrary to the requirement of fairness for data processing, they focus on profit instead of respecting the participant's exercise of right of self-determination.

Each of the decrees state that these companies do not provide information on the relating Sections of the Privacy Act for their clients, which is the ground of the invalid data processing contribution.

In March 2015 the Authority issued a report about the privacy requirements for product presentations, giving the results of official procedures and telling about the empiric results of the consultation held in January 2015 with the partner authorities. In the report, the Authority divided its suggestions into subgroups:

- The first called for enterprises doing this type of activity on what requirements need to be met when processing data, and bullet pointing out the procedures needed to be followed for legitimate data processing.
- Secondly, it made proposals for individuals who are interested in these sales demonstrations to help recognize when a company is operating with unfair methods and gave advice on how to be more cautious due process.

– Thirdly it has outlined the changes of the legal aspects.

The legislator has also recognized the untenable situation and amended some legislations regarding this topic. Out of the Authorities recommendations, dependent broking and borrowing rules had been restricted with amending the Act CCXXXVII of 2013 on Credit Institutions and Financial Companies. It has been prohibited to provide financial service combined with sales demonstrations. Aggravating the obligation to provide information was realized by amending the Act CLXIV of 2005 on Commerce. It created a mandatory requirement on establishing customer service by these companies, so clients are able to self-determinate on data processing.

These changes provide the involved a greater safety against dishonest traders, and the sales demonstration abuses can be effectively suppressed from data protection point of view as well.

III.2.3. Data processing for marketing purposes

In 2015 the NAIH examined again direct marketing-related data processing in the context of procedures. Direct marketing (DM) operations seek to set up direct connections to individuals with the purpose of marketing communication. This requires some personal data from the data subject which can be obtained by the advertiser only on the consent of the data subject. These companies typically offer direct marketing services for other businesses, such as e-mail marketing (eDM), telemarketing (call centers), mobile marketing (SMS, MMS) and creating database. In Hungary advertisers need to acquire a consent (opt-in) in order for him/her to send DM messages. Opt-in consent is a technical jargon and means that the advertiser has to attain the informed, explicit and prior consent fro the target person the latter stating that s/he wishes to receive marketing messages in the future whereas opt-out indicates the objection of the data subject to receiving the said messages.

Today, getting line on purchases and certain products, services is being realized most of the times on the internet. It is vital for companies to pass on their information, discounts to more and more buyers or to prospective customers. Newsletter, regular advertising are being sent out to applicants found in their database which generates a continued attendance on their websites, which is important to help reach advertisements placed on these sites and generate a higher purchase ratio. Maintaining the database and a continued expansion can greatly contribute to the steady development of these enterprises. However, it is crucial that during this activity, the personal data procession is justified.

III.2.3.1. Typical methods of setting up databases

Businesses have several possibilities on how to build their database in a legal way, for example:

1. *Collecting data on their own website:* by creating registry and providing newsletter signups enables the company to collect personal data. *eDM*: by assigning a business processing a database that is available for sending newsletters to send out the companies advertisement. In the course of eDM companies send newsletters to designated addressees sorted out from the database. This ad usually contains a link which will redirect the user to the company's website, where he/she can register, thereby setting up the advertising company's own database;
2. *Data collection:* assigning a company which practices in building databases. Typically, this is the form of a giveaway, in where the participating natural persons agree that their registered data can be forwarded to other companies and also for the principal undertaking.
3. *Telemarketing*: i.e. call centers are used for sale and setting up database. According to Section 160-161 of the Act C of 2003 on Electronic Communications (hereinafter referred to as: Eht.) and Sections 22-24 of 6/2011. (X. 6.) of the National Media and Telecommunication Authority Regulation service providers shall maintain subscriber lists for keeping data that is necessary for the identification of the subscriber and for the services used and that can be processed by the service provider under authorization by this Act or specific other legislation. In doing so, those subscribers who are registered in the subscriber directory – created under the Eht. – can be called for direct marketing purposes and have not made a prohibition statement, or delegating a company to perform call center operations which has a database available on the basis of relevant consent (natural persons in the database can be contacted through their phone numbers for direct marketing purposes), so the delegated company can call up these persons and recommend the principal's products/services and request personal data for the company.

III.2.3.2. Experiences concerning administrative procedures:

In 2015 NAIH adopted four decisions which evaluated data processing activities of companies providing DM (direct marketing) services.

The investigated companies have launched giveaways on their websites to set up their huge databases. The scope of the processed data in these databases

extended to basic data such as name, email address, phone number, postal address, date of birth and in some cases with continuous profiling, additional data such as marital status, number of person in the household, car, insurance, occupation, etc. This database then was used for e-mail marketing, telemarketing and assigned setup of database.

The database setup, the problems, mistakes, unlawful data processing practices and the related "best practices" can be summarized as follows:

1. When data is being collected on the own website, the data controller is obliged to provide detailed and easy-to-follow information. The manual needs to be accessible during the registration, too.
2. The most justifiable practice for setting up database was the eDM, because due to the nature of the service, special data are kept entirely under the control of the data controller, typically in this area we found no infringement either.
3. Those companies who set up databases and become data controllers through the transfer of the data typically do not pay attention to receive the proper consent of the data subjects. NAIH considers that in such cases, voluntary contributions are applicable if the person concerned has also the possibility to choose (checkboxes, ticking), which third party should receive his /her personal data. This way people can really decide, from which company he/she would like to receive inquiries in the future.
4. Serious infringements were revealed in relation with a telemarketing activity, notably when setting up database with the assistance of a call center. The often so-called "data rental" service is a triple cooperation between the data controller, the company who sets up database and the call center. According to the practices of direct marketing companies, the data was passed to the call center as the data processor for telemarketing purposes, for a specific period or one-time phone call. If the call center managed to arouse the interest of the called party during the telephone call, the call centers principal was hereinafter processing the data as its own database. According to NAIH, this solution does not comply with the data controller and data processor concept laid down in the Privacy Act, nor for the Sections regulating the data processor's activity. The call center making the telemarketing calls ignores the original data controller's instructions, but in the order and on behalf of whom the products and services need to be promoted and sold, so these companies, using the concept of data process made data available for third parties with no legal basis.

NAIH also investigated a practice where a marketing company without its own database provided data transfer upon customer demand without target groups and quantitative needs. The so called “mediatory-data brokerage” service – collecting the necessary data with its own database marketing firm – such as the right to use their own database of the transferred data which is provided for the contractual partner – from its standpoint as data processor.

In this construction neither of the parties are actual data processors, the transfer of personal data based on temporary nature does not exclude the Privacy Act from the application, the contractors are not related as data controller and data processor, but because of transferring data, they are considered as data controllers.

Furthermore NAIH considers that the “mediatory-data brokerage” activity does not meet the provisions of the Privacy Act because the adequate contribution of the involved cannot be presumed.

Another company, who is unknown even by the original controller of the database cannot control the data because the persons concerned have not contributed to this data processing and to get in touch with this company for receiving deals and offer for services.

NAIH has examined whether the above detailed “temporary data processing schemes” can be carried out lawfully and came to the conclusion that contracts for “hiring data” are contrary to the principles and requirements of the Privacy Act.

5. Purchasing database is also a possibility for gathering personal contact data. The legality of these purchases was also examined by the NAIH in one of the official procedures.

   If the controller as seller passes the database containing personal data to the buyer as a new controller, it is considered as transfer of data. To do so, the seller must have proper legal basis. In this case, the applicability of a new legal ground came up, Section 6 (5) point f) of Privacy Act. In addition, the controllers may also use Section 7 point f) as legal ground.

Whichever of the above legal basis the controller choses, the controller needs to apply the “balance of interest”. This test is a three-step process in which the data controller’s legitimate interest needs to be identified, as well as the interests of the subject of the data, the fundamental right in question as the weighting counterpoint, finally as a result of the weighting, it needs to be determined whether any personal data can be processed.

The test results and the essential conditions of the contract should be reported to the persons concerned in a comprehensible and clear manner. It shall also ensure efficient and unconditional objection against the transfer of the data. It is also important that the customer data controller can only process data according to the seller's hand-out. Any kind of modification of data processing (except for the choice of a new data processor) must be regarded as a new data processing for which the new data controller must acquire new approval.

III. 3. Investigation procedures

There are two common areas of investigation procedures: surveillance camera systems, operation of security cameras and data processing at workplaces. NAIH receives large numbers of complaints and consultation submissions on these two matters.

III.3.1. Camera cases

III.3.1.1. Observation of private property

In connection with observation of neighboring private property via using camera surveillance, the informational self-determination is only marginally compromised. Examining and deciding the legality of the surveillance is primarily available through the means of protection of possession, or within the framework of personal rights lawsuit.

In the above mentioned case, NAIH considers starting action in rem at the notary of the competent local government, because for notaries all the legal means are available by which they can restore the legal conditions.

In addition, monitoring the private sector unduly and disproportionately raises the possibility of bringing an action before the court because the violation of right to privacy.

III.3.1.2. Street cameras

1. At one part of the submitted consultations, NAIH received numerous questions from data controllers who wished to operate street surveillance camera systems.

2. The complaints focused on concerns about cameras installed by individuals and operated normally on private property, but held public areas under surveillance.
   According to these submissions, a widespread bad practice is followed by both individuals and companies, who are installing cameras because of security purposes on their own property, but are recording footage of public places as well.
   NAIH takes the view that cameras operated by private individuals can only monitor the area in their property, the viewing angle cannot be focused on public places or on another private property. Residents and other individuals' private sector who are passing by in public areas cannot be violated. At the entrance needs to be a clear call to indicate the entrants that cameras were installed for surveillance purposes.
   In Hungary, the viewing angle of the camera cannot be oriented to public places, since the observation of these places is possible through the express authorization by the law. So if a camera - based on its location and viewing angle - suited to observe public areas, this activity constitutes unlawful data processing, given the fact that the activity infringes the surveilled induvial right to privacy.
3. NAIH conducted investigations in several cases and pointed out that the investigated data controllers set up and operated the surveillance systems in public places illegally and also found shortcomings in informing the individuals concerned.
   The data controllers concerned adopted the findings of NAIH in all cases and remedied the shortcomings, and measures have been taken to ensure the legitimate operation of the established surveillance system.

III.3.2. Data processing at workplaces

In the year 2015 NAIH received a significant number of submissions concerning the world of labor. One part of them were consultative submissions, another part of them were complaints, both relating to the control of employees. Act I. of 2012 on the Labor Code (hereinafter referred to as Mt.) provisions allow employers to control the employees by technical means, which raises a number of privacy issues. Unfortunately, NAIH finds that a broad interpretation of the legislation by employers often constitutes serious violations of privacy rights.

It can be said that the majority of submissions tare made up of consultation. It seems to be the obvious reason that the employee and the employer has an under-hierarchical relationship and employees often do not dare to complain against

their job, although the Privacy Act upon request provides a guarantee to remain anonymous for the complainant during the NAIH investigation.

The cases concerning the monitoring of the employees' electronic communications, e-mail and Internet usage is significant. Increasing numbers of submissions were received concerning the monitoring of GPS systems used in motor vehicles and the using of cell information of mobile phones used by employees. The number of submissions regarding the monitoring of workers with cameras were also significant as experienced in the previous years.

NAIH's recommendation on the essential requirements of using electronic monitoring systems in workplaces also covers every technical devices which are used to inspect employees.

At the workplace, the employee does not lose his right to privacy, but this right is not an absolute right either. The employer's legitimate interests are connected to the legal processing of the employee's personal data in the scope of the employment. The data processing linked to the employer's scrutiny stemming from the Mt. and from the nature of the employment relationship is an instrument of safeguarding interests of the employer. During the duration of the employment relationship, for the proper functioning of the economic activity of the employer, workers right to privacy can be, in certain cases, with well-defined circumstances restricted while also maintaining assurance requirements. Its tools, methods cannot breach the dignity of the human being, private life of the employee cannot be monitored. On the other hand, the employer must comply with the principles of a fair and assigned data processing.

Using the monitoring technical devices mentioned in the Mt. can only be legitimate if the use of these devices is a proven and legitimate interests of the employer and goes with a proportional restriction of rights. It needs particular attention that the extension of the control is only as wide as the employees were informed by the employer previously. Also the control is only legitimate if the employer has defined detailed regulation.

Therefore the employer must notify employees in writing according to the conditions set out in Section 20 (2) of Privacy Act. If the mail system, Internet access and mobile phone cannot be used for private purposes, the information needs put special attention to this factor. Employees should be informed about the detailed rules of the inspection, especially its progress, steps and about who is entitled to

carry out an inspection and when and how employees may request information in relation to the technical instruments.

NAIH supports proactive attitude from employees, in order to ensure clear aspects of follow-up employer-employee rights and responsibilities and to avoid possible litigation. Each data processing at workplaces, NAIH developed the following compatible, good regulatory practices as „Best Practices".

III.3.2.1 Monitoring electronic communications

In the field of electronic communication control the received submissions are typically about cases when the employer hasn't provided the manual on how to use the workplace email account, and under or after the contract of the employment, it wishes to check up on the contents of the emails sent out by the employee, for example if any offense incurred.

NAIH's current practice of checking emails should only be used when it is absolutely necessary and there is no other possible way or traditional control method that digs less into privacy. Mail checks should be the last resort when other employers control is not available. Checking emails should always take place in order to meet a legitimate aim, such as for example, to obtain evidence. Checking emails without purpose is contrary to the legal requirements in force.

If the email system operated by the relevant body or organization cannot be used for private purposes, the right quality and highly detailed prior written prospectus should be drawn to the attention of the workers separately. When checking emails is inevitable, employers need to analyze the traffic data first, secondly checking emails sent in the specified time period, and the last resort is to check the actual content of the emails. Email checking may involve the processing of personal data of third parties outside the scope of the employment relationship, so proceed with extreme caution. It is important to point out that employers cannot be acquainted with the content of private messages even within the pursuit of the employer's rights.

III.3.2.2. Controlling the usage of the Internet

Instead of the inspection it is clearer and more relevant, if the employer determines in advance which sites are going to be blocked and sets a filter. It also makes sense to limit the visitable sites to those which are useful for the work. If,

due to the nature of work the restriction is not feasible, the opened page listing can be monitored only if the employer has informed the employee about the inspection or the possibility of the inspection in advance. NAIH believes that the appropriate regulatory practice for the control of Internet usage is to define explicitly and in detail how to use the Internet access for private purposes.

III.3.2.3. Inspection of mobile phone usage

For the sake of controlling the usage of the company's mobile phones, the employer also needs to indicate beforehand, what are the detailed rules for the use of company cell phones. The employer has its own discretion, for which purposes can be the companies mobile phones used for. The employer, however, has the legitimate right to demand control of the use of company mobile phones - in particular, that normally the employer pays the mobile phone bills -, this is possible if it has made provisions prior inspection. Based on the provisions of the Mt., the employer is entitled to inspect the usage and cost of the company cell phones made available for the work. NAIH's adopted practice when accounting additional phone costs is to ask for call details in an obscured format at the mobile service company, in which the phone numbers or the last digits of the numbers are in an obscured form.

III.3.2.4. Using GPS tracking

The data forwarded by vehicle-mounted GPS tracker is considered as personal data of the people found in the vehicle.

The data generated by the GPS also contains data not related to the employment which may be an infringement of the privacy rights of employees. As data controller, the employer shall consider whether checking the exact location of the employee is demonstrably necessary. NAIH recommends using the GPS application for logistical purposes, it needs to serve determining the position of the vehicle, rather than to follow the employee.

III.4. Recommendations on data protection

In 2015, NAIH issued four recommendations on data protection, which we describe below.

III.4.1. Recommendation on data protection requirements regarding prior notice

NAIH receives complaints mostly regarding the lack of prior notice on personal data processing of citizens. Prior notice on data processing has great importance on exercising their informational self-determination self-consciously. Prior notice on data processing gives people the chance to be aware of the possible intervention in their privacy and helps them to give the appropriate approval for processing their data. The importance of prior notice regarding the protection of fundamental rights emphasizes the fact that contribution to the processing of personal information can only be considered legitimate if it is based on appropriate information.

With issuing recommendations, NAIH would like to assist to the legitimate practice of data controllers:

a) The most important quality requirement for the prior notice is to be clear, readable and perspicuous. Avoid the use of jargon or drafting multiple and complex sentences. It cannot be accepted either when the data controller repeats the wording of the relevant legislation merely literally or only defines the concepts. NAIH's recommends summarizing the guide in tables or in a questions and answers form.
b) The data controller needs to provide the possibility that the information be continuously accessible and viewable. The information needs to be made available on the opening website. If the data controller would like to place the information in the general terms and conditions, it needs to be done well separated.
c) According to Section 20 (2) of the Privacy Act on prior notice, the name of the data controller and an indication on the purpose and legal basis of data processing is primary. Based on these requirements, it is emphasized that the data processing with general purpose is inadequate.
d) When data processing is based on consent, the guidance underlying the contribution needs to emphasize its voluntary nature. In the case of compulsory data processing, it should refer briefly on the specificity of this plea, namely that the data processing is undertaken regardless of the consent of the concerned, as the data processing is determined by law. In this case, the guidance needs to refer on the data processing conditions as well.
e) The guidance needs to define the range of the processed data sharp. For more complex data processing, information on the scope of the processed data is also crucial. Only this way will the person concerned be

able to measure how the data processing will effect on its privacy and can determine how he/she would like to approve data processing.

f) The guidance needs to particularize who and in what extent has access to the data. In this context, it is also necessary to mention the kind of data processing operations that individuals and organizations are practising.

g) NAIH considers important the fulfilment of Section 6 (5) of Privacy Act on guidance on data processing. Data controllers need to inform the concerned persons in a separate section (title, chapter, section), also separated from other conditions on the data processing based on Section 6. Based on this, it is expected from the data controller to explain understandable and in a clear manner why its legal interest in data processing outweighs the concerned person's interests and rights.

h) In the context of data processing, the information provided on the data subjects' rights shall include how requests can be submitted (in particular the contact address)and the time in which the request shall be replied since the data subject have the right to object to the data processing at the data controller on the first place. s III.4.2. Recommendation on data processing in regard of school class meetings.

III.4.2. Recommendation on how to get contact details of former students for organizing class meetings

In many cases it is a recurring issue how contact details of former students may be requested legally from former schools.

Referring to the fact that the law does not empower the educational institution for providing former students' contact details when organizing class meetings, the approval of each person for the data processing is needed. However, obtaining the prior consent of the data subject is not possible either. The data protection provisions are intended to protect people's privacy, but in the meantime shall not lead to unrealistic life situations.

The fact, that the data processing cannot be based on the law nor the contribution of the concerned, a new plea should be examined. In this particular case, the applicability of Section 6 (1) of Privacy Act should be considered.

Before providing the data, the educational institution needs to make sure that the party requesting the personal data actually is a former student him/herself and he/she is requesting the details of the class which he/she was once part of.

The institution may require evidence from the individual to prove the foregoing. The applicability of Section 6 (1) also depends on whether the data controller's or third parties' legitimate interest and the restriction of the individual's privacy is proportionate to each other.

Upon the evaluation of all circumstances, NAIH recommends that data processing related to class reunion is considered to be special, but Section 6 (1) of Privacy Act is still applicable.

Educational institutions shall release the former students' contact information for class reunion purposes. The organizer can only be a person who was in that class or was a former student in the same year, and this fact must be checked prior to data transfer. Based on Section 15 (2), institutions shall keep records of data transmission for proper instruction of former students. NAIH points out that the existence of legal basis is not yet sufficient for the lawful processing of the data, additional warranty requirements need to be met as ensuring the exercise of the concerned parties' rights and the enforcement of assigned data processing.

III.4.3. Recommendation on the faith of personal data after death

The recommendation would like to draw attention of companies providing Internet services and processing confidential data, which data processing is based on the concerned people's prior consent. These services are typically the Internet social networks, content providers, communication services (chat, forum, email) and online gaming.

Currently the Privacy Act has no provision on the processing personal data relating to a deceased person, if their treatment is not required by law, but on the consent of the person, if it would be still alive (such as providing data when registering on a social networking site).

Personal data is related to the natural living person, however, the obligation to protect this data after the person's death does not cease completely, and handling the deceased's data or its disclosure can affect the descendants' privacy as well.

The Privacy Act does not currently authorize the relatives to control personal data associated with the deceased person (such as deletion of the processed data, rectification etc.). The Section of the Civil Code relating to the right of rev-

erence creates the legal basis, that if any infringement of the memory of the deceased occurs, the relatives or testamentary allowance recipients for contacting the court.

The infringement of the memory of the deceased needs to be examined in the light of personal rights while he/she was still alive.

The Civil Code also mentions the protection of personal data, as well as the portrayal and the sound recording rights. The framework of right to personal data protection set out by the Civic Code is filled with provisions of the Privacy Act, so this type of data processing creates the right for relatives to turn to the court due to defamation of the deceased person.

The above mentioned possibility only complies with the situation, when the memory of the deceased was violated through data processing. Therefore NAIH considers that the social purpose of personal rights and protection of personal data would not be compatible with a provision that would extend the deceased rights – which are provided by the Privacy Act – on the relatives and successors.

With regard to the deceased person's personal information processed by online services via user accounts, the possibility of deletion these data has currently no statutory legal basis. This is only possible for relatives if the service provider provides an opportunity for the deletion under the conditions of use. The basis for this is the contractual relationship between the user and the service provider. In this view, NAIH drew attention that the established contract between the user and the service provider is typically terminated after the person's death. With the termination of the contract, the purpose of the processing of personal data is also eliminated therefore in principle, the data related to the deceased person should be deleted.

NAIH considers that it may be necessary in the future to create a new plea based on the law that regulates data procession based on consent related to the deceased person, which allows the deletion and termination of such data by relatives and successors. This may be necessary because the service provider typically cannot verify that by the death of the concerned person, the purpose of the processed data has ceased. This right, however, should not include the right to access to the deceased person's user profile and stored privacy (such as private correspondence).

Ideally, this right should be exercised only by the relatives and successors of the deceased by proving their family membership, and by properly identifying the data provided by the deceased person and the data provided by the relatives.

The requests to delete personal data should only affect the data which the deceased has provided in relation to the service, but non offensive data created by third party in connection with the deceased cannot be affected.

Having regard to the recommendation, NAIH called on the Minister of Justice for the possibility of creating a legal basis and procedures which endow the deceased's relatives and successors with the above-formulated rights.

III.4.4. Recommendation on costs incurred for the release of medical records

A number of submissions were received by NAIH for a recurring issue in relation to the issuance of health records generated by health care providers. These submissions asking about the possible amount of costs when copying these records.

Legislation does not regulate what amount of cost health care providers should charge, if the patient or other authorized person requests the release of medical records.

NAIH found that the health care institutions such as health care providers determine the copying costs of medical records in their internal rules which is not standardized, given the lack of regulation, and the defined costs are sometimes high. The reason is that there is no regulation that would determine the exact charges incurred in connection with copying such records.

NAIH considers that in connection with legal certainty, it is not an appropriate practice, where healthcare providers practicing different conditions when issuing medical records, so NAIH put forward the following recommendation:

NAIH recommends for the legislator the creation of a legislation about costs relating to the copying costs of medical records, fees, under which health care providers can develop a uniform tariff.

It must be considered, what kind of fee policy is being created, what amount of material costs, wages, energy costs are charged in such a way that the healthcare providers do not charge for additional funds.

NAIH recommends that raw material costs, technical costs and the costs of work should be charged, but other chargers - such as archival lookup fee, management fee – shouldn't be charged at all. In the opinion of NAIH, costs such as the administrator's fee, the consumed energy should not be included. The purpose of achieving profit while copying these records is not acceptable either.

While waiting for the legislation to be created, health institutions are encouraged to make create their policy on record copying in accordance with this recommendation.

IV. Data protection Audit and BCR's

IV.1. The experience of data protection audits in the field of public sector's data processing

There were more audits conducted in the public sector in 2015, the most interesting requests for audits came from

- the Prime Minister's Office in connection with the legal compliance of data processing within the social dialogue in the context of future Hungarian internet
- the Office of the President of the Republic in connection with the signature collection and newsletter service data processing on the Office's website (www.elobolygonk.hu)

The special feature of these requests was that the preliminary concepts were already submitted for justifying data privacy compliance before the actual data processing started. NAIH welcomed the initiatives since it significantly increases the efficiency of the data protection audit if the audit is carried out in a phase where data processing circumstances can still be changed significantly.

Another advantage of an early phase audit is that the information provided to the data subjects can be properly evaluated so there will be no need to change later. In this way, NAIH could also determine the minimum elements of the data process contract.

Summarizing the above, NAIH concluded that a significant increase in awareness of privacy and data protection mechanisms is noticeable, if the privacy risks are assessed during the planning phase of data processing. Accordingly, NAIH considers the above mentioned procedure to be followed, and also believes that the new concepts for data processing in the public sector (for example, within the framework of the European Union tenders) are worth for ex-ante evaluation within the framework of data protection audits.

IV.2. The experience of data protection audits while auditing the non-public sector's data processing

In 2015 there were several data controllers initiating audit services in the private sector again. As data processing carried out by the companies showed a very different specificity, therefore NAIH provides information preferably on the most common risks experienced during data protection audits.

On the one hand, NAIH examined whether the reported data processing operation meets the requirements of necessity and proportionality. While processing data under this criterion, controllers should be subject to the following aspects:

- whether the use of the system is essential to the aim of data processing, or it is merely a convenient and cost-effective way for it;
- while system l operate effectively in order to achieve a specific goal (efficiency);
- whether the limitation of privacy resulting from the operation of the system is proportionate to the potential benefit (proportionality), if the benefit is relatively small, such as increasing the comfort of the operation of the system or result in only minimal cost savings, is it proportionate to the potential benefit (mostly not);
- whether the target can be achieved by less restrictive means of privacy (lack of suitable alternatives). If some alternative measures would be equally effective to the objective pursued, the system operator is obliged to choose among the alternatives.

According to NAIH's experience, data controllers applying for audits do not measure the principles of necessity and proportionality. Consequently, certain circumstances of the data processing (for example, the range of the processed data and data processing operations performed on the data) are not in line with this requirement.

In accordance with the requirements of necessity and proportionality, NAIH concluded that in several case the principles are only partially fulfilled by the controllers. They also often treat the same range of personal data separately and evaluate separately what data processing goals they have. NAIH considers that this approach does not allow controllers to measure whether they meet the principle of assigned data processing or not, being aware of only processing such data which is capable of reaching the goal. NAIH has the following key experience during data protection audits: it significantly increases the level of data protection,

if the personal data is consciously assigned to the goal of the data procession separately.

NAIH also specified what kind of requirements data controllers need to comply with during prior notification of the concerned persons. The audit process is also based on NAIH's recommendation issued on 9 October 2015 (on privacy requirements of prior notification), however it also paid attention to the peculiarity of the data processing. NAIH experienced that the data procession notifications were only partially compliant with the recommendation, clarity and readability was an issue.

NAIH takes the view that the controllers are primarily focused on ensuring that the data processor contracts comply with Civil Code provisions. As a result, the data processing contracts were deficient from data protection point of view because they were not organized properly, for example what personal data does the data processing exactly cover, what obligations does the data processor have in the case of exercising rights by the concerned, or the manner in which the controller inspects the data processor.

IV.3. Binding Corporate Rules (BCR)

According to Section 8 (1) b) of Privacy Act, in the case of processing data to a data controller established in a third country, an adequate level of protection of personal data is ensured when the data processing is realized according to bind- ing corporate rules (hereinafter referred to as: BCR).

The definition of BCR is found in Section 3 (25) of the Privacy Act: *'binding corporate rules' shall mean internal data protection rules adopted by a data controller or a group of data controllers operating in multiple countries, at least in one EEA Member State, and approved by the National Authority for Data Protection and Freedom of Information (hereinafter referred to as NAIH) binding upon the data controller or group of data controllers that, in case of a data transfer to third countries, ensures the protection of these data by unilateral commitment of the respective controller or group of controllers.*

BCR allows transferring personal data by a multinational company located in EEA Member State to another member of the group located in a third country in such a way, that the transfer of personal data complies with the Directive 95/46/EC on the

protection of individuals with regard to the processing of personal data and on the
free movement of such data (hereinafter referred to as: Data Protection Directive).

Groups of companies wishing to use BCR need to demonstrate during the approval process that the created BCR ensures an adequate level of protection of personal data within the entire corporate group, and that the BCR is binding and enforceable in all group members regardless of their location, and also for the employees.

It results from the definition found in the Privacy Act that if a Hungary-based company as data controller wishes to ensure the adequate level of protection of personal data, it must submit an application for the approval of BCR to NAIH. NAIH's approval procedure is regulated in Section 64/A-64/C of the Privacy Act.

The legal background of the BCR is created by Article 26 (2) of the Data Protection Directive, EEA Member States adopted their national legislation in the light of the above. The Data Protection Working Party, created according to Article 29 of the Data Protection Directive (Article 29 Working Party) elaborated several working documents to assure that national data protection authorities evaluate BCR's on the same criteria.

In order to inform data controllers properly, NAIH created its standard application form based on the Privacy Act and the above mentioned documents of the Article 29 Working Party, which has been published on NAIH's website along with the conditions for approval.

NAIH's procedure has two types depending on whether it participates in the cooperation procedure as lead authority or not. In the first case, if according to the criteria's found in the WP 107 document, the data processor appoints NAIH as the leading authority, NAIH has to carry out the cooperation procedure with other authorities of the Member States. If another authority from different Member State has been appointed as lead authority, NAIH takes part in the cooperation procedure, and first receives the BCR documentation when the lead authority forwards draft BCR for comments. In this case, NAIH's formal procedure regulated in the Privacy Act will start when the lead authority confirms to the data processor that the text of the BCR was found adequate according to the 29th Working Party documents. This is when national approval procedures can be initiated.

Given that the BCR has been used in the majority of Member States a long time

ago, NAIH has created a third, simplified procedure type.
This applies in cases where the data processor submits an application for approval of a BCR which was approved at EU level prior to the entry in force of Privacy Act's relevant amendment on 1st October 2015. This claim must be proven by the data processor with the copy of the approval decision issued by the lead authority. In these types of procedures, NAIH does not require further substantive amendments, since in a jointly established cooperation procedure, national authorities already considered the BCR as providing adequate safeguards.

With regard to BCR approval procedure - in addition to the Privacy Act and the 29th Working Group documents -, the 20/2015 (VII. 31.) Regulation by the Minister of Justice on administrative services fees payed for the mandatory approval of the organizational regulations should also be applied, which determines the administrative service fee of the approval procedure. According to this regulation, the fee must be paid before the submission which needs to be justified on the relevant section of NAIH's application form.

The application shall be accompanied by the BCR's text in English and Hungarian language, the WP 133 standard application form in English language, and if available, the information verifying the prior of another Member State's data protection authority.

As a result of the procedure, in accordance with Section 64/C (1) of the Privacy Act, NAIH shall pass a decision on the approval of the BCR, and in order to facilitate the information of affected data subjects, publishes the data controller's, applying the BCR, on the Authority's website.

V. Freedom of information

Freedom of information (FOI) also had a special significance in 2015, NAIH continued its previously established practice and also faced new challenges. We once again call attention to the appellation "Privacy Act", as this is the term we use to refer on Act CXII of 2011 on the Right of Informational Self-Determination and on *Freedom of Information*.

The classic caseloads were the obligations related to state/municipally-owned companies' freedom of information; including the disclosure requirement of the Hungarian National Trading House Plc.[1] and the legal entities established by the National Bank of Hungary.

A number of enquiries were submitted because refusal of data requests in connection with studies ordered by national public bodies, which have been financed by public funds.[2]

Good progress was made concerning the costs of freedom of information requests, as the Ministry of National Economy, Tax Affairs State Secretariat in its resolution stated that since the completion of the freedom of information request constitutes a "public authority activity" on the basis of the VAT law, fees charged because of requests should be considered exceptional.

V.1. Publicity/online disclosure of the declarations of assets

From time to time, the publicity of the asset declaration of elected officials always gets into focus while investigating the two fundamental rights. In 2015 NAIH had to deal with the publicity of asset declarations in a totally new context, also with the balancing test between the protection of personal data and the FOI. Many municipalities wanted to decree the online publishing of asset declaration of the representatives, the major, the leaders of at least majority municipality-owned companies and all other local public bodies on their websites.

1 naih.hu/files/Infoszab_jelentes_NAIH-2015-4833-4-V.pdf
2 See for example the investigation of the Hungarian Olympic Committee naih.hu/files/Infoszab_allasfoglalas_NAIH-2015-4338-V.pdf

The public bodies subject to disclosure requirement have the possibility to publish on their website or in the central electronic register (www.kozadat.hu) other date of public interest than the standard disclosure list describes in Annex No. 1.

NAIH gave supporting opinions on requests regarding regulations based on Section 37. (3) of the Privacy Act on ad hoc disclosure list, and welcomed the publishing of contracts on their website, that haven't reached the worth of 5 million Forints described in the standard disclosure list.

However, the commitment to transparency sometimes could be limited by the protection of personal data. NAIH could not contribute to the acceptance of those initiatives where the municipality's representative body wanted to decree the online disclosure of asset declarations on the basis of "free" consent of the data subjects against the Privacy Act's relatively new rules. The Section 26. (2) got a new supplement regulation on purpose limited dissemination of personal data of public interest, so the NAIH would support that the online disclosure of public asset declaration of local representatives shall be regulated by law.

In some cases the municipalities tend to order in local decree or in FOI statues the disclosure of asset declaration of municipally-owned companies' leaders, which are not even personal data of public interest upon the law.[3] NAIH warned that except the persons concerned in Act CLII of 2007 on obligation to declare assets, without the authorization of law, municipalities cannot make asset declaration compulsory in local government regulations. According to Section 5 paragraph (1) point b) of the Privacy Act, municipality regulation can order the processing of personal data only by authorization conferred by law. Likewise the municipality cannot order the disclosure of non-public asset declarations according to the Section 5 part 1.

The asset declaration – except the identity records – of mayors and local government representatives in Hungary are data public on grounds of public interest according to Section 39 (2) of Act CLXXXIX of 2011 on Hungary's Municipal Governments and Section 26 (2) of the Privacy Act.

The consent as legal basis of publishing non-public assets declaration is solicitous in connection with the right of informational self-.

According to Section 5 (1) of the Privacy Act, personal data may be processed when the data subject has given his consent, or when processing is necessary

3 [NAIH/2015/2294/4/V., NAIH/2015/538/2/V., NAIH/2015/2628//V.]

as decreed by law or by a local authority based on authorization conferred by law concerning specific data defined therein for the performance of a task carried out in the public interest. Section 3 point 7 defines the data subject's consent, which shall mean any freely and expressly given specific and informed indication of the will of the data subject by which he signifies his agreement to personal data relating to him being processed fully or to the extent of specific operations.

To conclude, and in the light of these points, the given consent needs to be volunteer and without any interference. In the context of employment, difficulties could be faced with the voluntary nature of the concerned persons given consent.

Relevant to this case, NAIH has informed the local authorities that the publicity of data related to the public service task of the local representative bodies are welcomed and available for anybody free of charge. The voluntary nature of the consent given by other leaders and employees in bodies and companies created by the local authority for publishing their assets declaration, according to NAIH, cannot be guaranteed in a subordinate relationship.

V.2. Old-new practices relating to FOI requests and the fulfillment of the disclosure obligation

In connection with the amendment of the Privacy Act in 2015, NAIH tried to give guidelines for both enforcers and legislators to ensure that freedom of information is not restricted unnecessarily.

On the one hand, at the amendment of the Privacy Act, NAIH actively tried to orientate the legislator on how to word the provisions assisting the enforcement of the fundamental right to access to data of public interest. On the other hand, NAIH commented on the implementing regulations for the reimbursement of expenses, furthermore answering the consultation submissions helped to develop a reliable case-law.

V.2.1. May a body with public service functions request identification for fulfilling FOI requests?

Public information and data public on grounds of public interest can be accessed by anyone in regard of Article VI (2) of the Fundamental Law and Section 26 (1) and 28 (1) of Privacy Act.

According to Section 28 (1) of Privacy Act, data of public interest shall be made available to anyone upon a request presented verbally, in writing or by electronic means. Access to data public on grounds of public interest shall be governed by the provisions of this Act pertaining to data of public interest. According to Section 29 (1a) and (1b)

- the body with public service functions that has the data of public interest on record is not obliged to comply with requests for public information whereby the request is identical to that of submitted by the same requesting party within one year and with the same dataset provided that there were no changes in the dataset concerned;
- the body with public service functions that has the data of public interest on record is not obliged to comply with requests for public information if the requesting party does not provide his/her name, in case of a legal person its description, and contact details through which the requested dataset or any other information can be provided.

According to the amended Section 28 (2), unless otherwise provided for by law, the processing of personal data of the requesting party in connection with any disclosure upon request is permitted only to the extent necessary for disclosure, for the examination of the request as determined by Section 29 (1a) as well as for the collection of payment of charges needed for the disclosure. Following the deadline as determined by Section 29 (1a) and upon receipt of the said payment, the personal data of the requesting party must be erased without delay. Processing of personal data in this way is limited to 1 year, after this, the aim of the data processing vanishes, additional data storage creates unlawful processing of data.

This legislation follows that when requesting data, identification is not needed, and it is not a legal requirement either. The person requesting data needs to provide the contacting data only.

Referring to the request sent by the KiMitTud (WhoKnowsWhat) website, NAIH recommended that to fulfill the data requests submitted via the data requesting system, the automatic email address at KiMitTud and the name specified during registration is generally sufficient.

The personal data necessary for the fulfillment of the data request and for data processing objectives laid out in Section 29 (1a) of Privacy Act will be treated by the body performing state or local government responsibilities, as the requesting

party provides its name and email address, beyond those data, data processing operations such as determining the person's identity it is not necessary, thus constitutes unlawful data processing [NAIH/2015/4710/2/V].

V.2.2. Is it objectionable when the party requesting for the same data within 1 year, and the body with public service functions denied the request on the same data before?

The aim of the restriction accepted by NAIH is the following: if one has got to know the data, and there were no changes, to reduce the administrative burden, it is not necessary to fulfill the request. Ignoring the data request, however, remains unacceptable, and the administrative allowance is to be applied only on substantially completed former data request. When multiple data request arrives to a body with public service functions, NAIH recommends publishing the information on the website and providing a link for fulfilling subsequent data requests.

V.2.3. When does the deadline of fulfilling FOI requests start when the request is sent electronically?

Section 29 (1) of Privacy Act has reified the start of the deadlines of fulfilling data requests.

While the previously existing wording said that the deadline started when the body had become aware of the request, while according to the new provisions, it must comply with requests for public information at the earliest opportunity within not more than fifteen days. The starting date of the deadline is therefore the date when the email arrived to the body with public service functions, regardless of whether it is a business day, a public holiday or a day during the administrative brake. Data requests arrived during the administrative break can be fulfilled within the statutory time limits if – according to the general publication list and rules laid down in Section 37 (1) and Section 30 (6) of Privacy Act – the body provides an email address which is still supervised by a colleague during the break.

V.2.4. The mandatory regulations to be drawn up

During the investigations, NAIH found that deficiencies and overruns in relation of fulfilling FOI requests can be traced back to the practice of bodies with public service functions, as they did not prepare the manual on information on public interest.

NAIH recommends the following elements in the guide:

- The scope of the policy: requesting the data public on grounds of public interest, the employee's data public on grounds of public interest held by bodies with public service functions.
- Appointing the person or department responsible for fulfilling requests on data public on grounds of public interest.
- The procedural rules on fulfillment of the data demands: specialized case management system or creating some special rules in relation to the overall case management order; determining the mailing and electronic address, fax number through which they accept demands; answering the verbal demands; decision about whether a submission is to be considered as data request.

Section 35 (1) (2) (3) of Privacy Act state that

(1) The head of the data source subject to electronic publication shall provide for having the data and information specified on the publication lists defined in Section 37 published accurately, up-to-date and on a regular basis, and for having them sent to the data disseminator.
(2) Responsibility for the publication of the data by electronic means, continuous access, and for keeping them authentic and regularly updates lies with the data disseminator.
(3) The data source and the data disseminator shall adopt internal regulations for laying down the detailed rules for discharging the obligations referred to in Subsection (1) and Subsection (2), respectively.

According to the above, special rules need to be laid down on disclosure of the data by electronic means, but these rules can be integrated into the manual about the fulfillment of request for data of public interest.

V.3. Consultation cases in the field of freedom of information

In 2015, bodies with public service functions turned to NAIH asking for guidance regarding legal interpretation.

V.3.1. The publicity of KEHI-reports

Within the consultations the request from the Constitutional Court was a priority task regarding the publicity the Government Control Office (hereinafter referred to as: KEHI) reports.

NAIH helped the work of the Constitutional Court with its recommendations on KEHI's investigations regarding freedom of information.

Even the Data Protection Commissioner's investigations showed that while the legal safeguards ensuring the publicity of public funds have widened, the general public could not have had better knowledge about the public funds control of KEHI because the secret certificates issued by presidents of the body did not support the enforcement of transparency [ABI-2302/H/2015].

NAIH found through the course of its investigations that compared to the recommendations issued by the Data Protection Commissioner in 2005 there has been no major change in the control of government bodies and public relations.

Reflecting on NAIH's investigation [NAIH/2015/235/5/V, history: NAIH-2439-5/2014/V] KEHI argued that according to Section 11 (1) and (3) of the 355/2011 (XII. 30.) Government Decree on the Government Control Office (hereinafter referred to as: Government Decree), all investigation made by KEHI is done by the request of the Government, the Prime Minister or the Minister responsible for coordinating government activities, the purpose and the way of the data processing is being determined by them. In view of the above, in relation to KEHI reports, KEHI does not qualify as data controller laid down in Section 3 point 9. of Privacy Act.

According to KEHI, the investigation reports are decision-making data of the body or person ordering the investigation, which is based on Section 27 (5) of Privacy Act. This means that these reports are not public within ten years of the date when they arose.

NAIH put forward the following arguments:

According to Section 35 (1) of the Government Decree, "the publicity of the report prepared by the Government Control Office is based on Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information, as well as on provisions of laws regulating secrecy breeds."

According to Section 3 Point 5 of Privacy Act, 'data of public interest' shall mean information or data other than personal data, registered in any mode or form, controlled by the body or individual performing state or local government responsibilities. The "controlled by body or individual performing state or local government responsibilities" phrase means only, that the requested data is stored and

is physically available in the database of the body. While fulfilling the requests in connection with data of public interest, the body performing state or local government responsibilities qualifying as data controller does not therefore depend on the conditions laid down in Section 3 point 9 of Privacy Act, it is not essential to make the concerned body decide on the faith of the data, or set the aim of the data processing.

In the light of the data available and stored by the body performing state or local government responsibilities, the body is considered as data controller and is obliged by Section 26 (1) of Privacy Act even when different body or person requested the document or procedure at KEHI.

In the light of enforcement of freedom of information, data controller and data processor relationship in general can be considered as inadequate, this relation comes up in Section 3 (2) of Privacy Act, where personal data processing is due. Furthermore when speaking about the enforcement of freedom of information, this relation cannot be considered concrete because here we are talking about elements of personal data processing, such as the principle of purpose limitation, rights to information, legal base of data controlling.

In the light of the above, KEHI is considered as obligee of FOI request regarding the physically available data of public interest, which can be found in its database in connection with its investigation reports, even when the investigation was requested by different body or person and KEHI is not entitled to make governmental decisions[4].

According to Section 27 (5) of Privacy Act, any information compiled or recorded by a body with public service functions as part of, and in support of, a decision-making process for which it is vested with powers and competence, shall not be made available to the public for ten years from the date it was compiled or recorded. Access to these information may be authorized by the head of the body that controls the information in question upon weighing the public interest in allowing or disallowing access to such information.

This means that only the proceedings made by the body performing state or local government responsibilities within its own competences and duties constitute the possibility of using the reference to information underlying decision quality. It is common in public administration that the tasks and proceedings carried out by

4 You can find the whole report on our wesite: naih.hu/files/Infoszab_allasfoglalas_NAIH-2015-6986-2-V.pdf

a body is based on another body's decision or prepares other body's decision making. Before 1th October 2015, data of the decision-making process could only be such data which was created during the proceedings for the decision-making. This capacity of the data can only be possessed by its connection to the decision-making process. [21/2013. (VII. 19.) Constitutional Court decision]

It would be an unjustified and disproportionate restriction of freedom of information if the result of the proceeding in relation to KEHI's decision could not be made public referring to Section 27 (5) of Privacy Act.
The Constitutional Court has stated that legislations creating inhibitive effects on freedom of information need to be interpreted strictly. "In a democratic society, availability of data of public interest is principle; further in the alternative, restriction of the availability of data of public interest is exceptional." [12/2004. (IV. 7.) Constitutional Court decision]

In the procedure of KEHI, only those data will perform as data of the decision-making process which KEHI creates or records during its inspection and is necessary for the work of the employees of KEHI. In this relation, NAIH noted that the "internal use" of the data is inseparable of its decision-making nature. "The working documents, reminders, drafts, sketches, recommendations, mailing for internal use are usually documents created during decision-making processes, publishing these may significantly pull back the public servants during their work, and are normally exempt from public." [34/1994. (Vi. 24.) Constitutional Court decision]

The proposed investigation report based on Section 35 (1) of the Government Decree is the product of the procedure, which data cannot be determined as decision-making data on the grounds of preparing another body's decision. At this point, KEHI's procedure is considered done, decision-making data is only the data which was generated during the creation of this report, not the data found in the report.

In the strict sense of the word, in the light of KEHI's proceeding and its investigation report, we cannot talk about decision-making process, as according to Section 37 (1) i) of the Government Decree, the investigation report contains "investigation findings and recommendations", so the purpose of the investigation is not "decision-making" but wording the recommendation and concluding experience.

NAIH also highlights that KEHI has the control over the use of public funds and checks the sustainable management of national wealth, therefore the need for freedom of information arises significantly. Within the availability of data of public interest, transparency of public funds is crucial.

KEHI referred to Section 27 (5) of Privacy Act as a predetermined ground for refusal, which is unacceptable regarding the decision of the Constitutional Court about the publicity of the decision-making data. NAIH consequently integrates the interpretation regarding Section 27 (5) of the Privacy Act into its resolutions: the body performing state or local government responsibilities needs to clearly define, what decision-making is served by the data of public interest which is willing to be published and also whether the publishing would derail the effective implementation of the decision or leave the effective work done by public servants obstructed. [12/2004. (IV. 7.) Constitutional Court decision, ABH 2004. 217, 226-227.]

Furthermore, NAIH says the total concealment of the reports cannot be acceptable regarding also the interpretation of the Constitutional Court which says "the document as a whole – regardless of the content – cannot be qualified as decision-making data". [21/2013. (VII. 19.) Constitutional Court decision]

According to the 6/2016 (III. 11.) decision of the Constitutional Court, after obtaining the opinion of NAIH – in a procedure based on Section 27 of Act CLI. of 2011 on the Constitutional Court – the Constitutional Court has annulled the Budapest Court of Appeal's decision number 8.Pf.20.594/2014/6., because in the challenged judgement, the general obligation of the body performing state or local government responsibilities based on Section 26 (1) of Privacy Act was a way too restrictive interpretation by the court, as it was restricted on data controllers processing personal data in a concentrated manner defined by the legislator, defining the purpose of the processing of data. According to the challenged judgement, it could not be defined whether the contents of the KEHI-report had been investigated by the court, as the conclusion on the restriction of publicity had not been based on the examination of the content of the Report, that it is based concretely on the justification of the decision, and the refusal of disclosure of data based on the title laid out in Section 27 (5) of Privacy Act is prevalent during the whole Report. Thirdly, the Constitutional Court has declared the judgement contrary to Fundamental Law because it has not examined that what kind of decision has been served by the Report (or part of the Report) demanded by the requesting party, and accepted that it was data to substantiate the decision.

V.3.2. Names of public defenders and the number of their respective appointments

The Ministry of Justice also requested a resolution from NAIH in connection with the Hungarian Helsinki Committee v. Hungary procedure before the European Court of Human Rights (no. 18030/11), which is about the data request of the

Committee initiated in 18th August 2009. The Committee requested data from the Hajdú-Bihar County Police Headquarters and from the Debrecen police, in which it requested the names of the attorneys who were seconded in 2008, and also the number of the respective appointments.
The Debrecen City Civil Court decided on the publicity of the data, because it was certified as personal data of public interest, but according to the decision, the public defender is not a person with public service functions, therefore the data cannot be released as public data. The Supreme Court upheld the decision, then the Committee turned to the European Court of Human Rights. NAIH has made its view regarding the boarder of data protection and freedom of information, the dissolution area of the conflict of these laws and personal data of public interest under the then applicable Act LXIII. of 1992 on Protection of Personal Data and the Availability of Data of Public Interest (Avtv.). In relation to personal data of public interest, law enforcement bodies usually have a problem determining the group of persons, the persons acting on behalf of the body performing state or local government responsibilities, so this recommendation by NAIH – despite that is based on an ineffective legislation – can be useful in the future as well.

Persons specified in Section 19 (4) of Avtv. performing state, municipal government or other public tasks are representatives of the State, the State's and public authorities' acts are manifested through their activity. The relevant data are basically not considered to be data of their privacy, so these persons undertaking public duties need to be aware that their personal data in relation to their public duties might become public. The scope of the subject according to Section 19 (4) of Avtv. is: any person attending to statutory State or municipal government functions or performing other public duties provided for by the relevant legislation.

The concept of "person…performing other public duties provided for by the relevant legislation" is clearly identified with a person with independent competences and duties such as local government officials (for example the President of the Republic, the President of Parliament, the President of the Constitutional Court, the President of the Curia, President of the National Bank of Hungary, the Prime Minister, other ministers, mayors etc.). These people are obliged to make data regarding them available by their individual concern.

According to 6/1998 (III. 11.) Constitutional Court decision, the actual effectiveness of defense rights is a prerequisite to the constitutionality of the system of criminal procedure.

The public defender is representing the right of the defense and works on behalf of a body performing public duty, and by making available his/her name and task conferred by the State cannot conflict its privacy. The availability of the number of the respective appointments can not infringe business secrets as the expense of the central budget is considered to be data available for public interest even if a natural person is the holder of the payment.

VI. Legislative activity of the NAIH

Pursuant to Article VI (3) of the Fundamental Law the NAIH shall be responsible to oversee and promote the enforcement of the rights to the protection of personal data and access to public information and information of public interest. The framework of the enforcement of information rights is determined by law therefore our Authority shall monitor the legislation process and the application of legal norms so that it can propose amendments if it is deemed necessary. According to point a) Section 38 (4) of Privacy Act NAIH shall have powers to make recommendations for new regulations and for the amendment of legislation pertaining to the processing of personal data, to public information and information of public interest, and shall express its opinion on bills covering the same subject. In addition, the European law also requires the inclusion of the NAIH into the national legislative processes whereby Article 28 (2) of the 95/46/EC Data Protection Directive prescribes each Member State shall provide that the supervisory authorities are consulted when drawing up administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data. Recitals (53) and (54) of the said Directive point to the fact that certain processing operations are likely to pose specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, such as that of excluding individuals from a right, benefit or a contract, or by virtue of the specific use of new technologies; the amount posing such specific risks should be very limited and prior checks may take place in the course of the preparation either of a measure of the national parliament or of a measure based on such a legislative measure.

The main area of the legislative involvement of NAIH is the reviewing of legislative bills in the form of formal administrative consultations or discussion. On the volumes of legislation and on subjects to be regulated, NAIH has less involvement, mainly because these are being defined by social regulatory requirements and policy considerations.

Distribution of legislative files by year and legal instrument

Legal regulation/year	**2013**	**2014**	**2015**
Act	86	33	79
Government decree	89	63	133
Ministerial decree	92	85	126

Government resolution decree	28	21	61
Other (parliamentary resolutions etc.)	15	7	27
Total	**310**	**210**	**426**

Number of remarks in opinions are shown in the chart below.

Type of remarks	**Number of remarks**
Relating to data protection	298
Relating to freedom of information	53
Other	137
Total	**488**

It can be seen that the number of cases and resolutions have significantly increased in 2015. Out of the cases from 2015, the amendment of the Privacy Act and the large public projects can be highlighted.

VI.1. The amendment of the Privacy Act

The Privacy Act provides the basic rules and general legal framework on the rights of informational self-determination and the freedom of information. This amendment seems to be the first essential, partially conceptual correction of the Privacy Act and probably the last amendment before the EU regulation on protection of personal data enters into force in Europe. In the last few years, NAIH initiated the amendment of the Act several times and prepared technical proposal for it as well. In this context, the following can be mentioned:

- The amendment just follows decision of 4/2015 (II.13.) of the Constitutional Court, which concluded that the legislator has failed to ensure the validation of the fundamental right to access to data of public interest through a substantive revision of data qualification when qualifying data of public interest and data public on grounds of public interest and thus restricting the publicity. The Constitutional Court has called upon the Hungarian Parliament to enact the missing rules and remedy the unconstitutional legislative omission.
- As a result of the administrative consultation, observations of the law and public bodies have been integrated into the content of the draft.

– The Parliament has decided on the acceptance or rejection of the amendment proposal of the bill.

However, it can be stated that the new effective ruling is mainly consistent with NAIH's efforts, that is:

– the reception of the legal developments in Europe,
– bringing the rules into line with the challenges of the infocommunication technology of the XXI. century,
– the simplification of the legislation.

NAIH believes that one of its key task is to help interpreting the legislations regarding the basic rights on information which stems from the Fundamental Law regarding the protection of fundamental rights.

The amendment of Section 71 of Privacy Act made the data cognitive powers of NAIH more differentiated, thus excluding the availability of some so-called particularly important data stored at law enforcement authorities and security services. The prerequisite of inspection of data control is making the data available for the inspecting body. Thereby reducing the scope of NAIH's jurisdiction on request for data means that the inspection of data processing which fall under cognitive restriction cannot be carried out in the future, deteriorating the independent data protection control. This summary statement is based on the fact that in case of a data which is not available for NAIH, in accordance with Section 71 (3) of Privacy Act, NAIH calls the minister for data control, which means that the legality will not be measured by an independent external body, but someone who might have an indirect interest in the inspected bodies data processing.

The differentiation of NAIH's data cognitive power is constructive on one aspect. The rule which intends to clarify that when NAIH is about to inspect a document which also contains data directly not available for NAIH, the document needs to be provided for NAIH with the making the unavailable data unrecognizable (Section 71 (3c) of Privacy Act).

VI.2. Big data processing projects of the State – central biometric face profile database

The preparation of the drafting legislation regarding the central biometric face profile registry was continued in 2015. The enactment of the legislation is done,

therefore NAIH's recommendations will be displayed in the light of the framework of the legislation. These recommendations were provided for the Ministry of Interior during the consultation of this bill.

NAIH's conceptual standpoint is that a mechanical or mechanical face recognition with human assistance is an application of a biometrical data processing technology which substantially affects the right of privacy and by its very nature, the affection is difficult to predict. Put simply, the usage of biometrical technologies to process data present a huge risk, whereas particular consideration must be given by the State to protect the privacy of the affected and the rights to protection of personal data. NAIH made recommendations on creating legislations which determine the constitutional conditions of the biometric data processing.

In this case it is crucial, that the legislation created a State biometric face profile database and facial image analysis center where the identification of unknown persons and the analysist support of identifying persons are done by human work with IT support. Using human resource creates a natural barrier on the speed and amount of data process. This also means that the later elimination of human resource will create a fully automatic facial data identification, which will need a revised guarantee scheme of data protection.

The Ministry of Interior's proposal contained a data process aim, which allows the restriction of informational self-determination within constitutional framework, and also where a central biometric facial image database is needed, and where the aim of data processing in another way would be more difficult to reach. The data processing aim is the identification of the criminal of unknown identity with the help of the currently available facial profile. For all this, NAIH has examined whether within constitutional framework, creation of a central biometric facial profile database is possible or not. Namely according to our view, even from essential state interest – like law enforcement and national security –, creating and using a central biometric facial profile database is only acceptable if the data processing comply with the constitutional and legal requirements .

NAIH recommended the following data protection criteria:

– Processing and using biometrical data falls under the scope of a personal data processing, thereby it should be consistent with the constitutional requirements of protection of personal data. This is why a government decree is not an option, only a legal act can determine the implementation of the central biometric face profile database and the data processing.

– The biometric profile or template (the Hungarian legal terminology had not yet clarified which term should be used) is not identical with the data out of which it was created. So the biometric facial profile is not identical with the facial image. This is essential because it clarifies that the eligibility for facial data processing does not entitle the data controller to create a bulk of automated, machine process-suitable profile. The biometric profile can only be processed on the consent of person concerned, or the processing of the biometric profile is required by act indicating the type of data.
– The legislative framework of the central biometric face profile database shall prevent the generalization of processing of biometrical profile data, to avert the facial profile being a universal identifier code. Therefore the act shall declare that:

    • biometric facial profile data cannot be collected by any other public body,
    • the central biometric facial profile database needs to be separated from the data source database (from the personal data and address register), natural personal identification data cannot be stored, linking data processing unauthorized needs to be prevented,
    • passing biometrical facial profile to any data controller body by the central biometric facial profile database needs to be strictly banned.

– Creating a biometrical facial profile database on the whole nation can only be used in conjunction with the essential state interest. Using the database for other purposes would violate the concerned person's informational self-determination.
– The legislation needs to clearly define the possible aims of data processing. State bodies' eligibility needs to be defined in connection with the database.
– The legislation needs to clearly define that within the actual aim of data processing, for whom can be asked for portrait identifier service (for example unknown suspect).
– It needs to be defined, under what conditions can governmental bodies turn to the central facial image analysis system and how can they use the services.
– It would be constitutionally unacceptable if state bodies would secretly observe the nationals, so special legislative framework needs to be created on the secret street information collection in connection with the biometric identification or other, mandatory monitoring, which

- cannot be realized on the level of community dimensions;
- cannot be a mass data collection, not even in pseudonym form;
- it can only happen for a legitimate aim.

– Implementation of the bill would significantly limit the right to personal data protection of great mass of citizens. This means a far-reaching decision which requires the Hungarian people's opinion.

As a result of the negotiations, NAIH's above detailed proposals have been implemented into the bill. (NAIH/2015/3009/J)

VI.3. Big projects of the State – National Unified Card System and the e-card personal ID card

The preparation of legal regulations about the National Unified Card System (hereinafter referred to as: NEK) and e-card personal ID card (hereinafter referred to as: e-SZIG) have also been achieved. These two regulatory matters are linked with the common infocommunication technology background.

The following recommendations of NAIH have been implemented into the NEK regulation:

– If further card is assigned to the primary e-card, it should be made available for the user to limit the use of the card and the availability of the data of these cards.
– Further anonym card should be available without natural personal identification data.
– In the NEK system, such connection code should be used to communicate with, which does not hold the personal data of the concerned.
– During the usage of the card, card acceptances cannot log data out of which the cardholder's activity can be deduced.
– From the central card registry, providing data is only available if the name and card ID of the affected person's is provided.

NAIH recommended in connection with the e-SZIG amendment of Act LXVI of 1992 on Keeping Records on the Personal Data and Address of Citizens (hereinafter referred to as: Nytv.) that the storage unit of the card should be designed that only authorized body can access the data (Section 29/B (1) of Nytv.). The data

content of the card needs to be processed only by card acceptor with statutory entitlements.

VI.4. Big projects of the State – connecting databases

On the 28th of July 2015 several Hungarian newspapers brought down the communique of the Prime Minister's Office about the connection of state bodies' databases in accordance with the EU administration development program. The news appeared on the Hungarian Governments' official website as well. The scope of the databases have not been specified, but NAIH draws attention that if the connection affects not only infrastructure improvements but also the databases storing personal data, the implementation of the connection affects the right to protection of personal data. According to the foregoing, NAIH requested information from the Secretary of State responsible for EU development projects in the Prime Minister's Office on whether what database of state bodies are affected and whether the connection of the databases are prepared on data level as well.

The answer of the Secretary did not contain any specific information on the planned database connection, it was only referring to the related government decision. In this context NAIH points out that the connection of database of State bodies is only possible if it is in line with the statutory requirements of processing personal data and with the principle of divided information systems. (NAIH/2015/4928/J)

VI.5. Big projects of the State – the single framework of electronic administration

In 2015 the Ministry of Interior has prepared a bill regarding electronic administration. According to NAIH, the "Unified Digital Administration Field" (hereinafter referred to as: EDÜT) conception is about spreading the modern information technologies on national level with increased governmental involvement. These systems usually have a central element in State hands (central register, communication point) whereby the Government can directly affect the operation of it, and can collect data as well. Such centralization of data is not necessary, good practice examples from foreign countries proof that electronic card systems and electronic administration infrastructures can be created on less centralized levels

as well. However centralization can only be judged on grounds of protection of personal data, when large-scale inspection of the citizens is possible and segments of their privacy can be controlled by the State.

In the bill reviewed by NAIH, EDÜT would have a central customer ID registry (hereinafter referred to as: KÜNY), where every those people's data will be stored, who are make use of the electronic identification service of the State. During this procedure, the client's data will be queried, which creates a data transfer register available for monitoring and logging electronic administration activity.

The obligation of logging data transfer done by the data controller is established by the Privacy Act to prove to the concerned persons, what personal data was transferred to which body or person. The logging of data transfer is also personal data processing, therefore it needs to be questioned, whether the logging of these transfers serve to protect personal data, or the protection of personal data would be realized through the restriction of this very logging activity. According to NAIH, the logging of data transfer should be done on decentralized level, referring to the "privacy by design" principle. Therefore in terms of protection of personal data, NAIH welcomed the incorporation of the proposal into the bill. (NAIH/2015/5944/J)

VI.6. Big projects of the State – the capacity extension of the Paks nuclear power plant

Although this project is not about info-communication development but the expansion of the nuclear capacity of the Country, the related legislation is an instructive case study on the ground of informational fundamental law. While preparing Act VII of 2015 on the investment related to the maintenance of the capacity of the Paks Nuclear Power Plant, and the amendment of certain laws related (hereinafter referred to as: Paks II. tv.), the Minister of National Development has not sent the bill to us asking for opinion, although Section 5 of the bill ruled about the limitation of the availability of information. Therefore, we have only become aware of the proposed regulatory content, when the Minister has submitted the bill to the Parliament under number T/2250 at 1st December 2014.
NAIH has challenged Section 5 of Paks II. tv. (NAIH-2782-2/2014/J)

The NAIH statement – considering Hungary's national economic interests and the importance of steps for the elimination of energy dependency – has pointed out, that when creating legislation on the publicity of data regarding Paks nuclear pow-

er plant, international and EU legal documents deserve special attention. Thus primarily the UNECE Convention on Access to Information, Public Participation in Decision-making and Access to Justice in Environmental Matters (Aarhus Convention) and the Directive 2003/4/EC on public access to environmental information and repealing Council Directive 90/313/EEC.

The Preamble of 2003/4/EC and Article 3 point 6 of the Aarhus Convention supports the national legislation to provide wider scale of rights on the accessibility of information. The bill number T/2250 is restricting the fundamental right to access data of public interest and data public on grounds of public interest which is contrary to Section 27 (5) of Privacy Act and also ignores the Aarhus Convention.

Furthermore Directive 2009/71/EURATOM establishing a Community framework for the nuclear safety of nuclear installations was amended on 8th July 2014 and according to the new regulations, Member States have implementation obligations providing proper opportunity for the community to join the decision-making process on allowing nuclear installations. To fulfill these obligations, rules on accessibility of data needs to be differentiated to inform the public according to the rules laid down in Aarhus Convention and in the Directives.

Section 20 (7) of the T/2250 bill contained restrictions on access to data about the nuclear facility and on its architectural forms during the licensing process, and also on the access to trade secrets. In connection to this, NAIH has found that the need for restriction needs to be measured carefully, in relation to the fundamental right to freedom of information and to the publicity of managing public funds both laid down in the Fundamental Law. According to NAIH, the contested provisions do not provide a basis to restriction of publicity of managing public funds. Respecting the investors' interests are not commensurate with the restriction of the fundamental right to freedom of information.

The Parliament has adopted the rules on accessing data in Paks II. tv. with a changed content. NAIH considers without doubt that the capacity extension of Paks nuclear plant is strategically important regarding the long-term energy supply of the country, and the safer production of nuclear energy is also crucial. Which is why – according to Section 27 (2) of Privacy Act. – certain part of data of public interest about the investment can be restricted in a different legislation. Section 5 of Paks II. tv. is in consistent with Section 27 (2) of Privacy Act to the extent that only certain types of data public interest is affected by it and it targets aims laid down in the Act (national security interest, to ensure intellectual property rights). However the way of restricting publicity raises questions:

- The restriction affects extensive set of data ("business and technical data") consisting many types of data which require different perception in terms of restricting their publicity and the period of restriction. However a common period of time has been set out for restriction.
- The rigidity of ex lege restriction can be softened, when in case of request on data of public interest, the data controller could consider the need for restriction. But according to the regulations, the data controller must strictly reject the fulfillment of the data request if it is related with data set out in Section 5 of Paks II. tv. even if based on the information available, restriction of publicity is not necessary.
- The restriction may affect data which unconditional restriction for a 30 year-long period is not necessary.

NAIH points out, that due to the described characteristics of Section 5 of Paks II. tv. a special responsibility belongs to the data controller. Restriction of access to data of public interest should not go beyond what is necessary in order to achieve this objective. Thereby we have contacted the government official responsible under case number NAIH/2015/1894T for maintaining performance of Paks power plant to draw attention in this context:

- There might be business and technical data which fall under Section 5 of Paks II tv. that are public according to other legislations, such as Act CXCV. of 2011 on Public Finances or Act LXXXI. of 2001 on promulgation of the Aarhus Convention adopted in 25 June 1998 on access to information in environmental matters, participation in decision-making of the public and ensuring the right to justice. In accordance with the above, Section 5 of Paks II tv. must be interpreted strictly in such a way that it does not affect data which other legislation defines as accessible.
- We understand that Section 5 of Paks II. tv. does not exclude the data controller to publish such business and technical data on its own choice which does not interfere with national security interests or does not infringe intellectual property rights, for the prevail of access to information of public interest. Therefore NAIH initiated to create a website in order to inform the public, where the data controller can publish data generated during the preparation and implementation of the project, in particular about the environmental impact of the investment and data on the use of public funds. (NAIH/2015/1894/T)

VII. Cases concerning classified information

VII.1. The 4/2015 (II. 13.) decision of the Constitutional Court

In cases affecting classified information NAIH conducts either an investigation proceeding or an administrative proceeding for the control of secret.

As we have already mentioned in Chapter VI.1. the amendment of the Privacy Act in 2015 has significantly changed the procedures carried out by the Authority, in particular the administrative proceeding for the control of secret and the right to access classified data. The amendment followed the Constitutional Court decision of 4/2015 (II. 13.) which states that the assertion of freedom of information on legislative levels is determined by the Privacy Act, also defining its terms and limits.

According to Section 27 (1) of Privacy Act, access to data of public interest or data public on grounds of public interest shall be restricted if it has been classified under the Act on the Protection of Classified Information. According to this Section, the data controller can deny the request on access to classified data legally. If the requesting party turns to the court, the court will consider the denial based on Section 31 (2) of Privacy Act. Under previous rules, the data controller needed to prove only that the request was targeted classified data set out in the Act CLV of 2009 on Protection of Classified Information (hereinafter referred to as: Mavtv.) Consequently the courts procedure was only formal. According to Section 2 (2) of Mavtv., classified information is only available for those with administrative capacity or public capacity and it is necessarily required.

According to Article I. (1) of Fundamental Law, respecting and protecting the fundamental rights is the State's absolute obligation. This means, the State needs to provide the conditions necessary for the enforcement of fundamental rights.

The Constitutional Court has found that the right to access data of public interest can be violated if the data request can be formally denied according to Section 27 (1) of Privacy Act. Namely because by limiting the right to access data of public interest there is a content requirement: the restriction needs to be necessary and proportionate in relation to the objective pursued with the restriction. Besides, the possibility for effective judicial remedy against the restriction of publicity needs to

be ensured, with a content analysis of the justification about restriction of publicity. If accessing public data can be restricted by referring to a fact about restriction of publicity and the justification of the content of the restriction has not been proven undoubtedly, then the right to access and dissemination of public data is unfounded, thereby constitutes unnecessarily restriction.

VII.2. The relationship of court proceedings and administrative proceedings for the control of secrets

Having regard to the new administrative procedure rules for the control of secrets, NAIH believes that the amendment of the Privacy Act was due not because the previous rules were contrary to Fundamental Law, but because a constitutional problem has emerged in other areas, and this problem can be sold with the use of administrative proceedings for the control of secrets. According to the Constitutional Court, it was concerned that when classifying data of public interest and data public on grounds of public interest, the legislator did not ensure – against the restriction of the publicity – the enforceability of right to access data of public interest through the substantive review of the data classification.

The legislator has used the administrative proceeding for the control of secrets as a tool for resolving a constitutional problem. If the data controller denies the request to access data of public interest and the refusal is based on its classified nature, and the requesting party turns to the court for the revision of this refusal, the court will start NAIH's administrative proceeding for the control of secrets and at the same time suspends the trial. In this case, the Authority must start the administrative proceeding for the control of secrets and cannot use the rules of the investigation proceeding during the examination of the legality of the classification, which rules are laid down in the Privacy Act.

Therefore, it is provisionally concluded that Privacy Act helps the Authority with the mandatory investigation, but at the same time, according to Section 62 (1) of Privacy Act, if the investigation of the Authority suggests that the classification of certain national security information is unlawful, the Authority may open administrative proceedings for the control of classified data. NAIH's experience is that the submissions handed in by nationals or the press do not start actual administrative proceedings for the control of secrets, because the submissions do not contain information on possible unlawful classification of national classified information.

NAIH has effective legal methods to control the legal instruments of classification, which helps to discover the fact pattern effectively. At the same time, the Authority's findings are not compulsory for the court.

The outcome of the procedure started by the court: if the Authority finds that the classification of the information was unlawful and calls the classifier to delete the classification who – let us suppose – accepts this and does not call for a judicial review in this matter, 64 days from the date of notification, the classification of the national classified information will change and the requesting party can access the data.

When the classifier calls for a judicial review (within 60 days), then it needs to prove that the classification was lawful. The court will be made available with the review of the Authority, the copy of the classified information, the proposal on the classification, the reasoning of the classification. In this sense, NAIH's procedure is a preparation of the litigation: it collects the evidence. If the requesting party would be the plaintiff in the litigation, this could not be guaranteed.

VII.3. The application of law related to the administrative proceedings for the control of secrets

VII.3.1. The subject of the administrative proceedings for the control of secrets

During these proceedings, the finding of the fact is about the verification of the legality of the classification. The classification is lawful if it complies with Sections of Mavtv. (basic principles, rules of classification etc.), and according to the Constitutional Court, the classification of the data of public interest and data public on grounds of public interest needs to be done with taking public interest for the publicity of the information into account, and the classification is proportionate with the interest for publicity.

VII.3.2. Administrative proceedings for the control of secrets in case when the classification of the national classified information no longer exist

What kind of effects does it have on the procedure, when the classifier has terminated the classification of the national classified information as the subject of

the procedure? According to our first determination, the answer can be found in Section 62 (1) of Privacy Act: if the court, according to Section 31 (6a) initiates the Authority's procedure, NAIH starts administrative proceeding for the control of secrets. So the Authority does not have any discretion: if the court initiates the procedure, it must be started necessarily, regardless whether the classification of the information has ceased in the meantime due to review, override or invalidation of classification. What is the focus of the proceeding for the control of secrets in this situation? Here is the answer:

If NAIH finds infringement of the rules on classifying national classified information, it applies the sanctions laid down in Section 63 (1) a) of Privacy Act: in the event of any infringement of the regulations pertaining to the classification of certain national security information – shall call upon the classifier to modify - in accordance with the law - the level or term of classification of information classified at the national level, or to have it declassified. When there was no infringement, according to point b), confirms that the classifier acted in compliance with the classification rules on national classified information.

VII.3.3. The legal succession of the classifier

The amendment of the Privacy Act made clear that in the proceedings for the control of secrets, the classifier is a client. This raises questions on legal interpretation, because the Authority carries out ex post verification of the legality of classification. Since then, there is a chance for the replacement of the classifier. In this case, the classifier who made the classification of the national classified information is missing, and question raises whether the previous classifier will be the real client or not.

In this respect, NAIH has noted that the classifier jurisdiction is not a privilege related to a person. It is a task and jurisdiction, a role and competence laid down in Section 3 (3) and Section 4 of Mavtv. So the client of the administrative proceeding for the control of secrets is always the person who is entitled to the dispose information within its classifying jurisdiction (primarily practicing the revision of classification).

If the public task in relation to the classified information has been eliminated, or the body with public service functions has ceased, the Authority has to contact the National Security Authority in order to clarify matters. The National Security Authority will take care of the completion of the review of classified information, according to Section 20 (2) of Mavtv.

VII.3.4. The content requirements of the recommendation on classification

According to Section 6 (2) (3) of Mavtv., when the originator prepares a recommendation on classification of information, it needs to provide the public interest which is being referred to protect the information from, the level of the classification and the validity of the classification. It needs to contain the facts and circumstances that make the classification necessary.

This is important because the reasons for classification later can be learned from the classification recommendation. This is why it is not enough if the justification of classification is only based on the general extent of damages laid down in Annex 1 of Mavtv.

VII.3.5. Marking the classified information during the classification proceeding

In a national classified information case in 2015 we faced that during the inspected classification procedure the classification recommendation has referred only to a document as matter of the recommendation, the classifier was referring to the classification recommendation. In connection with the incident, NAIH found that it is essential for the right to access public data and legal certainty that during and after the classification proceeding it should be clear which data is affected with the classification of national classified information. Hungarian secret control rules are based on data principal, not documents, but data can be blocked from public view with classification decision. This is why the Authority considers, that even the classification recommendation needs to contain the data designation, despite that Section 6 (3) of Mavtv. does not require it pronouncedly. We believe that it is not sufficient if the classification recommendation only refers on a single document, because – as we already mentioned above – the grounds of the classification decision later can be known from the classification recommendation. For the enforcement of the right to access public data, the restriction which permanently deprives an information or document from the public, cannot be considered in line with the Constitutional Law. The restriction can effect only that part of the information which it really requires. Restriction to access every data of public interest in a certain document when only a part of the data is restricted is unacceptable.

NAIH finds that during the classification proceeding, failing to point out the classified data is such a procedural error that the only way to correct it is if in the classification decision, the classifier makes clear which information is affected by the classification decision.

VII.3.6. Can a data in the same time be defined as classified information and as not classified information as well?

This question was raised when NAIH was investigating a case in which the legality of interrelated classification proceedings were investigated. The proceedings were carried out at the same body performing state or local government responsibilities, and has affected the same information. Some of the classifications were earlier dissolved by the classifier, but one classification was upheld. As a result, one of the classification inspected by the Authority was a classified information, but another copy of the information was in a document which has already lost is validity of classification. On this point, we have made the following observations:

- According to Mavtv., the classification subject of the national classified information is the data, not each copy of the data, that is to say not its occurrence on a data storage device. The decision of the classifier needs to affect every appearance of the classified information during the classified data procession done by the controller, independently of its occurrence in certain documents. A data cannot be classified information and not classified information in the same time.
- Section 2 (1) of Mavtv. sets out the necessity and proportionality of classification. Section 5 (2) c) requires the classification as stipulation of classifying national classified information. If the classifier later dissolves the classification of a national classified information, it means that the restriction of access to the information is not needed anymore. This effects every occurrence of the information, regardless to which document it appears.
- On this basis, NAIH founds that if the classifier classifies the same information in different classification proceedings, and later dissolves the classification in one of the documents, then it needs to dissolve every other classification of this information.

VII.3.7. The data content of the reasoning of classification

The decision on classification of national classified information puts the lid on the fundamental right to information. It may be done only on legal basis. The restriction of rights needs to be justified subsequently as well. As mentioned earlier, reasons of classification can later be known from the proposal itself if the classifier accepts the terms of the classification. Otherwise - according to Point 2 of 29/2014. (IX.30.) decision of the Constitutional Court, "*according to Article VI. (2) of Fundamental Law on right to freedom of information, it is a constitutional requirement in relation to Section 6 (4) of Act CLV of 2009 on Protection of Classified Information that the classifier, if departs from the classification recommenda-*

tion, its decision on classification of information needs to be substantially justified in detail, out of which the grounds of restriction of publicity needs to be stand out particularly."

NAIH experiences that the recommendation on classification is often missing during classification proceedings, and also there is a lack of detailed written justification. This happens usually where many classified information is being dealt with (law enforcement agencies, national security agencies). Usually the classification recommendation contains only general information which are set out in Annex 1 of Mavtv. as extend of damages within levels of classification. The individualized justification of recommendations is associated with high administrative workload, this is why it is important that Mavtv. created another legal instrument. With the help of Section 6 (8) of Mavtv. the Authority can subsequently explore the reasons of the classification decision.

The Mavtv. does not set out, how detailed the justification of classification decision needs to be, so NAIH requests the following details from the classifier:

1. First it needs to be clarified, which publicity of information is being restricted by the decision of the classifier. The identification of the data storage device is not enough in which they secured the classified information during the proceeding, but pointing out the publicity of the data content which is affected by the classification I also crucial. This is because the subject of the classification is the data, and only in the context of specific data content can be judged whether the classifier has rightly recognized the correlation between the information and the public interest protected by the classification (the need of classification), and also whether the level of the classification was determined properly.
2. The necessity of the classification has to be pointed out. This shows whether the classifier has made the classification within its role and competence.
3. Showing the adverse effect on the public interest if the protected information would be published within the validity period of classification.
4. The detailed reasons of the level of classification (showing the extent of damages if the secret is breached).
5. Detailed explanation of the validity period of classification.
6. It needs to be clarified whether the interest in the classification is more important than the public interest in the accessibility of data.

VIII. NAIH's international cooperation

Speaking of our international relations, foreign guests, delegations who visited NAIH in 2015 came mainly from Asia – China, Japan, and Vietnam – and were interested in freedom of information and its legal instruments.

The biggest international news – next to the EU data protection package mentioned earlier – was the so called "Schrems-case", which fundamentally effects the transfer of data abroad (mainly to the USA).

VIII.1 The "Schrems-case"

The Austrian Maximillian Schrems asked Facebook to provide information on his personal data which was processed at the company and faced that endless number and different personal data was recorded by Facebook. Then he submitted a complaint against Facebook at the Irish Data Protection Commissioner (DPC), as Ireland being the country where Facebook has its European Headquarters, asking to check whether the company had processed his personal data according to European rules. The DPC rejected the complaint, saying there was no case to answer in regard of the Safe Harbor plea. That status was called into question by the 2013 Edward Snowden revelations, and the question referred is whether a member state, such as Ireland in this case, is in that event bound by EU law granting the US Safe Harbor status. Or, alternatively, may (or must) the relevant office holders of the member country pursue their own investigations in the light of factual developments in the Safe Harbor agreement.

On 18 June 2014 the case in the Irish High Court was referred to the Court of Justice of the European Union (CJEU). In its judgement (Judgement in Case C362/14 Maximillian Schrems versus Data Protection Commissioner) the CJEU has held, that the Safe Harbor brought by the European Commission cannot restrict or overwrite the investigation of national data protection authorities in relation to data protection provided in third countries. Secondly, the Safe Harbor agreement is invalid, as the European Commission has not investigated the whole legal system of the USA in regard of EU data protection guarantees, that is ignored the US authorities' – especially secret services – nearly unlimited cognitive privileges.

According to the court's decision, the satisfactory resolution of the situation would be if the United States within its own law or by international agreement would

make the data protection guarantees (required by the EU) enforceable. Voluntary agreements do not constitute enough protection when third countries legislations require the opposite. Requesting data from EU citizens on grounds of public interest or national security interest raises difficult issues.

It will be decided in 2016, that the European Commission and the US government can reach an agreement on such a system. If not, it may be expected that the national data protection authorities of the Member States will carry out coordinated procedures to examine data transfers to third countries, with special attention to the United States. The procedures will also examine the different legal solutions like general terms and conditions (SCC) or binding corporate rules (BCR), on how acceptable they are when laws of other states make them possible to be played out.

VIII.2. Budapest Drone Conference

Drones are small aircrafts originally developed for military use. Their task is aerial surveillance, usually by taking images and recording videos. Today, both in the European Union and in Hungary are appearing in increasing numbers, despite the general lack of national and EU regulations in this matter. In addition, military, law enforcement, commercial, academic and private use are also known and widespread.

Since 1990s, European data protection authorities are continuously dealing with the impact of drones on privacy, since these tools – especially since they have become almost fashionable – can much seriously affect our private lives than closed-circuit cameras. The observations made by drones are imperceptible, intrusive and continuous, moreover, the device itself is also available for anyone to purchase.

On 5-6th February 2015 NAIH organized a scientific conference in this matter with hundreds of attendants. The conclusions of this conference can be summarized as follows: the civil use of drones are favorable within the commercial, government and industrial sector, and also for private individuals.

But even the legal use of these things can threaten the individual's privacy. The processed data is atypical and it is also connected with control of personal data so "privacy by design" and "privacy by default" principles have special importance in this matter. Control is absolutely necessary on both European and national levels, where data protection provisions should be presented.

Recognition technology with a neutral solution is important during civil use, exceptional attention should be paid to transparency and adequate information, and effective anonymity, and masking, blurring technology needs to be developed for the protection of privacy of individuals, in compliance with the principle of data minimization. NAIH's recommendation on data procession with drones can be found at: http://naih.hu/files/ajanlas_dronok_vegleges_www1.pdf

VIII.3. International projects

VIII.3.1. Arcades-project

„ARCADES" means „introducing dAta pRoteCtion AnD privacy issuEs at schoolS in the European Union".

During 2014-2016, the project supported by the European Commission with the participation of the Polish, Slovenian and Hungarian data protection authority and the Vrije University in Brussel aimed to create a unified set of teaching aids which might help in this regard as nowadays the youth encounter more and more spying and data collecting devices and other new technology appliances which put the privacy of the most vulnerable–young people–at risk.

In October 2015 the Handbook for teachers was created (in detail: http://naih.hu/arcades/dokumentumok.html) and disseminated to 200 Hungarian teachers within a two-day seminar, where "the best data protection class" contest was also published for Hungarian schools.

VIII.3.2. The Macedon-project

As recognition of NAIH's international activities, a decision was made that the consortium of Slovenian IPS Institute and NAIH, led by the Hungarian Vialto Consulting Kft. has won the tender called „Support to access to right on protection of personal data in Macedonia (EuropeAid/135668/IH/SER/MK)". The tender's aim is the development of protection of privacy in Macedonia. The two-year period gives NAIH's professionals a great opportunity to hand over their experience and knowledge to a country's data protection authority which is catching up to EU legislation levels. Main themes are modern data protection conceptions, usage of modern data protection strategies like built-in data protection, the balance be-

tween information rights, the aspects of privacy for international justice, social relations, and the management of the economy of organization.

VIII.4. Citizens' request for information in connection with the Schengen Information System (SIS)

The SIS, as the system controlling security risks stemming from the abolition of internal borders and the tightened control of external borders is operating with strict privacy standards. Its compliance with these standards are monitored by the European Data Protection Supervisor (EDPS) and by Member States' data protection authorities. If anyone would like to get information whether its data is stored the SIS, or would like the correction of its data or requesting the delete of its data can submit its request to any police department, government office or Hungarian embassy. These requests are being evaluated by the SIRENE Office, who can refuse the information where appropriate, but needs to inform the client about the legal basis of the refusal. Against the decision of the SIRENE Office, revision can be requested at NAIH.

In 2015, nineteen cases have been submitted to NAIH in this matter (three Hungarian and sixteen foreigners). At one point, the request was aimed to disclose data in connection with a third person, to acquire its citation address and file a damage claim against the person. The Authority informed the requesting party that data cannot be acquainted about third persons in SIS-II nor at the Hungarian, nor at foreign law enforcement authorities. Only delegated authorities for law enforcement purposes are eligible for this.

VIII.5. Participation in the work of international bodies

VIII.5.1. Participation in the work of Article 29 Working Party (WP29)

VIII.5.1.1. Cooperation subgroup

In 2015 the Article 29 Working Party has decided on the creation of a subgroup helping the cooperation between authorities. The leader of the group is NAIH's vice-president. The subgroup has a wide range of tasks, inter alia the conse-

quences of the Schrems-decision or the development of a data dictionary in every language of the EU. The most significant task is to prepare the application of the new data protection rules.

Joint preparation is coordinated via workshops, with the participation of authorities, examination of the one stop shop and other innovations in connection with the data protection package.

Preparatory work is also a task, such as creation of guidelines, sample forms and the website of European Data Protection Board.

VIII.5.1.2. Technological subgroup

This group has created the WP29's opinion on Usage of Drone's, which has proposed recommendations for legislators and manufactures in connection with data protection.

With the cooperation of the industry group of cloud-based IT, the subgroup has analyzed the Data Protection Code of Cloud-based IT developed by industry collaboration. Formal approval of the Code did not happen, but it has been recognized that the Code helps the adequacy of the EU data protection expectations. The subgroup has also provided the forum for online data processing, connection with the big international data controllers, data protection risks in connection with new technologies etc.

VIII.5.1.3. International Transfers Subgroup

According to the amendment of the Privacy Act, data controllers established in Hungary are entitled to grant the protection of personal data through BCR's approved by NAIH. The Authority, to attend a wide range of reconciliation in connection with BCR's has joined the WP29 International Data Processing Subgroup. Here, the Schrems-case, the invalidation of the Safe Harbor decision and other international affairs have been examined in connection with binding corporate rules.

VIII.5.1.4. Borders, Travel and Law Enforcement (BTLE) subgroup

The subgroup has provided a detailed recommendation on the EU Directive draft, drawing attention to the creation of consistency of concepts, principles, legal instrument (for example, here you will be required to notify the supervisory data protection authority within 72 hours of the data protection incidents, however it

is preposterous that the controller assesses the risks). On several occasions the draft refers to the Regulation in the case, when data processing is not realized on criminal purposes. The recommendation also addresses the problematic distinction between certain categories of data subjects, as well as the protection of rights of minors as the subjects of the data.

WP29's recommendation on the usage of drones was created partly by the subgroup. The subgroup has also dealt with the application of TFTP (Terrorist Finance Tracking Program), passenger data privacy issues, E.U.-U.S.A. data protection framework agreement, privacy issues of cybercrime, details the EU-US Data protection framework Agreement.

VIII.5.2. JSB Europol (Europol Joint Supervisory Body)

By creating the Europol Most Wanted List, in the question of the legal basis the resolution of the Member States were negative. To prevent the Europol being a data controller without legal authority, with a new technical solution, Member States would be able to send the data in question through a content manager software to Europol which would publish the data on the list only. The debut about this continues in 2016.

The JSB has provided its report about the data procession of victims of human trafficking, which drew up the expected levels of compliance with data protection guarantees. The final version of the report is available at:
http://www.europoljsb.europa.eu/media/276812/thb%20version%2007adopted%20jsbeupol030615.pdf

Various strategic agreements exist between some members of the private sector and the Europol. Europol's Cybercrime Centre (EC3) used information from firms providing Internet services (for example, virus research firms), the analysis of these results will also be shared with Europol. In practice, some companies providing online services can filter suspicious behaviors based on different algorithms, and when sufficient data is available to be transmitted – even as an attachment of an accusation – to the police. The JSB made it clear, they are aware of the fact that in the fight against cyber-crime there is often no need for personal data processing in order to analyze the perpetrators of methods, such as a virus source code analysis does not involve personal data service. However, there are concerns about providing data to Europol which has not been requested, so the scope of the information available needs to be the responsibility of the national units.

According to the Europol-draft, the JSB Europol as an independent inspection body ceases – its recommendations will continue to be in force – and the task of the secretariat will be taken by EDPS.

VIII.5.3. SIS II CSG (SIS II Coordinated Supervision Group)

On 9th April 2013, the 1987/2006/EC on the establishment, operation and use of the second generation Schengen Information System (SIS II) has entered into force and establishes a joint coordination type inspection team, which was formed as SIS II coordination inspection team in the course of 2013. Interesting discussion topics in 2015:

The US Global Entry (for a simplified entry for frequent travelers for fee) program has only two members from the EU (Germany and the Netherlands) so it is advisable to implement its monitoring at national level.

The erasure of data of stolen cars which therefore are on the wanted list, stored in SIS II system generated discussion.

According to the CSG' view, for example, the data of vehicles identified during roadside checks need to be deleted from the system, since the purpose of the data processing binds to the identification and seizure of the vehicle. This goal is achieved by the confiscation of the vehicle, further data processing has no legal basis, and the data should be deleted.

The SIS II system operator eu-LISA agency informed the Working Party that in connection with personal data processing, now it is possible to apply the so-called „terrorism-related activity" as well, which is a broader category than terrorism and refers to complicity.

The EDPS ha sent its report (carried out in February 2015) on data protection inspection to the data protection authorities of Member States which contains mostly technical recommendations for the system operator eu-LISA. Out of the report, NAIH has created a short extract and – with the approval of EDPS – has sent out to the SIRENE Office as the Hungarian national data uploader body.

In the Schengen data protection inspection of Belgium carried out in May 2015, NAIH's representative has participated as a leading expert. The report of the inspection has been adopted by the Scheval Working Party in October 2015.

VIII.5.4. JSA Customs (Customs Information System Joint Supervisory Authority) and CIS CSG (The Customs Information System) (Coordinated Supervision Group)

The JSA Customs future, as the inspector of processing data of EU's "old third pillar" is not yet clear, it may cease after 1th April 2017 and the role of its secretariat will be taken by the EDPS. According to OLAF (European Anti-Fraud Office), the number of active users of the customs information system has increased up to 8000 users. A new function, "restricted visibility" is now available, so the data upload can select the persons who can later access data.

The CIS CSG consists of Member States' data protection authority representatives and the members of EDPS. EDPS has reported on the CIS and FIDE inspection, according to the final report, most of the recommendations have been fulfilled at the system operator OLAF.

In 2017, the Registered Export System (REX) will start, where export activity of businesses and private individuals will be recorded, the data of businesses who are doing taxable activity between Member States and third countries.

VIII.5.5. Eurodac CSG (Eurodac Coordinated Supervision Group), VIS CSG (Visa Information System Coordinated Supervision Group)

The Eurodac CSG was informed by eu-LISA, that the growing number of fingerprints stored in the system the software had to be updated to increase the storage size, and also the Eurodac Change Management Group was set up to monitor the system's technical background. Under the new system, with more advanced algorithms the identification and treatment of the injured finger prints will be easier.

The European Union Agency for Fundamental Rights (FRA), in relation to each Member State statistics raised the problem of inaccurate/outdated data, and that they might contain sensitive data as well. A uniform decision of Member States is required in this matter.

The VIS CSG working group was informed by eu-LISA about the latest statistics of the VIS system: most data is provided by France, Spain and Germany, the most queries arrive from France, Spain, and Poland.

On quality of fingerprint recordings has been also presented in a table of statistics, which stated how many good and bad recording are done by each Member States.

VIS CSG prepared is report on its operation, which contains NAIH's report as well.

VIII.5.6. PCC SEE (Police Cooperation Convention for Southeast Europe Secretariat)

PCC SEE Working Party took place between 16th and 18th of December 2015, a propose has made for the Council of the European Union to help the conclusion of the implementing convention set out in Article 33 of PCC SEE. This would provide a legal framework for exchange of criminal records. NAIH is also part of the subgroup dealing with this issue.

VIII.5.7. The Convention No. 108

The preparation to reform Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Protection of Individuals with regard to Automatic Processing of Personal Data adopted in Strasbourg, on 28 January 1981 (Convention 108) is going on for years (now, EU's reservations impede the finalization of the text). The Convention is the first international document in the field of data protection that is legally binding, and now being joined by 47 states.

In 2015 the Convention's Advisory Committee Bureau (TP-D) – in which NAIH has also became a member – dealt with important general issues, such as air passenger data records (PNR), a single legal framework for tax and administrative purposes of international automated data exchange agreements, the fight against terrorism, and Big Data.

Contents

Nemzeti Adatvédelmi és
Információszabadság Hatóság

1125 Budapest, Szilágyi Erzsébet fasor 22/c
Postal address: 1530 Budapest, Pf.: 5

Phone: +36 (1) 391-1400
Fax: +36 (1) 391-1410

Internet: http://www.naih.hu
e-mail: privacy@naih.hu

Published by: National Authority for Data Protection
and Freedom of Information
Translation: László Czebe
Reader: Julia Sziklay
Publisher: Attila Péterfalvi, President

ISSN 2064-3098 (Printed version)
ISSN 2064-3128 (Online)