Annual report of the

National Authority for Data Protection and Freedom of Information

of 2014

B/3002.

National Authority for Data Protection and Freedom of Information
Budapest, 2015

Preface

Welcome to the Reader!

2014 signalled the knowledge in the fields of technology and data protection. All devices are growing to be increasingly smarter around us: phones, watches, vehicles and even perhaps our fridges. Have also users become smarter acting cautiously? Do we consider, upon downloading an application, transferring a considerable amount of personal data from our phone in exchange for service advantages by a single button press? Do we supervise our children when paddling on a tablet or smart phone, surfing on the net or chatting on social sites?

I believe it is of crucial importance for domestic and foreign privacy officials and experts to focus on the state-of-the-art technologies affecting privacy and to protect personal information in our fast-developing world. This conclusion is affirmed by a statement on the perils of societies under surveillance adopted by data protection authorities at an UNESCO summit in Paris last December. Our authority, beyond investigating individual complaints concerning data protection and freedom of information, kept giving high priority to children's privacy rights in conjunction with the "Key to the internet" project and also did not let drones fly over our agency as we examined the challenges these machines pose to privacy in our recommendation. We have been passing on our knowledge and experience, gained during daily practice, to the public on conferences as well as in the framework of data protection expert courses held at Eötvös Loránd University. Meanwhile our Authority's core activity maintains momentum. The Investigation Department continued to protect fundamental rights based on the ombudsman values whilst the Administrative Department sanctioned infringements by imposing financial penalties.

Following the initial experiences of 2013 the data protection audit procedure has become more popular. We faced an increase of queries in 2014 though several data controllers were enquiring after the procedural steps only and postponed their application to 2015. The increasing number of interests clearly shows that the audit lived up to the expectations; it not only raises awareness among data controllers but also provides an efficient tool to have their data protection related documents and procedures reviewed by qualified privacy experts. Data controllers involved in the audit mechanism were satisfied with our procedure either many or few suggestions had been formulated in our audit assessment report. The proof of the achievement of this mechanism is that after a successful audit in 2013 a data controller had his subsequent data processing process audited by our authority.

Anyway, I wish to commemorate a remarkable anniversary as well. Even though it does not belong to the present annual report, You, Honourable Reader, will take this publication in 2015 therefore it is inevitable to remember the commencement of the ombudsman era which dates back to 1995. Data protection ombudsmen from that date as follow: Dr. László Majtényi (1995-2001), Dr. Attila Péterfalvi (2001-2007), Dr. András Jóri (2008-2011). The National Assembly elected the first commissioners in June 1995, including the data protection ombudsman, and the work began in September of the same year in the Budapest shared office, in Tüköry Street. The basic elements of an operative office had to be created from the scratch, we had to hire employees, respond to dozens of complaints received from the very beginning, review of draft bills and sets of secret lists(?) and perform expert-level consultations. It was a busy but productive period that we will keep in our good memories. Afterwards came the time of consolidation when the both domestically and internationally welcomed new institution advanced to taking a firm root, that is to say, the Hungarian society got to know the new agency

and “used” it in a smart way with a view to protect their information rights, what’s more, the administration as well as professionals were eager to turn to the Data Protection Commissioner for advice, even beyond their legal obligation to collaborate. The organization, however, has progressively “outgrown” its frames by 2011, the classical ombudsman role, based primarily on the means of persuasion and mediation, has increasingly been improved with enforcement powers; finally the legislation decided, in the course of the ombudsman reform process, to transform the institution into data protection enforcement authority, both in terms of its name, organization and status. This “extraction” was not free from conflicts and lot of criticism was voiced even from experts, however, I am convinced, both as the first President of the Authority and former Data Protection Commissioner, that as a result of these changes the protection level of informational rights has been more powerful and effective. The reason is simple: now we possess strong enforcement powers rather than “soft”, ombudsman-like tools to tackle infringements and accomplish prevention. Nevertheless our Authority, in its legal practice, continues to rely on ombudsman-like interpretations, the procedures concerning protection of data of public interest still resemble the original methods and in the field of the data protection the legal protection has become clearly stricter. I do hope the Honourable Reader, consulting our website continuously and reading our annual reports, will also be satisfied that this statement is truthful.

Budapest, 3rd of March 2015

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

I. Statistical figures and remarkable activities of the Authority

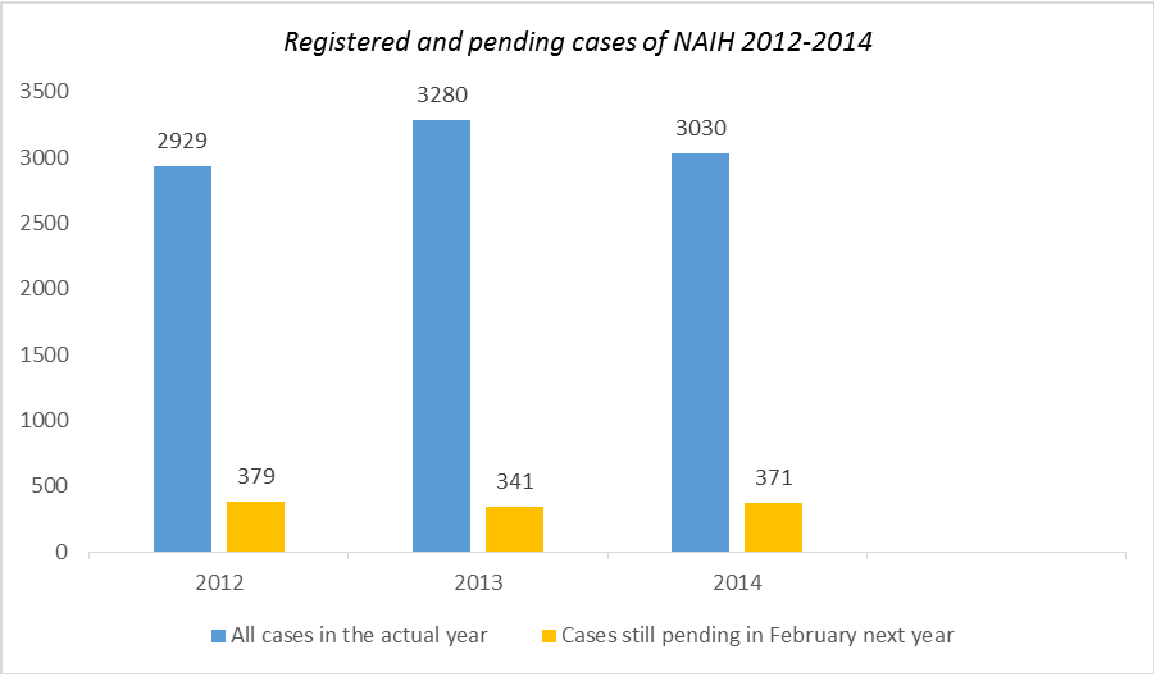
I.1. A statistical summary of our cases

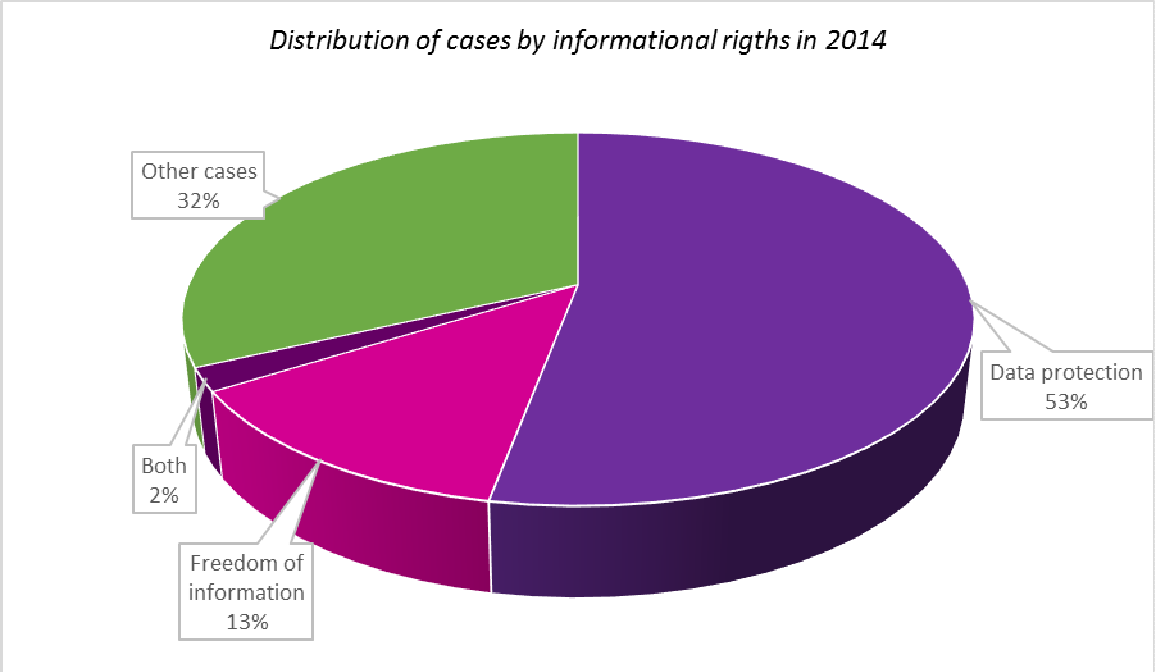
This chapter provides a statistical overview of the year 2014, the third year of the operation of the National Authority for Data Protection and Freedom of Information. Thus we have the opportunity to arrange the statistics of the preceding three years into times series and to get an insight into the actual trends. The subsequent data reflect only on quantifiable activities, however, we need to take into account that several significant and important duties in our work cannot be expressed in sole figures. These include customer service, rendering service both by phone and in person, consulting activity; the number of all these soars exponentially as well as attending conferences, workshops and giving presentations. In 2014 we had to perform a great task in organizing the registration of data processing activities regarding election procedures, processing applications and responding to enquiries in writing and by phone. We keep on placing particular emphasize, beyond our general functions, on our commitment to even provide assistance and guidance, either in writing or orally, in cases which do not affect the terrain of informational rights or the core competences of our Authority.

In the year of 2014 we had altogether 3030 registered cases which was less by 250 than those in the preceding year, however, more by 101 than those in 2012. We received altogether 9950 notifications for registration into the data protection registry; out of them 9624 were new applications, 297 modification requests and 29 deletion requests. Out of the new notifications 2437 came in by post and 7187 via e-mails, that is to say, two-thirds of notifications were registered and processed electronically.

In 30 cases out of the total 3030 data protection administrative procedures were launched. In some of these procedures multiple data controllers were involved, i.e., in certain single cases numerous organizations became subject to these procedures. 2026 cases out of all incoming submissions were handled as investigation cases, the additional 1004 cases associated to other competences of the NAIH (consultations and enquiries concerning data protection registry, reviews 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”.

2260 cases from the year 2014 could be completed until 1st of February 2015; thus a total of 371 files remained from the previous year which, in terms of scale, equals to numbers from the preceding year. Consequently 88% of cases could be settled in that year.

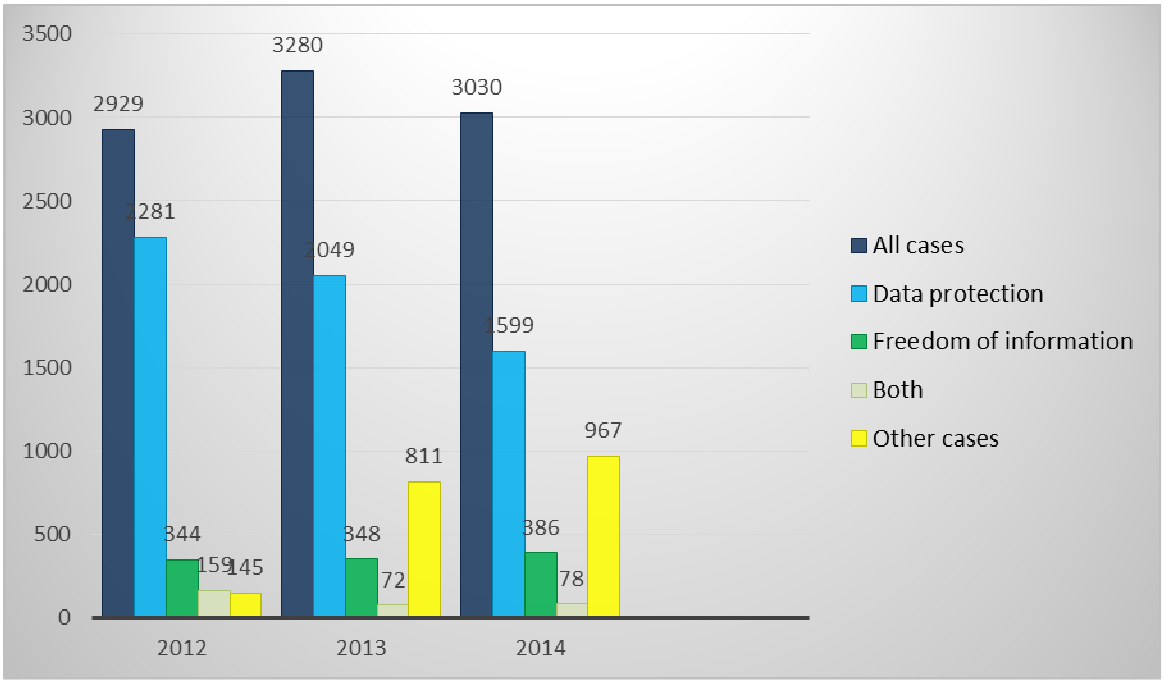




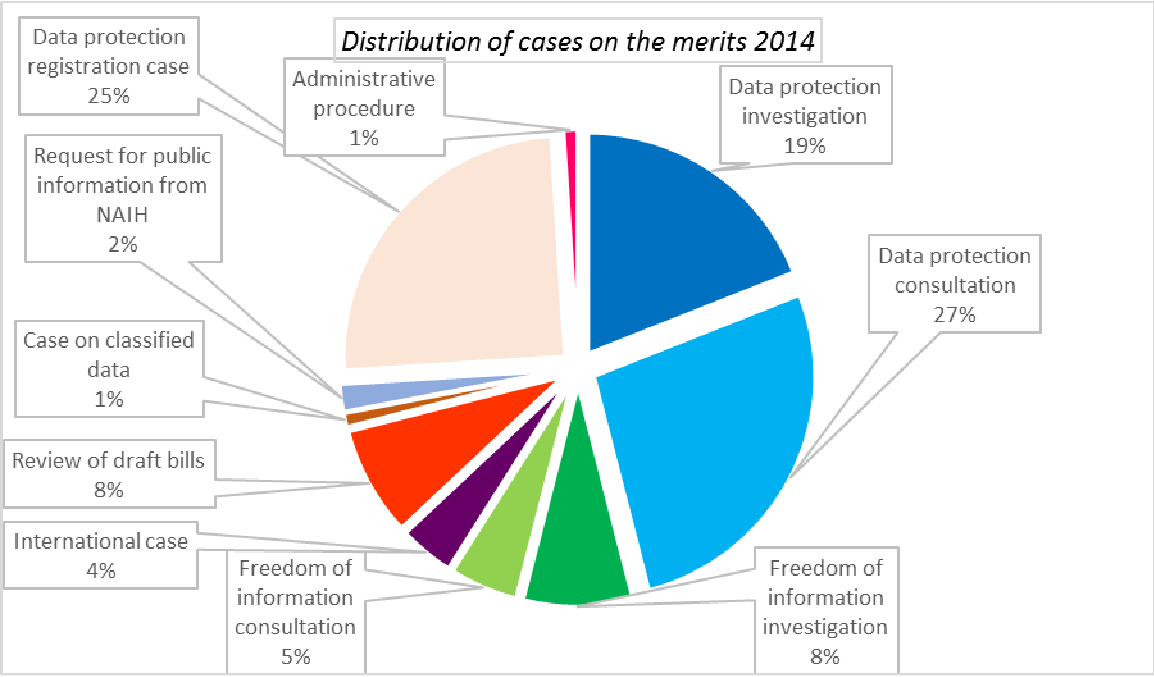
According to the Privacy Act the Authority shall be responsible, among others, to supervise and promote the enforcement of the rights to the protection of personal data and access to public information and information of public interest. The above chart depicts the Distribution of files by information rights; you can see that the high volume of registration and relating consultation cases (691 files) are defined in the other category. As a result, the distribution of caseload by information rights as follows: 1.599 cases (53%) relating to data protection, 386 cases (13%) relating to freedom of information, 78 cases (2%) affecting both information rights, other files that belong to the competence of the Agency: 967 (32%). Consequently, we had altogether 464 (15%) complaints concerning the right of access to public information. This figure clearly shows an increase in incoming cases compared to that of 420 in 2013, both in terms of quantity and proportion.

It is obvious that the number of cases did not vary significantly; though it exceeded the figures of our first year, 2012, the Distribution of the caseload changed in 2014. Data controllers, seeking to comply with the Privacy Act, do report their data processing activities and, as a consequence, numerous reports would be subject to investigations and thus the number of "other cases" boosted this year.

Distribution of incoming files 2012-2014



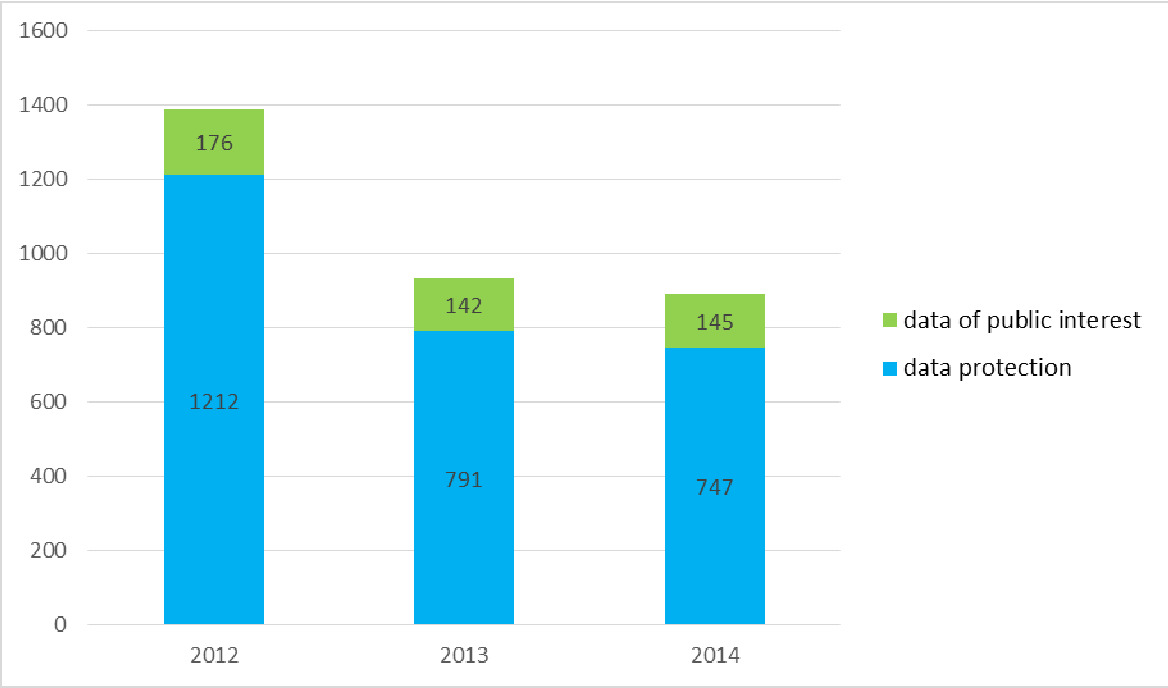
In 2014 we reviewed 219 draft bills, a 30% decrease compared to the previous year which is understandable given that last year we had general parliamentary elections which entails a cut in the pace of legislative work and draft bills. This data is close to that of the 2012 figure (210 reviews). In the course of these evaluations we initiated the amendment of 21 regulations. 31 submissions were transferred to other agencies, 5 out of them to the Fundamental Rights Commissioner's Office. Out of all cases, investigations in 218 data protection files and 58 freedom of information files were rejected which accounts for 9% of our overall caseload. The ratio of these cases remained unchanged compared to the preceding year.



Investigations on the merits were made in 723 cases, 514 of them (72 %) affected data protection and 209 (28 %) involved freedom of information. Infringements were concluded – till the conclusion of this annual report –In 354 investigations, 239 of them revealed breaches related to data protection while 115 infringements linked to publicity of data.

We had altogether 892 substantial consultation cases; where the petitioner, either the data subject or the data controller, requests information and legal guidance on the conditions and legality of an actual data processing activity. Predominantly we faced questions like “Am I entitled to…?” or “How shall I proceed lawfully…?”Consultation notifications were received largely from national or local authorities, private data controllers, social and business organizations. Legal opinions issued in these cases play an important role in enhancing the compliance culture hence progressively contributing to the prevention and elimination of infringements or to the establishment of best privacy practices, what’s more, the broad enforcement of data protection, transparency as well as privacy awareness can be facilitated.747files out of the total consultation cases related to data protection whilst 145 files associated to the disclosure of data of public interest, the obligation of electronic disclosure as well as the affordability of data requests and the technical means thereof. It is interesting to note that the number of consultation cases did not change compared to the files subject to investigation, moreover, their ratio still increased measured up to other cases.

Number of consultation cases 2012-2014



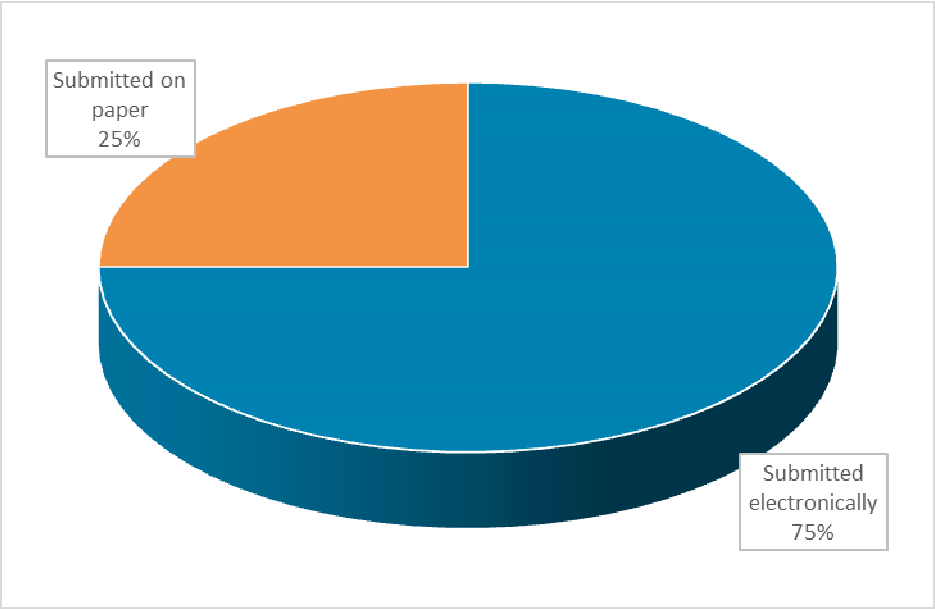
In 2014 we processed altogether 108 international cases, additionally, 11 investigation cases had cross-border relevance (EU or third country data controllers or processors were involved). A total of 25 files included data processing of classified personal data or data of public interest. These sets of cases are outlined in different chapters of the present report. In 2014 we received 41 data requests of public interest; all of them were fulfilled. The number of data requests fell slightly in contrast to the previous year. We also handled 9 data protection audit cases; 5 out of them were actually carried out in 2014.

I.2. Public register of data controllers

1.2.1. Statistical figures on notifications to public register

In 2014 we received 9.624 applications to the public register out of which 7.187 were submitted electronically and 2.437 on paper. The number of notifications sent on paper dropped by half in contrast to the preceding years suggesting that more and more data controllers are using the "NAIH Avatar" framework programme dedicated to notifications which can be found on our website. It is better to send the applications electronically since the transmission as well as the preparation of resolutions is quicker this way and, additionally, the system performs a preliminary check upon completing the form and, thus, facilitates the proper application process. In contrast to the previous years there was no change in the process of applications, amendments or deletions as well as methods of corrections.

Distribution of registered applications



1.2.2. Consultations regarding the public register

In 2014 we received 588 submissions concerning the public register, a large part of which was considered to be consultations. In these petitions clients requested information on the registering of various data processing activities (newsletters, webshops, CCTV operation, "whistleblowing" schemes [reporting cases of corruption]), the completion of data processing reports and the contents of registered data processing processes.

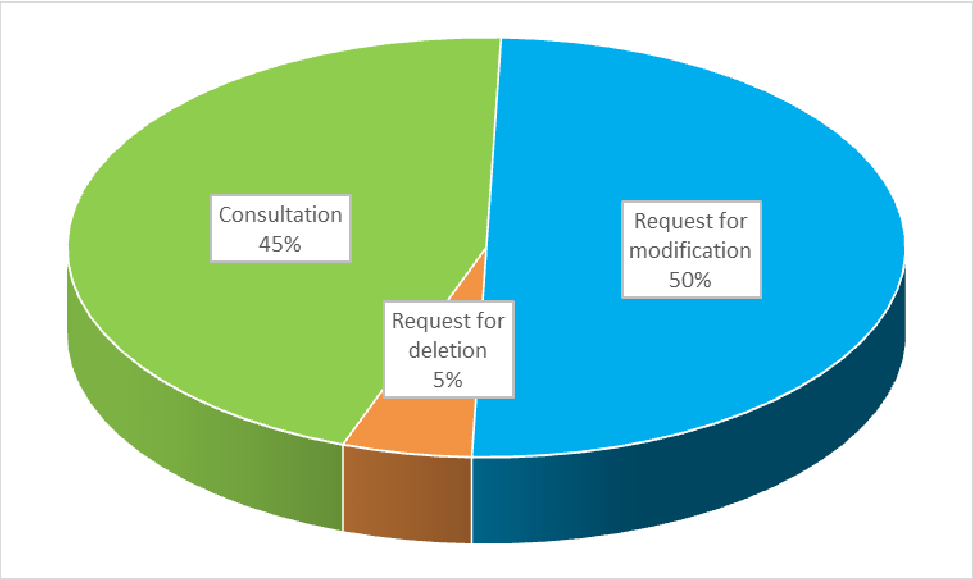
1.2.3. Completion of the form

Although our Authority, with a view to facilitate the correct interpretation of both the law and the practice, published its position of the registration notification on its website on the 20th of May 2014(http://naih.hu/adatvedelmi-allasfoglalasok,-jelentesek.html) alongside with a previously issued detailed form completion guide and a "Frequently Asked Questions" section, receives numerous enquiries in relation to the completion of the form.

1.2.4. Distribution of queries concerning public register

Out of the above mentioned 588 submissions 297 were requests for amendment and 29 for deletion.

Distribution of queries relating to public register



Further we got several inaccurate or insufficient registry forms, at which the common failure is that, in case of a reference to the law, the accurate provisions regarding the legal basis and term of data processing was not specified.

1.3. Rejected requests

Pursuant to Section 14(a) of Privacy Act adata subject may request from the data controller information on his personal data being processed. In these cases the data controller shall provide detailed information about the data relating to him, including those processed by a data processor on its behalf, the sources from where they were obtained, the purpose, grounds and duration of processing, the name and address of the data processor and on its activities relating to data processing, and - if the personal data is made available to others - the legal basis and the recipients. The data controller, however, may deny providing information to the data subject in cases specified in the Privacy Act (national defence, national security, prosecution of criminal offences, protecting economic and financial interests etc.). Pursuant to Section 16(3) data controllers shall notify the Authority of denied requests yearly, by 31 January of the following year.

According to Section 26 of Privacy Act citizens shall have the right to access to the data of public interest and data public on grounds of public interest. Data of public interest shall be made available to anyone upon request presented verbally, in writing or electronically. The right of access to data of public interest, however, may be restricted by the Privacy Act on the grounds prescribed above at the data controller's responsibility (national defence, national security, protecting financial and foreign exchange policy interests, foreign relations etc.). Data controllers shall notify the requesting party on the denial and keep records on the requests refused, including the reasons, and shall inform the Authority thereof each year, by 31 January.

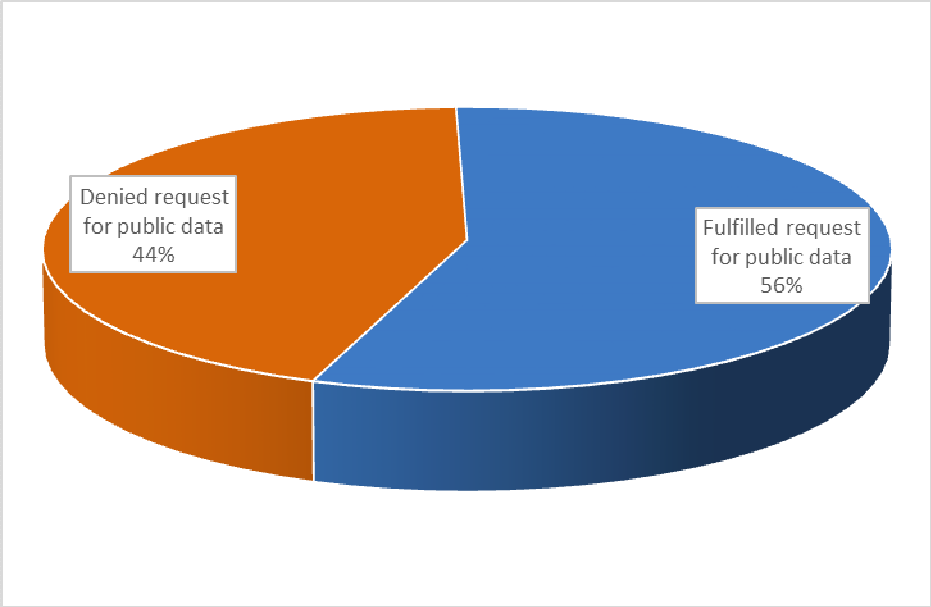
The Authority received 114 notifications on requests for public information relating to the year of 2013. Altogether 50 public institutions informed us on denials containing as much as 424 rejections.

The remaining 64 public bodies, according to their notifications, did not deny any requests in 2013.

Grounds of denials included, but not limited to:

- the request was not related todata of public interest;
- the requested data were not supposed to be published according to law;
- the time limit restricting the publication was not expired;
- the requested data were not processed by the recipient organization;
- the requested document contained classified data;
- the requested data constituted business secrets;
- the recipient organization could not be regarded as data controller relating to the data requested.

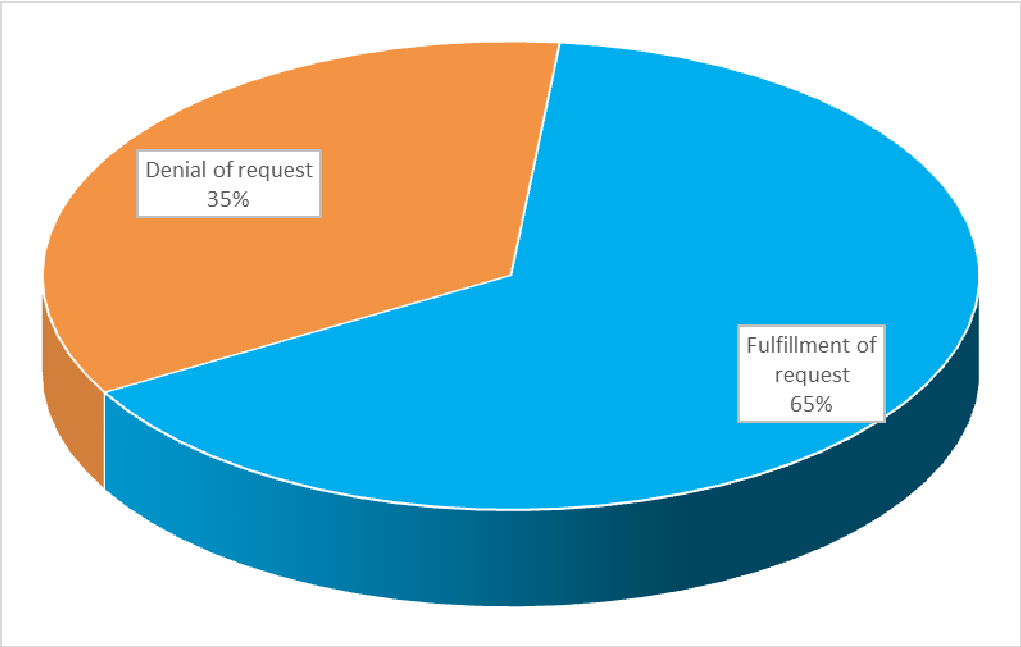
Distribution of performed requests for public information



1.3.2. Denial of requests for personal data processing

In 2013 17 data controllers sent in their notifications to our Authority. 11 out of them had not refused any requests whereas 6 data controllers had denied altogether 126 requests. Since the Privacy Act doesn't prescribe an explanation on the grounds of denial we don't have details about his.

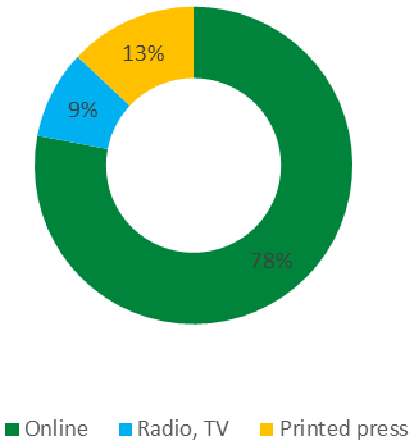
Distribution of performed personal data requests



I.4. The presence of NAIH in the media between 1st of January 2014 and 31st of December 2014

This subchapter summarizes the media presence of our Authority. Between the 1st January and 31st December 2014 the Authority appeared totally 3947 times in the media including appearances in TVs and radios 375 times on 16 stations, in the press 508 times in 64 different editions and on the internet 3064 times on 266 online media service providers.
These media appearances involved oral and telephone statements, interviews, communications as well as reports on recommendations or statements.

Distribution of appearances by media 2014



(source: Observer Budapest Media Co. Ltd

I.5. Conferences, presentations, the conference of internal Data Protection Officers

The President, Vice-President and experts of our Agency held presentations at about thirty conferences.
The Authority keeps paying attention to the activity and support of internal Data Protection Officers (hereinafter referred to as DPOs). In 2014 we organized the DPO conference on the Privacy Day, the 28th January 2014. At the event we presented the activity in the Agency's previous year, our findings as well as the resulting conclusions and trends. The Authority kept dealing actively with the "Key to the internet!" child protection project aiming at providing an enhanced protection to children in the online world. Besides, DPOs were informed on the audit procedure, our experience concerning data protection administrative procedures as well as legal issues arising from actual cases.

The goal of the conference is to set up and maintain regular contacts between DPOs and the Authority that is becoming increasingly important. This is reflected by the fact that the number of participants is increasing year-on-year and, on these occasions, several questions are raised either in relation to the presentations or in other privacy relating fields which facilitates the mutual brainstorming. The conference is also vital to our Authority as thus we can get a feedback on the actual data protection issues and problems to be solved. This kind of consultation enables to create a uniformed legal interpretation and a common practice both in data protection and freedom of information cases.

Beyond the conference, the NAIH strives to give high priority to the submissions and notifications from DPOs. There are clear demands for verbal and written consultations; DPOs regularly turn to the Authority with their queries.

The Agency keeps a record on DPOs with the objective of maintaining contacts and organizing the conferences. In various institutions it is prescribed by law to appoint an internal DPO, but in numerous organizations DPOs are assigned on a voluntary basis. Both (the mandatorily as well as the voluntarily appointed) DPOs are members of the conference.

II. Monitoring of technological developments on fundamental information rights

Pursuant to Section VI(3) of the Fundamental Law the NAIH shall be responsible to supervise and promote the enforcement of the rights to the protection of personal data and access to public information. Therefore the Authority, in its capacity, monitors the domestic enforcement of these rights. Researching the conditions of enforcement of information rights we can identify a complicated structure of aspects including legislation, legal awareness, social values and the acceptance of information rights. Although, beyond the effects of the above mentioned factors belonging mostly to the society, the consequences of the technical-IT development are becoming more remarkable. We can see a rapid improvement in this field which calls for particular attention because the technological development is getting more capable of influencing the everyday life of people, thus changing the interpersonal relations and affecting social relations, including the enforcement of information rights. The technological-IT developments, based on the results of scientific studies and achieved in the circumstances of the market, take form in products and services which meet a genuine need: make people's life easier and safer as well as open up new perspectives in information, entertainment, keeping contacts and work. Though these new technologies have their disadvantages as well that shall also be considered when evaluating the factors impartially.

Assessing the actual trends of development, from a data protection point of view, the following aspects worth mentioning:

The ever faster processing capabilities of computers and the ever bigger data storage devices ensure increasing data processing activities. The novel types of PC processors and storage devices, under a given cost claim, are capable of processing and storing more and more information. The revolution of sensors is unfolding before us: beyond microphones, the image sensors of cameras have become mass market products and can be found, word-for-word, at every turn, i.e., not only in PCs but also in public surveillance systems, in CCTV surveillance systems aimed at providing security services, in mobile phones and similar info communication market products. However it is a novel phenomenon that producers equip the ordinary, so called "smart devices" with new sensors. By these appliances one can collect information on the physical activities, physiological and psycho physiological parameters (pulse ratio, blood sugar level, respiration frequency, reflex time etc.). The operation of these new sensors, during the flow of data processing, can expose an individual's privacy areas in such an extent that had been unavailable for data controllers before.

At the dawn of information technology computers had to be placed into air conditioned rooms. Afterwards personal computers (PCs) appeared at homes. Today, numerous smart electronic products are designed to keep them with the user in bags, pockets or on the body. Appliances which are not to be set up in certain physical locations (machine rooms, offices, apartments) but are supposed to be used for personal purposes, including mobile telephony, e-mail correspondence and visiting social media sites, are gaining ground increasingly. These devices are in more direct and closer contact with the user than a PC. The personal mobile appliances enable the monitoring of the whereabouts and movements of the user. The collection of positioning data is possible in many ways. Some devices contain GPS modules. Mobile phones can be located via cell information. If the smart device connects to a wireless network, the estimated location of the appliance can be determined, given the network termination point. By retrieving data from

the location and movement sensors of smart tools we can also explore whether the user is currently walking or travelling.

The improved capabilities of PCs and sensors, their miniaturisation as well as their becoming cheap mass market products resulted in an unprecedented diversity of info communication appliances. The personal smart devices, discussed before, belong to the first group. The second, quite heterogenic group includes the intelligent household appliances and gadgets which are also equipped with different sensors and, during their functioning, are capable of connecting to the internet or local networks and communicate, without human intervention. For instance, we can mention the so-called smart grids, the introduction of which is presently on the agenda in the Hungarian energy utility service market. In the preparation works the Authority was also involved.

Data processing through the internet is becoming less linked to certain geographical locations. So-called cloud services are expanding which enable both data storage, processing and application services. Various popular e-mailing, social and office applications are supported by these cloud services, in several cases without the users being aware of it. Cloud services, however, bring about new data protection risks and threats:

- services are not blocked by country borders as the personal data can be "anywhere in the cloud". If the actual location of the data processing activity cannot be determined the jurisdiction of states and the regulations to be applied could be in doubt.

- Usually, cloud services are not provided by a single company but several service providers' collaboration is inevitable. Under such circumstances the liability for data processing is also shared by various data controllers. As a result, the difficulties in clarifying the responsibilities make the data subjects hard to exercise their rights, to claim legal remedy for data breaches or compensation for damages from data controllers.

Technological development is driven, however, not only by users' demands but also by the fact that personal data gathered via the new products and services is becoming increasingly significant for multinational IT corporations. This information can be utilized for market research, personalization of marketing messages, and optimization of currently available services, for the planning of novel products and services and data trade.

In our globalized times single states have limited capabilities in developing privacy technologies or setting the direction of the progress. In addition, states are the most frequent users of data processing technologies through the operation and development of public administration, law enforcement agencies, infrastructure system and the extensive state-run social provision system.

There are numerous theories on the state regulator role in the technological field. According to some extremist views the state control and observation, via modern technologies, is tending to intrude into the privacy of people which eventually will result in the emergence of a surveillance state. Others emphasize that countries are using monitoring and data collection methods with the objective of maintaining public order and ensuring public safety, what's more, they are enacting privacy laws and regulations in order to protect individuals from the extreme data demand of corporations and other data controllers. Our Authority doesn't wish to do justice in this matter. Instead, we intend to display our findings in the field of state-run IT technologies in light of our investigations and resolutions of 2014.

II.1. Biometric technologies

There are numerous examples for state-run biometric technologies today, e.g., the records of fingerprints and DNA samples in the criminal records, the biometric data storage in biometric passports or the biometric inspection of visitors of sport events following the recent amendment of sport laws. In 2014 the Ministry of Interior proposed the introduction of biometric technologies in several fields including the issuance of arrest warrants and production of ID cards. In its resolution our Authority emphasized the risks of biometric data control as it has a direct and serious impact on the privacy and data protection. The NAIH, by examining the development of biometric technologies, identified multiple factors which may endanger the exercise of privacy and data protection rights:

- Under market competition conditions the wide scale usage of technological appliances spreads enormously. The society and the legislation, however, need time to realize the effects of this development on information rights as well as to react, with special regard to establishing appropriate regulations. Therefore the imminent danger persists the biometric technologies advance speedily and, as a result, apps become common and widespread to such an extent that they no longer comply with data protection requirements. If this takes place it will become doubtful whether the adverse effects can be subsequently eliminated and reversed.

- The biometric index used for person identification is a record which is directly, ultimately, unchangeably and unquestionably linked to the data subject. Thus the biometric index used for person identification is, by its nature, a unified person identification code. The distribution of universal identification codes, incl. e.g. biometric index data, would contradict the requirements of separated information systems, the theory of which was elaborated by the Constitutional Court, and would successively challenge the system of sector specific identifiers and association records.

- Certain biometric person identification techniques don't require the collaboration of the data subject which allow a covered surveillance. The extensive usage of face recognition gadgets and similar biometric technologies could result in situations where public places and public transport means would cease to be scenes of private life. Everybody could expect being continuously and automatically observed in secret upon exiting the apartment. This situation would obviously harm the privacy and data protection rights. The application of biometric technologies should not pave the way to the secret and general surveillance.

The government has a major responsibility in preventing the increase of biometric technologies from endangering the privacy and data protection rights of individuals. The NAIH proposed the following aspects to be considered in relation to biometric data processing:

- The basic clarification concept is that the biometric index data is not identical with the personal data from which it was created (for instance facial image, signature). As a result, data controllers who are, by law, permitted to process initial data are not automatically authorized to create a biometric index from an initial data and to carry out biometric data processing.

- A prerequisite for the biometric data to become a universal and general identification code is that a reference biometric database covering the whole (adult) population comes

about. Conversely: if there is no reference biometric database covering the whole (adult) population existing, then the biometric profile cannot become a general and universal identification code. Since the application of a general and universal identification code would continue to be unconstitutional, therefore it is necessary to restrict the creation of a reference biometric database covering the whole population.

- It were unconstitutional if a government organization, by means of biometric data processing methods, would monitor the population extensively therefore it is necessary to amend the rules governing the information gathering activity of law enforcement and intelligence agencies so as to prevent his from happening. A legal framework shall be set up in order to safeguard the covert investigation, based on biometric identification or any other kind of mandatory surveillance,

    - not to become extensive;
    - not to become stockholding, even is pseudonym arrangement;
    - to function only for a legitimate purpose specified by law.

II. 2. National Universal Card System (NEK)

Our Authority reviewed the concept and bill on NEK multiple times. The Ministry of Interior, taking over the preparation of NEK in 2014, took into account our comments and recommendations. During discussions we managed to hammer out a consensus over the constitutional requirements with respect to electronic cards in the following basic points:

- From a data security perspective of cardholders it is favourable that the authorisation of card issuance in NEK is conducted in a regulated way. In this regard it is scrutinized whether the card issuing authority complies with the technical, personal and safety requirements relating to the NEK. We have the opportunity to examine the fulfilment of these conditions following the card issuance as well.

- The framework regulation enables the issuance of anonym cards for services for which there is no need to reveal the real identity of the cardholder to the service provider (the card receiver).

- Card receivers gain access to those information, stored on the card, only which have been made accessible to them by the cardholder. This is essential because in the unified card system multifunctional cards can be introduced, on conditions stipulated by law, so that another secondary (virtual) card (i.e., database and functions) is associated to the already (physically) existing primary card.

- When used, expiration date of cards can be queried online from the central system, however, creating log files by this central register is not permitted. That is to say, the central system may not accumulate concrete card usage information that may affect adversely the privacy rights of the data subject, i.e., information from which conclusions can be drawn on habits, interests, consumption, and activity/sport profile of the individual.

- The central register contains the identification information of cardholders and cards separately. Moreover detailed information as for what kind of cards an individual holds

can be revealed only to designated government organizations stipulated by law, for example courts of justice and intelligence agencies, in order to fulfil their duties. Although these organizations have limited access to the central register: they are allowed to get information as to what NEK cards an identified person actually holds.

II. 3. Association codes

The association code is a temporary sequence created with the objective of facilitating and establishing lawful links among different data processing activities.

The Resolution Nr. 15/1991. (IV. 13.) of the Constitutional Court, which laid the foundations of data protection as well declared the universal prohibition of using general personal ID numbers, defined the principle of purpose limitation, the theory of shared information systems and the precondition of collecting personal information from the data subject only with his consent and knowledge as integral elements of right to data protection. Following the Constitutional Court's decision, with regard to the requirements of shared information systems, the identification methods of individuals is of particular importance. The identification methods and codes replacing the universal personal identification number was determined by the Act XX of 1996 (Szaztv.). The Szaztv contains provisions on the association register, the three different special identifiers as well as the linking the register of persons and address records with several other registers via association codes. Besides, additional laws (Act on Health Services, Act on Processing of Health Data) encompass regulations on, partly anonymised, data disclosures to be carried out by means of association codes. Though, unlike the special identifiers, there are no general rules in effect governing the creation of association codes, save the association codes of the register of persons and address records. Hence our Authority performed site checks at data controllers, applying association codes, to inspect whether the creation methods of association codes complies with the basic data protection rules. Pursuant to Section 7(4) of Privacy Act, for the protection of data sets stored in different electronic filing systems, suitable technical solutions shall be introduced to prevent – unless this is permitted by law – the interconnection of data stored in these filing systems and the identification of the data subjects.

If there are no clear data protection safeguards on the creation of association codes defined by law, data controllers, applying association codes, shall outline such kind of rules. It cannot be ruled out that data controllers are creating association codes from personal identifiers of data subjects or from other type of non-volatile personal data. Currently there are no prohibitive regulations that would prevent multiple data controllers from using association codes for different purposes, created from the same personal data with the same methods. In the absence of prohibitive regulations it became also common that data controllers don't limit the use of association codes for a certain data processing programme or for a definite time period but keep on applying the codes for the entire data processing activity.

It shall be noted that if the same association code is linked to the same person in different data processing activities then the association code could become a general identifier and, as a result, would establish the technical conditions for linking different data processing movements.

- A data controller operating in the health sector was scrutinized in 2014. At the end of the investigation we concluded that the association code creation method failed to make the data processing anonymous.

- During the initial legislative work, with a view to ensure the protection of personal data, our Agency suggested that the NEK bill should contain clear rules for the creation methods of association codes in order to prevent that conclusions be drawn to personal data from the association codes.

- The Authority reiterated the need to regulate the creation method of personal data by law upon reviewing the Bill No. T/311. on the amendment of various education laws.

Further cases on the government application of technological developments including the legal implications of data collection by drones, covert information gathering by spywares as well as data retention obligations of electronic telecom service providers are discussed in other chapters.

III. Data protection administrative issues

III. 1. Data protection administrative procedure

In 2014 particular attention was paid, in the course of administrative procedures, to the following data privacy issues – beyond considering launching such procedures based on citizens' submissions:

1. data processing in the field of debt recoveries
2. data processing in the field of sales demonstrations
3. direct marketing techniques

In the year of 2014 30 data protection administrative procedures were initiated, this is more or less identical to the number in 2012 (32) but a little bit less than we had in 2013 (40).

In most cases we investigated not only the single complaints but also scrutinized the whole data processing flows in general. Several cases are rather complex and numerous files have to be examined as there are multiple data controllers involved and, therefore, their operation and collaboration are also subject to investigations. As a result we have a large backlog of files from 2014. In 7 files from 2014 final decisions have been made. In 6 cases infringements were revealed and financial penalties as much as 32.800.000 HUF have been imposed.

In 2014 the NAIH concluded (including cases from the previous year) altogether 18 files, out of which in 17 cases infringements were revealed and in 16 cases financial penalties imposed amounting for 45.350.000 HUF.

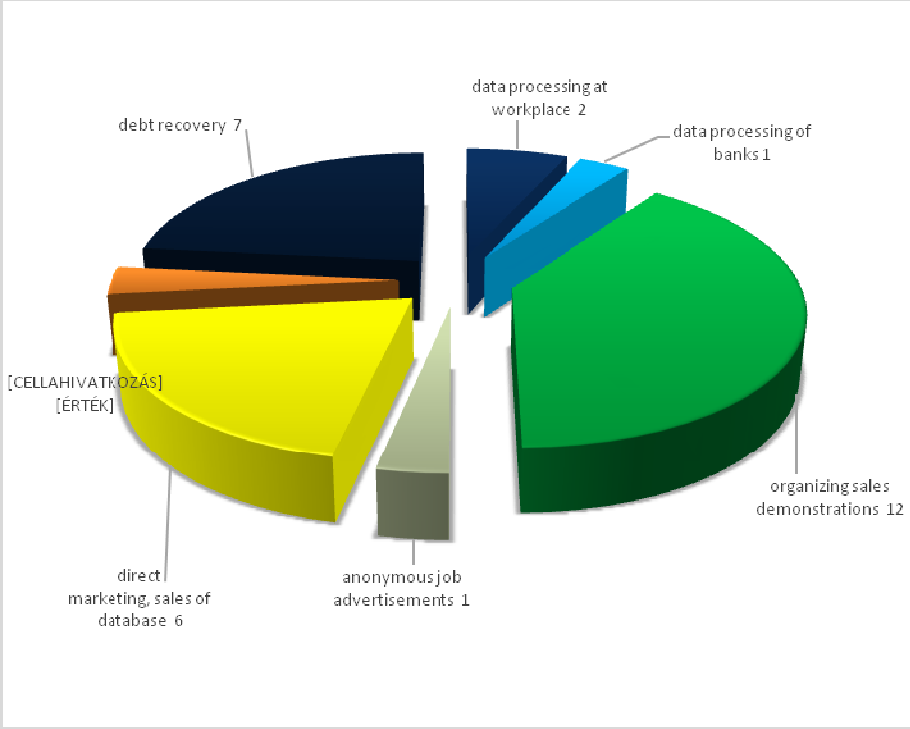
	Number of resolutions/orders	**Number of resolutions imposing financial penalties (out of the preceding cases)**	**Amount of penalties in HUF**
Expanding cases in which a decision was made in 2014	11 resolutions	10	45.350.000
Files of 2014 with a final decision	6 resolutions; 1 order	6	32.800.000
Total	**18**	**16**	**78.150.000**

Distribution of 30 data protection administrative by topics:

- data processing in labour relations – 2 cases
- data processing in the banking sector – 1 case
- data processing at sales demonstrations – 12 cases
- anonymous job advertisement – 1 case
- direct marketing, selling of database – 6 cases

- registration of websites, data processing of minors – 1 case
- debt recoveries – 7 cases

Distribution of data protection administrative procedures by topics



In light of our 3 years' experience it can be observed that the NAIH carried out detailed investigations and, in order to clarify all relevant facts relating to the cases, we employed an IT expert as well. What's more, in the course of spot inspections our legal experts have the opportunity to gain insight into the daily operation of different companies.

The decisions of the Authority serve as a reference not only for the parties to the proceedings but also to other stakeholder institutions in respect of their prospective data processing activities.

Financial penalties imposed by the Authority become due within 15 days following the issuing the final decision. The unpaid financial penalty – that constitutes a public debt enforceable as taxes – the NAIH collects by way of the revenue office.

III. 2. Professional relations with other stakeholders

III. 2. 1. Memoranda of cooperation

With a view to establish and maintain professional relations the NAIH approached two government bodies, namely the Hungarian Competition Authority (GVH) and the Hungarian Central Bank (MNB), and concluded memoranda of cooperation with them. In accordance with these agreements the parties assume to notify each other about cases where overlapping competencies might arise, mutually discuss potential law amendment proposals as well as provide opportunities for joint expert consultations. As a result, proceedings and information exchange could become more effective and flexible in the overlapping cases.

The agreement concluded with the MNB seeks to enhance the coordinated protection of personal data of consumers using the services of financial institutions. To this end, in line with the pact, the authorities may even propose joint investigations.

According to the agreement tied with the GVH the partners annually review and evaluate the state of play in the data-based services market and discuss the fields of potential common actions.

III. 2. 2. Expert consultation on data protection administrative proceedings with respect to sales demonstrations

Based on the findings of 2014 the NAIH organised an expert meeting concerning the infringements and proceedings on sales demonstrations. The National Consumer Protection Authority (NFH), the Health Registration and Training Centre (formerly Health Authorization and Administration Office), the GVH as well as the Consumer Protection Directorate of MNB attended the meeting. The relevance of the consultation has been made by the fact that the above partners keep receiving complaints from citizens in relation to sales demonstrations. In these cases it is very difficult to achieve sufficient results, this topic dates back to decades. In this regard there has not been a comprehensive and broad dialogue among the above-mentioned stakeholders so far. The respective authorities presented their experience and legal competencies. Several experts stressed that the companies holding these demonstrations do not provide (adequate) information (for instance: the terms and conditions of borrowing, data processing, the features of the goods etc.) to the consumers that is verging on the deception and misleading. It is a common practice that the organizing businesses are reluctant to collaborate, hard to reach, they cannot be found at their official seats or do have their seats overseas, trying to conceal their events from the sight of authorities and evade legal liability.

The participants agreed that it is essential to establish a common forum to ensure cooperation and exchange of expertise as well as to share information within the framework of law as this kind of collaboration may lead to more effective investigations of firms in question. For this purpose the parties decided to designate a contact person at each partners with the intention of organizing common actions. They set the objective of rendering information to the most affected data subjects, especially to reach out to the elderly, by other ways of communication, for example, involving even NGOs. What's more, the parties decided to publish information leaflets, news articles and campaign brochures as well as to share resolutions and decisions on sales demonstration cases.

The NAIH is assured that through this expert collaboration the unfair practices can be combatted more effectively.

III. 3. Priority investigation aspects

III. 3. 1. Sales demonstrations

Product sales in the course of a sales demonstration are unusual forms of sales activity whereby customers, given the nature of the transaction, need greater protection, also in terms of data protection. Sales demonstrations bring up mostly consumer protection issues – e.g. right of withdrawal –, however, data protection challenges are also frequent. 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. Our Authority has been receiving complaints from individuals challenging the data

processing of businesses organizing and holding sales demonstrations. Thereby it is clearly visible that this is a long lasting problem involving a large section of the society.

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. Considering former complaints and findings as well as taking into account the above factors the NAIH seized the opportunity, specified in point b) of Section 38(3) of Privacy Act, devoted lots of attention to the issue and launched numerous data protection administrative proceedings in 2014.

It is quite difficult to conduct these proceedings because the companies affected are reluctant to collaborate and "evading" the authorities. The clarification of cases is also hampered by the fact that in numerous situations there are no single company acting as the only controller but an entire network of companies or concerns in complicated relations with each other including purchasing parties, invoice issuers, call centre operators and additional sub-contractors whose agents hold the "presentations." On these events organizers persuade the mostly senior attendees to purchase disproportionately expensive goods with professional marketing techniques, prizes and seemingly attractive borrowing options.

There are several ways of approaching clients: by phone, internet, postal letters, advertisements in the press, distributing leaflets and purchasing databases. As a result they are setting up their own database containing customers' personal data. The main points in these cases are that companies typically obtain the personal details (name, address and phone numbers) of customers from illegal sources, provide false information to the attendees and clients, record and keep too many personal data and their data processing activities fail to comply with the basic principle of fair processing.

The invitations to the events describe the programmes as being "health day", screening test, and free health condition review (e.g. cardiovascular or diabetes checks and risk assessment) which aims at presenting and testing medical devices and examining human organs. Invitations do not say that the "health day" is actually a sales demonstration where organizers seek to convince the attendees about the inevitability of the products and persuade them to purchase, simultaneously holding preventive healthcare presentations. The "health day" impression is strengthened when the organizers ask the participants to bring along their Social Security Card (TAJ card) as if there were some social insurance implications of the event. So rather than providing appropriate prior information but seeking explicitly to conceal the real purpose of the event and the data processing. By doing so they violate the rules of purpose limitation and proper information. Often they have health surveys completed by the attendees or keep records (sometimes infrared camera footages) that the participants do not even know which companies, for what purpose and how long these sensitive information wish to process. Health data constitute sensitive personal data and, as such, controllers must seek informed and written consent from data subjects for processing these information. The law, in any event, doesn't authorize these companies to process health data and, according to the position of our Authority, there is no need for recording health data on these events.

In 2014 the NAIH investigated 12 cases relating to businesses organizing sales demonstrations where 5 decisions have been taken so far. The other proceedings are still in progress.

In the course of investigations we learned that other government authorities, including the National Competition Authority, the Mediation Board of the Chamber of Industry and Commerce and the Consumer Protection Offices of County Government Administrations, are also

scrutinizing almost all companies holding sales demos. In some cases even charges have been filed in the police on the suspicion beyond reasonable doubt.

It shall also be noted that these companies are reluctant to cooperate and their replies to our queries are rather formal, lacking any content as to its merit. If there has been a change in ownership the new executive didn't provide any details on the previous activity of the company, in other cases the change in management has not even been registered in the company records. It may be considered that the main reason for the proceedings to be prolonged is that the clarification of facts becomes difficult due to the reluctant collaboration of data controllers.

Completed proceedings revealed numerous infringements which were common in the practice of all data controllers. Before processing operations are carried out the data subject shall be clearly and elaborately informed of all aspects concerning the processing of his personal data, such as the purpose for which his data is required and the legal basis, the person entitled to process the data and to carry out the processing, the duration of the proposed processing operation etc. The NAIH established in all its decisions that data controllers fail to comply with their above obligations, that is to say, they neither inform, already at the first contact (by phone), the data subjects, the contact details of whom they retrieved from purchased databases, on, at least, the identity of the data controller and the source of the data nor provide sufficient information in the leaflets or application forms with the attendees about their informational self-determination rights. If the clear and adequate preliminary information of data controllers, as a prerequisite for commencing a processing operation, the Authority stipulated the unlawful data processing (missing legal ground) of data subjects' personal data.

The notification on the purpose of data processing is also prescribed by law. If the invitation highlights that the presentation is organized with sales purposes the invitees may be aware of the nature of the event, though, this doesn't even comply with the legal requirements of sufficient preliminary information as defined by the Privacy Act. Invitees, directly approached, are witnessing only at the scene that the event, instead of being a "health day", is held with a view to sale goods and process their personal data. This process is not only deceptive but also unlawful, in terms of data protection. In some instances organizers recorded the ID card information of attendees, upon their entering the event, or obliged the invitees to show proof of their identity. In conformity with the relevant law we concluded that organizers are not allowed to do so.

Similarly we considered illegal the practice when, during the conclusion of a sales contract, much more personal details have been recorded than needed. In this regard the supply of names and addresses of buyers is enough, the recording of further details could be necessary for contacting purposes (additional personal particulars including place and date of birth, ID card number and mother's name may be required in case of purchases on credit, for credit scoring). The NAIH concluded the infringement of the principle of data minimisation when the controller, for direct marketing purposes, processed personal data which were unnecessary (for example place of birth, mother's name).

In various cases our Authority found other types of infringements as well. Several data controllers didn't comply with requests for data deletion, another company published health data along with identifiers on its website. Another controller, violating the principle of fair processing, published a communication on its website pretending that its processing activity had been authorized by the NAIH.

Financial penalties imposed were as much as millions of HUF, except two decisions, with an additional penalty reaching its maximum, 10 million HUF. The Authority always considers thoroughly the circumstances when imposing fines: the character, the seriousness of violations,

the number of persons affected, the factors increasing or reducing the amount of penalties and the revenue of companies (one business realised an income of 700 million HUF, another company, already liquidated, made a profit of billions HUF).

Controllers which received less severe fines didn't operate a call centre, the number of individuals affected was much lower (three thousand and forty-two thousand, respectively) and the infringements were also less serious.

In several decisions, when it came to imposing financial penalties, the NAIH set the goal of general prevention with regard to the frequency of sales demonstrations and to the serious and numerous infringements to data subjects.

We often faced difficulties in enforcing the fines because the companies are seeking to evade paying the penalties, complying with their obligations and trying their best to find a loophole in the process.

The Authority compiled a report on its findings and drew the attention of the companies, interested individuals and the legislation to the difficulties as well as the bad practice encountered and proposed possible solutions.

III. 3. 2. Data processing relating to debt recovery companies

In the past years the over-indebtedness of the people attracted keen and growing interest and, as a result, we have received submissions complaining about the data processing practice of debt recovery companies. In Hungary there are numerous businesses acting in this field.

Debt recovery is a for-profit activity carried out on behalf of the creditor or a third party with the purpose of enforcing an expired and due debt. The aforementioned definition doesn't include legal proceedings in relation to enforcing a due debt (payment warrant proceeding, judicial enforcement).

Investigations completed in 2013 suggested that numerous concerns arose in this field and a large number of individuals are affected therefore we kept on scrutinizing businesses active in this domain.

2 data protection administrative proceedings, initiated in 2013, have been completed in 2014 where we established infringements and imposed fines on corporations involved.

7 new procedures have been launched in 2014 involving 9 companies, out of which in 2 cases has been finalized so far, other cases continues into 2015. In the two finalized files one resolution and one order has been issued. In the resolution we imposed financial penalty on a debt recovery company whilst in another case dealing with a smaller company and acting as data processor by virtue of an agency contract the Authority dismissed the proceeding.

In the case of a factoring and a debt recovery company, the latter acting by virtue of an agency agreement and both belonging to a multinational corporation, we took decisions in 2013 (case numbers: NAIH-625418/2012/H. and NAIH-6254-19/2012/H.). The Capital Administrative and Labour Court repealed our decision and remanded for new procedure on the grounds that the clarification of the facts, with respect to the separate registers and call centres of the companies, the assessment of privacy policies as well as the number of people affected by the infringement, was not sufficient. Although the court pass judgment on the merits and affirmed our position

emphasizing that *"persons other than the debtors are not eligible to be clients, data processing of personal data of third persons not parties to the debt recovery legal relationship violates the principles of purpose limitation and necessity."* Based on the court's ruling the Authority launched a new procedure in 2014. The investigation of the appointed forensic expert is still pending.

Compared to proceedings carried out in 2013 the inspection aspects extended, the major items of which included:

- collecting and recording of personal data of the neighbours and relatives of debtors,
- scope of personal data of debtors,
- preliminary information,
- legal base of data processing, the applicability of novel legal bases [Section 6(1) of Privacy Act],
- the requirement of fair data processing,
- the enforcement of purpose limitation and data minimisation,
- data processing for other purposes and the use of data for the collection of own incomes,
- the position of data controller and processor.

The following important factors and aspects can be highlighted from the above items:

Preliminary information

In light of past proceedings we can draw the firm conclusion that the absence of preliminary information is not a single issue but a general practice of debt recovery companies. We are of the opinion that privacy policies comply with Section 20 of Privacy Act only if they contain not only general provisions on the data processing but also specify detailed, special rules. Data subjects truly don't have access to privacy policies of these controllers, namely the debt recovery companies, from other sources. Without knowing it they cannot assess the rights of the companies and the impact thereof affecting their personal data and, as a consequence, they cannot take an informed decision on the processing of their data.

The legal base of data processing and the applicability of new legal bases

In the course of data protection administrative procedures the Authority shall oversee the compliance with law, in this capacity we shall evaluate the validity of legal bases indicated by controllers.

To this end, the Authority examined whether or not there is a reference to the applicability of the balance of interest [the directly applicable point f) of Article 7 in the EU Data Protection Directive], as legal basis, with regard to the circumstances of data processing, for instance the privacy policy, the information in the data protection register, the information of data subjects. In view of these implications we examined whether or not, in the concrete case, there were conditions under which the principle of balance of interest could have come up.

The Authority is of the position that, during their proceedings, they don't need to examine separately whether or not the legal basis of balance of interest could authorize the data processing in question if the controller investigated based their data processing on a different ground.

Two versions of the principle of balance of legitimate interest are encompassed in the Privacy Act: the one applies when personal data may be processed if obtaining the data subject's consent

is impossible or it would give rise to disproportionate costs, and the processing of personal data is necessary; the other scenario is when the data subject withdrew their consent. But in both cases the controller may have legitimate interests, or s/he may be legally obliged, to process the personal data in question. In this case stricter burden of proof lies with the data controller and s/he has to verify that conditions specified by Section 6(1) or 6(5) of Privacy Act prevail.

In conformity with the legal norms and the internationally adopted principle of transparency data controllers have to verify that their activity is in compliance with the principle of purpose limitation, defined in Section 4(1)-(2) of Privacy Act, and the balance of interest.

In accordance with the Opinion 06/2014 on the "Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC" of the Article 29 Working Party (hereafter: 29WP) of the EU (hereinafter referred to as Opinion 06/2014) a balancing of the legitimate interests of the controller, or any third parties to whom the data are disclosed, against the interests or fundamental rights of the data subject. As a result of the comparison we can learn whether or not the point f) of Article 7 may serve as legal basis.

If the balance of legitimate interests fails to comply with the balancing test, as defined by point f) of Article 7 of Directive 95/46/EC, the data processing shall be regarded by the Authority as unlawful, in conformity with the position of the 29WP.

The enforcement of purpose limitation and data minimisation

In numerous cases the NAIH found that the debt recovery companies, in order to evaluate the willingness of customers for agreement and their liquidity, assess the income and wealth situation as well as the workplace and family conditions of data subjects. According to our findings the dataset processed by debt recovery companies is too excessive.

There is no legal rule in effect which would exhaustively list the information debt recovery businesses may require from debtors, however, the Civil Code, the Privacy Act as well as principles of data minimisation and purpose limitation specify the limits of their data processing activity. If the debt recovery company stores personal data which don't impact the debt recovery procedure, the legitimate purpose is missing, that is to say, its data processing can be regarded as unlawful. Debt recovery companies are not obliged by law to assess the liquidity and financial situation of customers and other individuals, neither the practice and nor the internal rules of these businesses make it necessary to do so.

There may be cases where the financial background and liquidity of debtors may be evaluated because the terms of agreement requires that the debtors comply with certain, preliminarily specified conditions but the companies investigated didn't introduce such kind of decision making process, hence they don't need the personal information in question. The only exception in this regard was a Hungarian branch office of a multinational banking corporation as, acting both as a lending and debt recovery institution, the bank, in accordance with the sectoral regulations, may assess risks not only prior to the conclusion of the lending contract but also during the entire duration of the contract. During the debtor follow-up procedure the financial institution has to monitor the compliance with the conditions including the financial background of the customer.

The data controller and processor position

The Authority, following the examination of concrete agency contracts, has adopted its position as to whether the activity of financial organizations acting as agents should be regarded as data processors only.

In order to determine in what cases the debt recovery organization has been appointed to function as processor and if its activity is truly limited to this operation can be decided only by inspecting the agency agreement itself as well as the operation process. In general it can be observed that the debt recovery practice of debt financial companies that they perform not only technical processes with personal information obtained in the framework of agency agreements but they also utilize them, irrespective of their principals, and take independent decisions within the given legal context.

If principals delegate some specific tasks to their proxies, the data controller position of both parties continues to exist, during the entire length of mandate. Thus, if the terms and conditions of data processing are developed by multiple data controllers, then, in line with the prevailing court practice, all controllers shall remain liable for the lawfulness of the whole data processing and, as a result, in debt recovery proceedings both the principal and the proxy shall be considered as controllers, as highlighted above.

However the proxy, beyond their data controller functions, can operate as processor as well if they carry out obviously technical procedures under the sole supervision and instructions of the controller (e.g. sending payment notices based on the principal's templates).

Data processing for other purposes and the use of data for the collection of own incomes

The inspection of agency contracts drew attention to other types of claims. It is a general practice that debt recovery companies make use of clients' data, beyond collecting the debts of their principals, to recover their own incomes and impose the costs thereof onto the debtors without having a legal relationship with them. Although the organization informs the debtors in writing that the claim stems from the principal or continues to conceal the composition of the fees. The contract concluded by the parties contains provisions on the fees and they strive to charge them to the customers, "over their heads." As a consequence, the debt recovery company enforces its claims as if it were that of the principal thus unlawfully confusing the purposes of data processing. This unfair income-generating method could be revealed by enforcing fundamental data protection principles, especially the purpose limitation.

In case of enforcing revenue which belongs to the proxy rather than the principal the debt recovery company (proxy) process personal data for its own purposes which activity is separate from that of the principal and, as a result, a distinct data processing activity takes place. The Authority investigates each data processing independently. The principal, in the absence of an authorization for data export, has to obtain consent from data subjects for every single data processing activities distinctively.

III. 3. 3. Recommendation and legislative proposal

As described above, the law does not contain specific provisions regarding the debt recovery activity, there are no special rules for this kind of data processing. This situation may lead to different and contradictory practices. This can, in certain cases, jeopardize the enforcement of

information rights. In light of this experience the NAIH deems it important that, in terms of data protection, a uniform and lawful practice do emerge in this field. To this end, and taking into consideration points a) and c) of Section 38(4) of Privacy Act, we issued a Recommendation to businesses with the title "Data protection requirements concerning debt recovery and factoring activities" on the 3rd July 2014. This Recommendation envisaged minimal criteria and set forth proposals to the legislation.

III. 3. 4. Direct marketing

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. 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 from 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.

DM companies provide generally the following services:

- marketing letters via traditional postal way,
- e-mail marketing (eDM),
- telemarketing (call centres),
- mobile marketing (SMS-MMS),
- setting up databases.

The Authority examined the DM field and the companies creating and operating databases for the first time. The launch of investigations were justified not only on the grounds of recent complaints but also by our findings in preceding investigation procedures in which numerous petitioners claimed they had received unsolicited marketing messages from businesses to whom they had not given their consents to do so.

The NAIH initiated six data protection administrative proceedings in 2014 where data processing activities of DM companies were inspected; in two of them a decision has been concluded.

The companies investigated create databases by launching prizes on their websites. Personal data processed in these databases include not only basic information – name, sex, date of birth, phone number and email address – but also additional data like family status, number of people and children in the household, their ages, education, occupation, net salary, position, bank name, phone service provider, possession of car or weekend house etc. The number of individuals affected ranged from 40.000 to millions. Data subjects consent to the privacy policy as well as to the processing of their personal data by ticking a checkbox. Marketing activity and sending of promotions have been indicated as purpose of data processing.

The Authority scrutinized primarily the following three DM techniques: eDM, telemarketing and the establishment of databases:

a. In the course of eDM companies send newsletters to designated addressees sorted out from the database.

b. When setting up databases they are collecting personal data, by virtue of a mandate from their partners, in an opt-in model. By consenting to the privacy policy and participating in the prize game data subjects express their consent to the processing of their personal data not only by the company organizing the prize game but also by partner business entities to which their personal information were sent with a view to utilize them in order to sending promotional messages.
c. Personal data are transferred to customers for a certain time period or for a single phone call from their database. If, as a result of the phone call, the interest of the party approached could have been raised the company may process the personal data for its own purposes. Companies don't obtain consent to this service, business party to the "data rent contract" are regarded as data processors and are not listed in the privacy policy, no information is accessible thereof.

Our Authority concluded the following as a result of data protection administrative procedures:

Firstly, data controllers violated the provisions of Section 20(2) of Privacy Act as regards the preliminary information requirement. Data controllers, beyond failing to provide sufficient information on the valid rules on data protection, the duration of data processing or the identity of controllers, didn't deliver satisfactory information on the main purpose of data processing, which is the fact that they are pursuing data trade, that is to say, they are selling personal data for consideration.

The data controller, by urging registration on the website, seeks to create an enormously large database with a view to realize a huge income not only by reaching out to potential customers but also by making direct profit through the selling of the database. The vending of the database is to be deemed as being a remarkable condition and, as such, the privacy policy shall contain information on it.

In our view data controllers are applying a too general, consequently unacceptable, approach when they merely indicate the "*marketing"* purpose in the privacy policy. Marketing activity is a collective term that can take place in different ways that's why the not sufficiently appropriate description may lead to the concealment of diverse data processing purposes and methods.

In relation to services of DM companies the NAIH drew the following conclusions:

a. We didn't find illegal DM practices, the personal data of persons remain in the possession of controllers, they are not transferred to third parties, and newsletters are sent out directly by the controllers without hiring third parties.
b. In the course of establishing databases the controllers and their partners are utilizing the database created during the prize game independently, for their single purposes thus their practice cannot be deemed to be a joint data processing activity but data transfer between independent data controllers.

This processing activity was found to be inappropriate since the above described practice, relating to the obtainment of consent, didn't comply with the rules of the Privacy Act and, secondarily, the Act on Commercial Advertising Activities and Act on Electronic Commerce.

Supplying personal data takes place in order to be involved in a prize game therefore people registering consent to the privacy policy and hence approve the utilization of their personal data for DM purposes. A strict prerequisite for consent to registration should be appropriate preliminary information. Since registering people give a single consent to multiple data controllers when registering, they don't have the opportunity to choose which companies they

give consent to and which they don't. The Art 29WP emphasizes in its Opinion of 15/2011 that consent can only be valid if it is freely given, that is to say, the data subject is able to exercise a real choice; consent has to relate to certain concrete data processing activities and form consents are inacceptable.

Thus a freely given consent also implies, beyond consenting to merely a registration, a real choice as to whether or not the data subject consents to the transfer of his/her personal data being transferred to a third party. If s/he does, s/he can choose from multiple controllers because, in the present case, one single consent is required for data processing activities carried out by totally diverse companies. Since controllers act independently, if the data subject were to deny to some data processing, this action wouldn't hamper the entire data processing activity.

In our view the privacy policy shall be made public in such a way that data subjects do have the opportunity to decide to which data transfer s/he consents.

c. In case of "data rent" for telemarketing purposes, neither call-centres importing personal data nor their principals, the goods of whose they are promoting, are perceived as data controllers by companies investigated.

   If, however, we are inspecting the above mentioned practice whereby companies under scrutiny are controllers and call-centres are functioning as their data processors, one can conclude that this doesn't comply with definitions specified in points 9 and 18 of Section 3 of Privacy Act and Section 10 (1), 10(3) of Privacy Act, respectively, either because the calls are initiated in its own interest or on behalf of the business the goods of which it is promoting. They cannot be regarded as data processors in accordance with Section 10(4) of Privacy Act either for they are all interested in the data processing business activity.

   As a result the Authority concluded that the contracting parties and their principals shall be deemed as data controllers rather than processors whereby the DM companies transferred personal data to third parties regularly and in a large number without proper legal basis.

   The NAIH also investigated whether or not this temporary data processing structure can be performed legally. In this case the legal basis could be the data subject's consent and the necessary preliminary information should be made pursuant to Section 20(2) of Privacy Act. To this end, the controller should specify, as defined at data collection, the companies to which personal data are "*temporarily*" transferred. However, whilst in case of data transferring agreements, the principal giving the mandate to the creation of database receives personal data of persons having registered in the campaign (where the appropriate consent can be obtained), in the structure of telesales data this cannot be achieved as consent has to be given to a concrete data processing activity; data subjects cannot provide consent to a data processing which is unknown at the time of the registration.

   The NAIH drew the conclusion that the data processing practice followed in the course of "data rent" contract contradicts in its entirety to the principles and requirements of Privacy Act.

   The NAIH, in its decision, obliged the companies to pay financial penalties and called them on to harmonise their practices and privacy policies with the law, subsequently to notify data subjects about the changes and ask for a confirmation of consents from the individuals (who confirmed registration) and perform deletions (who didn't confirmed).

III. 4. Court cases

The decisions of NAIH can be challenged before the court. In the administrative lawsuit the Capital Administrative and Labour Court may uphold or repeal the decision of the Authority, in the latter case the court remands for new procedure.

Actions were commenced in seven cases, out of decisions having concluded an infringement in 2014; the lawsuits are pending at the time of composing this annual report. Court decisions were passed in 3 files following the finalization of the annual report from the year of 2013.

The court upheld our decisions in two cases whilst in an additional case our order for the controller to pay fine and modify the bad practice was annulled and for new procedure remanded. One can find a summary of these files below:

1. NAIH-1073/2013/H

Data processing under scrutiny: a complainant had become a victim of a sexual violent offence in 2013 and her name was disclosed by multiple websites. The attorney at law of the complainant approached the editors of the news sites and called on them to remove the name of the victim from all articles, links, press coverages, video footages and archives without any delay. As some data controllers failed to fulfil the request, the attorney lodged a complaint with the NAIH.

Provisions of the decision:

- 200.000 HUF data protection financial penalty payable
- banning unlawful data processing
- initiating the deletion of the possibility of searching for the name of the data subject in internet search engines
- ordering to give sufficient information on the data processing

Action of the plaintiff:

- the NAIH should have issued a notice in conformity with Section 56(1) of Privacy Act, the Authority didn't provide legal redress
- the NAIH didn't clarify the facts sufficiently
- the NAIH interpreted the notion of sensitive data incorrectly

Ruling of the court: dismissal of the case

- Section 56(1) of Privacy Act shall not apply in the case as this provision refers to the investigation procedure prior to the administrative procedure
- unlawfulness persists, fine may be applied
- the NAIH clarified the fact thoroughly

2. NAIH-798/2013/H

Data processing under scrutiny: on a dating website (and on related websites) there were 500 datasheets per homepage where the age of registered users were below 16.

Provisions of the decision:

- 1.500.000 HUF data protection financial penalty payable
- indicating the data controllers identity, specifying their competencies, detailing the data transfer to the controller's partners
- modifying the practice concerning the obtaining of consent
- terminating the practice by which people registering on a certain website automatically registering into other databases as well
- sending advertising emails unlawfully following the deletion of the profile/data
- provisions relating to the acknowledgement in the General Terms and Conditions (GTC) don't comply with the law, namely, neither the consent is freely given nor the determined and explicit consent nor the sufficient information apply

Action of the plaintiff:

- there is no law in effect banning the registration of minors below the age of 16, it is a nonsense to require parental consent and the age cannot be verified
- one can always unsubscribe from newsletters
- the NAIH lacks powers to require the amendment of the internal rules
- the plaintiff felt aggrieved at the Authority considering the number of minor users as an aggravating circumstance
- the financial penalty imposed by the NAIH is exaggerated and it makes the normal operation of the business impossible

Ruling of the court: dismissal of the case

- the statement of consent of minors under the age of sixteen shall be considered valid only with the permission or subsequent approval of their legal representative
- the amount of the fine corresponds with both the Section 339/B of the Civil Procedure Act and the Privacy Act
- the number of 500 minors can be regarded as remarkable
- the amount of fines imposed in other case is irrelevant
- one can make out the aspects of deliberation with respect to the fine from the decision
- the data controller may be called on to perform the necessary steps as determined in Section 61(1) of Privacy Act
- partners having concluded a memorandum of understanding decided on the purpose of data processing jointly, they qualify as data controllers irrespective of their access to the data

3. NAIH-608/2013/H

Data processing under scrutiny: in case of anonymous job advertisements complainants claim they cannot follow up the processing of their personal data after registration and applying for the jobs, they cannot find out who will receive their applications as well as they cannot exercise their

rights as determined by law, that is to say, they cannot request information on, and object to, the processing and they cannot request the modification and deletion of their personal data. According to the controller the website investigated is merely a hosting provider, it doesn't act as a data controller hence it isn't liable for the data processing of applicants.

Provisions of the decision:

- 200.000 HUF data protection financial penalty payable
- modifying the practice concerning the obtaining of consent for sending marketing e-mails
- the data controller performed actions related to data processors only considering the personal information in applications, however, determining the purpose with the advertiser and defining the method it qualified also as data controller
- the consent of the data subject is not freely given, determined and explicit

Action of the plaintiff:

- the NAIH didn't clarify the facts sufficiently
- the Authority qualified the plaintiff as data controller wrongly
- the decision doesn't contain the aspects of deliberation
- the decision suffers from formal defects

Ruling of the court: partial dismissal of the case, remand for new procedure regarding the order for the amendment of data processing practice

- the notification shall outline the subject of the proceeding, the investigated time period is uncertain
- the date of the unlawful action shall be taken into account for the application of a sanction
- the applicable law shall be determined clearly
- the practice of the plaintiff doesn't comply with the data protection requirements set for consent
- the consent shall be requested for each single data processing

The follow-up of the Weltimmo case

The Weltimmo case is not a novelty in our annual report. Its inclusion into the 2014 annual report has been justified by the fact that, with regard to the issues of jurisdiction and applicable law, it was referred to the Court of Justice of the European Union (hereinafter referred to as CJEU) for a preliminary ruling. The CJEU has been asked to consider whether the NAIH had jurisdiction to hear the case and to apply the Hungarian law.

The Weltimmo case, which began in 2012, is a typical example of the situation when the activity of the data controller is designed to provide service to Hungarian customers, however, it formally settled in another country and registered its activity therein seeking to evade Hungarian jurisdiction. In the concrete case all factors of the data processing could be considered as being Hungarian save the registration of the company in Slovakia.

The Authority already provided detailed description in its 2013 annual report about the investigations and findings (infringements) performed relating to the service provider of websites ingatlanbazar.com and ingatlandepo.com. The NAIH, for infringement of several provisions of

Privacy Act, imposed fine on the data controller and ordered him to modify the data processing practice. In the course of the judicial review the Capital Administrative and Labour Court, upholding major points of the decision on the merits and with a view to clarify the facts more thoroughly, repealed the decision of the Authority and remanded for a new proceeding. Although the data controller appealed the court's ruling and, as a result, it was referred to the Supreme Court of Hungary (Curia) which, afterwards, turned to the CJEU for legal interpretation of the case.

In its appeal letter the data controller challenged the jurisdiction of the NAIH. The company is settled in Slovakia, however, its factual activity targeted exclusively Hungary. Firstly, this is confirmed by the fact that the real estate sites of the company were formulated exclusively in Hungarian, consequently, they targeted customers from Hungary. Secondly, on the website one could find real estates only from Hungary. Our Slovakian partner authority didn't receive complaints in this regard. The Hungarian affiliation has been proved by the fact that the data controller specified a Hungarian bank account for the handling of payments. Finally we can conclude the clients were associated with Hungary and the estates advertised were found exclusively in Hungary. The Hungarian link is supported by the circumstance that the Hungarian authorities launched a criminal procedure against the general manager of the data controller on the charge of fraud in the where the investigative authority established, and the public prosecution office emphasized, the company is not present on its official seat in Slovakia, doesn't perform an economic activity, it can be regarded as being solely a "mailbox company."

The NAIH is of the firm view that the practice making it difficult for data subjects to enforce and protect their rights should be avoided. We are of the opinion that one cannot create a right on the official seat of a company, the factual operation shall be taken into consideration as outlined in the Data Protection Directive. The routine, the data controller can evade liability by simply relocating the company to another country, cannot be supported.

The Authority conducted the proceeding and, as a result, took a decision whereby it condemned the controller again and imposed a fine. The judicial review is still pending, however, the procedure is suspended due to the preliminary CJEU process.

IV. 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 the Authority 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.

That being said, the main area of the legislative involvement of the Authority is the reviewing of legislative bills in the form of formal administrative consultations or discussions.

IV. 1. Statistical figures

The number of cases was a third less compared to the previous year as displayed by the chart below.

Distribution of legislative files by year and legal instrument

Legal regulation/year	**2012**	**2013**	**2014**
Act	49	86	33
Government decree	60	89	63
Ministerial decree	70	92	85
Government resolution	12	28	21
Other: (parliamentary resolution, order	16	15	7

etc.)			
Total	**207**	**310**	**210**

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

Statistical figures of remarks on the merits in opinions

Type of remarks	**Number of remarks**
Relating to data protection	145
Relating to freedom of information	21
Other	53
Total	**219**

In order to uphold the high standard of the information rights protection, beyond the decreasing number of reviews, the proactivity becomes more important in our legislative activity. In this spirit, the Authority has been monitoring the legislative process and proposed its recommendations and opinions both to the competent Ministry and the committees of the National Assembly. This characterised our work in 2014 therefore we are taking account, in this annual report, of the opinions in connection to ex officio procedures.

IV. 2. Legislative proposals

IV. 2. 1. The amendment of Privacy Act

The Authority, in the course of its work, continuously collects the information regarding the quality of legislation which were sent to the Ministry of Justice along with amendment proposals to the Privacy Act in October 2014. The topics of the proposal were similar to that of the 2013 which were detailed in the annual report of 2013. However, the content of the proposals of 2014 was enriched by our findings from the preceding year. The novel suggestions included the following three policy objectives:

- compliance with the developments of EU legislation,
- enhancing or maintaining the standard of information rights protection in the face of rapid technological change,
- simplifying procedures with a view to reduce administrative burden on citizens and businesses.

The subsequent proposals can be mentioned:

- Having regard to the fast evolving biometric technologies and the ensuing privacy risks the Authority suggested to set up a more complex and detailed framework for biometric

data processing, including the limitation of the creation of a comprehensive biometric database covering the whole Hungarian population as well as the prohibition of the establishment of a wide-ranging and continually operating biometric surveillance infrastructure.

- We sent our recommendations on the framework of biometric data processing to the Ministry of Interior, too which, acting as a supervisory authority over the police, the civil intelligence services, the register of persons and address records and the central register of ID documents, will be expected to become the core public body applying the biometric systems.
- In order to facilitate the access to public information the NAIH suggested that public bodies with public duties react more quickly and flexibly to data requests if they face with intense demand from individuals; they should publish this information electronically within short time.
- However the Authority 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 Fundamental Law does not empower us with the competence to launch subsequent review at the Constitutional Court in case of infringement of privacy laws. The Fundamental Rights Commissioner (FRC) has the competence to initiate such a proceeding therefore our Authority can approach him if it perceives an information right violation and the proposing of an amendment is not sufficient. Although the professional cooperation between the NAIH and the FRC is excellent, with the purpose of providing the same high level protection to personal data as other fundamental rights have we think it would be crucial to regulate the ties between the two organizations on a statutory level. The subsequent constitutional review procedure of the NAIH could be regulated similarly as defined in Section 3 of the Act CXI of 2011 on the Fundamental Rights Commissioner.

The novel recommendations encompassed the rationalisation and simplification of the investigation and data protection administrative procedure as well as the administrative proceedings for the control of classified data and the registration procedure.

IV. 2. 2. Revision of data retention rules

The CJEU in its judgement declared that the Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks (hereafter: Data Retention Directive) and amending Directive 2002/58/EC was invalid. The Data Retention Directive was transposed into the Hungarian law by the Act C of 2003 on Electronic Communications (hereinafter referred to as: Eht.) consequently the provisions of the Eht. regarding data retention will be challenged. However it does not follow from the CJEU ruling that the Hungarian law should be amended, that is to say the respective provisions of the Eht. should be repealed, the CJEU supported its view with arguments which should be taken into consideration upon assessing the constitutionality of the Hungarian rules. The Curia acknowledged that the fight against serious crime, in particular against organised crime and terrorism, is indeed of the utmost importance in order to ensure public security, the legal means applied disproportionately restricts the protection of privacy and personal data. The CJEU stressed, in its ruling, the lack of specific aspects (relating to certain persons and circumstances) as compared to a general data retention practice. These factors coincide with to a large extent the fundamental principles of necessity and proportionality applied in the Hungarian practice.

The NAIH is of the opinion it would be appropriate to review the whether or not Hungarian regulations concerning the data storage and data retention obligation of electronic communication service providers (ECSPs) for law enforcement purposes are consistent with the Hungarian and European data protection standards therefore the NAIH proposed the amendment of data retention rules with the Minister for National Development (*NAIH-1410/2014/J*).

In another relating case from 2014 the Ministry of the Interior proposed a draft bill for review which sought to introduce the data retention obligation, enacted similarly for ECSPs in the Act C of 2003 on Electronic Communications before, to electronic commerce service providers as well.

According to the position of the Authority the Hungarian Fundamental Law regulates the fundamental rights in conformity with the Charter of Fundamental Rights therefore one cannot ignore the findings of the CJEU declaring that identical legal norms collide with the Charter. However necessary the enactment of data retention obligations for electronic commerce service providers may be, it were adverse if the Hungarian legislation would regulate the issue on the basis of principles that have been rejected by the CJEU (*NAIH-2791/2014/J*).

IV. 2. 3. Revision of e-signature rules on EU level

In 2014 the European Parliament (EP) adopted the draft Regulation (hereinafter referred to as Regulation) on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. With a view for the Regulation to enter into force completely in 2016 several rules need to be adopted which are expected to give concrete and uniform substance on EU level to some general provisions of the Regulation. The NAIH is of the view that the Hungarian data protection practice, in the field of electronic identification and trust services, drew up numerous advanced examples which could be shared with experts involved in the preparation work on EU level therefore the NAIH is willing to provide expertise to government officials of the Ministry of Justice dealing with the folder (*NAIH-1995/2014/J*).

IV. 2. 4. Data processing in misdemeanour proceedings

The director of a health institution complained about the data request of a police department dealing with a misdemeanour case. The data request concerned patients wearing leg prostheses with a view to identify a perpetrator of an offence. The head of the said institution was of the opinion that the data request violated the rules on the protection sensitive (health) data.

The NAIH launched an investigation procedure in the course of which we concluded that the Act II of 2012 on Misdemeanours, Misdemeanour Procedures and Misdemeanour Register (hereinafter referred to as Szabstv.) insufficiently regulates data requests. One cannot find provisions in the Act governing data requests at all. The current practice of authorities in this regard is not consistent and transparent. It is worth mentioning that authorities, instead of lodging a data request, are likely to summon the individuals (the heads of state institutions) in possession of the information, however, these persons did not witness the offence.

Our investigation revealed the Szabs. actually lacks the safeguards which would ensure the enforcement of the protection of personal data in relation to these requests hence the Authority recommended the Ministry of Interior to add a data protection clause into the Chapter X (Taking evidences) of the Act.

IV. 2. 5. Internet data traffic tax

The Authority perceived that the draft bill Nr. T/1705. on amending certain tax laws and the Act CXXII of 2010 on the National Revenue and Customs Office foresaw the introduction of an internet data traffic tax. The NAIH concluded that the said tax would not restrict the access to data of public interest, however, the charge relating to the download of such data could indirectly influence the conditions of access to public information. For that reason we approached the President of the National Assembly in charge of legislative process and drew his the attention to the fact that, since the enactment of the electronic freedom of information law as well as the spread of electronic administration, the access to public information has increasingly been taking place electronically. Also the internet, as an information transmitting medium in the society, has become an essential channel for spreading information and the freedom of speech (*NAIH-2454/2014/J*).

IV. 2. 6. The publicity of data processed by sport associations

In the course of monitoring the legislative work we discovered that an amending proposal, submitted to the draft bill Nr. T/2141 on the founding of the budget of Hungary, intended to enact into the Act I of 2004 on the Sporting Activities (hereinafter referred to as Sporttv.) that sport associations are, except carried out in their administrative functions, not subject to Privacy Act. In view of this the NAIH drew the attention of the Legislative Committee of the Parliament to the fact that, pursuant to Article VI(2) of the Fundamental Law, every person shall have the right to the protection of his or her personal data, and to access and disseminate data of public interest. The basic provisions of this Article are laid down in the Privacy Act that's why it would be unconstitutional if the Sporttv., by excluding the effect of the Privacy Act., would remove the provisions safeguarding the enforcement of basic information rights with respect to data processing of sport associations. In addition, the adoption of these amendments would also undermine the international commitment and the EU legal harmonisation (the requirements of Directive 95/46/EC) obligation of Hungary (*NAIH-2915/2014/J*).

IV. 2. 7. Regulation on the national security supervision

After several years the revision of the national security supervision has satisfactorily been resolved in 2014. Previously, the NAIH signalled firstly data protection concerns to the National Security Committee of the National Assembly in August 2012 when the then draft bill (the subsequent Act LXXII of 2013) sought to introduce a continuous national security supervision. Following the adoption of the amendment the Constitutional Court concluded that the constant security supervision was unconstitutional and, consequently, annulled the related provisions in its decision of 9/2014. (III. 21.). Though the cancellation of certain provisions in the Nbtv. (Nemzetbiztonsági törvény – Act on National Security) brought about internal incoherence which required an additional amendment. The draft bill Nr. T/2077 of 2014 on Amending the Nbtv. and relating regulations, beyond seeking to terminate the internal incoherence, aimed at enacting the notion of national security review. Similarly to the preceding concept of continuous national security supervision the national security review endeavoured to perform national security inspections at any time during the public servant relationship, also during the 5 year intervals, with a view to find out whether or not the person complies with national security requirements.

To this end, the NAIH examined the rules on national security review and informed the President of the National Security Committee of the National Assembly accordingly.

According to the NAIH's view the regulations on the national security review eliminates the concerns and deficiencies for which the former concept, the continuous national security supervision, was thought to challenge data protection aspects. Indeed, the 2014 draft bill defines the personal scope who may be subject to supervision and clearly regulates the cases of possible supervision determining conditions with regard to data protection as well as specifies the officials with the right of initiative. Moreover the scope of personal data subject to processing, by prescribing the completion of a survey as well as by determining the purposes of the supervision, is evidently regulated. Last but not least, the law defines a reasonable deadline for the supervision and requires the ensuing information of the data subject (*NAIH-2351/2014/J*).
The Authority, in following up the legislative work and with a view to promote the enforcement of rights to the protection of personal data and access to public information, seized the opportunity to propose recommendations and amendments to the respective committee of the Parliament in the following bills:

- Draft Bill Nr. T/156 on the Amendment of the Act I of 2004 on Sporting Activities (*NAIH-1387/2014/J*),
- Draft Bill Nr. T/311 on the Amendment of Several Education Laws (*NAIH-1501/2014/J*),
- Draft Bill Nr. T/2250 on Investments concerning the Capacity Extension of Nuclear Power Plant of Paks and other relating laws (*NAIH-2782/2014/J*).

V. Investigation cases – Data Protection

One of the major duties of the Investigation Department is to examine the submissions and consultation requests addressed to the NAIH. These petitions accounted for about 60% of the overall number of registered cases and affect both data protection and freedom of information issues. Officers of this department are also dealing with data protection audit matters.

V. 1. Whistle-blowing systems

On the 1st January 2014 the Act CLXV of 2013 on the Complaints and Notices of Public Concern (hereinafter referred to as Pktv.) entered into force. The Act makes possible for data controllers (employers) to enact codes of conduct and to set up a whistle-blowing scheme for their employees. The main objective of the system is to combat law infringements and corruption and promote ethical company management by enabling citizens to report, in the course of a procedure ensuring the protection of their personal data, unlawful or unethical events they may face.

Last year the NAIH received numerous petitions relating to the interpretation and application of the rules of Pktv. and the employees of the Authority faced various queries in the course of customer service by phone. Hereby we would like to raise the two most frequent issues.

First, several questions were addressed as for how to publish information on the whistle-blowing scheme. Section 13 of the Act stipulates that data controllers shall ensure everybody has access to the code of conduct. Section 14(2) stipulates that data controllers shall publish a detailed description in Hungarian language about the operation and procedure of the system. The NAIH is of the view that data controllers shall refrain from the practice as to disclosing the whistle-blowing notice exclusively on the internal network (intranet) since, in this event, it cannot be accessed by other stakeholders (sub-contractors, suppliers) who also may submit a report. Instead, data controllers shall publish a description about the operation of the system on their website, according to law. The NAIH emphasized that controllers are not required to disclose the whistle-blowing rules on the website in its entirety, without modifications. It is sufficient, too, if data controllers publish an information with satisfactorily specifying all relevant regulations and the proceeding. This method enables the controller not to disclose sensitive information (e.g. business secrets) on the website whereas not undermining the proper functioning of the scheme.

Second, we received numerous signals as for Section 14(3) of Pktv. relating to the ban on processing sensitive personal data in the system.

V. 2. Data requests by the police to electronic communication service providers (ECSPs)

In the past years the NAIH dealt with the data requests by police sent to various organizations and based on Section 71 of the Act XIX of 1998 on the Criminal Procedure Code (hereafter: Be.). The majority of these petitions came from institutions who had been addressed by the police and asked for a legal interpretation of the Be. and Privacy Act.

The most significant data requests included the ones when the police wished to obtain the entire cell information set of a certain geographical point (a mobile base station) for a certain time period. Another telecom provider challenged the police's data request from a different point of view. In its answer the company stressed that the data traffic of the mobile base stations were not stored in the format as per demanded by the police, however, following the selection and systematization, the phone call traffic data "*can be extracted*" from the data retained in accordance with Section 159/A(1) of the Eht.

The police's data requests, based on Eht. and Be., are of particular importance from a data protection viewpoint as the CJEU, in the Joined Cases C-293/12 and C-594/12, ruled in its judgement of 8th April 2014 that the Data Retention Directive[1] was invalid. The CJEU, with this ruling, annulled the EU norm behind the Section 159/A of the Eht. on data retention.

Pursuant to Section 71(1) of Be. the police may approach any business organization for the purpose of demanding information and the requested party shall fulfil the request (or inform the police on the obstacle of fulfilling the request). The Legislator enacted the fundamental safeguards of data protection into Subsections (3)-(4) of Section 71 of Be. According to Section 71(3) the data request may include personal data to such an extent only which is essential in realising the objective. In the request the purpose and the scope of the data shall be indicated. In accordance with Section 71(4) if the requesting party get to know information which is incompatible with the purpose of the data request the personal data shall be deleted.

Hence, in the course of submitting and fulfilling a data request the protection of personal data – particularly the provisions of the Privacy Act – shall be considered. One of the most important basic principles in the Privacy Act is the purpose limitation as defined by Section 4(1)-)2).

Consequently, the police shall precisely specify what personal data and for what purposes are demanded. In addition they shall indicate why this data request is necessary. If it turns out later that, as for the purpose of the data processing, unnecessary and inappropriate personal information have been supplied to the police these data shall be deleted.

As to the lawfulness of the police's data requests the NAIH is of the view that it is irrelevant whether the data request can be fulfilled, directly or indirectly, from the lawfully retained data. All data requests shall be judged upon the provisions of the Be.

Therefore the ECSP shall provide the requested information of a certain mobile base station if the demand complies with Section 71(3) of Be. and the position of the Authority. Section 71(3) of the Be. entitles the service provider to demand from the police:

- a verification that the request covers personal information that is necessary for the purpose only,
- a clear description on the purpose and scope of personal data requested.

Though the Be. does not entitle the service provider to perform a check on the effectiveness and relevance of the data request or to demand from the police to satisfactorily demonstrate its request. What's more, according to Section 159/A(4) of Eht., the requested ECSP shall be responsible for the lawfulness of the data request. This liability includes exclusively the completeness, quality and timeliness.

[1]Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

Besides, ECSPs are allowed to call on the police to delete, in conformity of Section 71(4) of the Be., the personal data used in a criminal procedure which do not support the purpose of the data transfer any more. Should the more precise data request from the police comply with the conditions as set out in Section 71(3)-(4) of the Be., the ECSP shall fulfil the data request, in accordance with Section 71(1) of the Be.

V. 3. Data processing in the financial sector

We received numerous petitions in 2014 affecting the data processing activity of financial institutions. The biggest problem in this field is that either data subjects are not provided with sufficient information as for what personal data shall (or shall not) be rendered compulsory to financial service providers in the framework of their legal relationship or they are given misleading information in this regard.

Data processing (due diligence, statement on ownership etc.) of financial institutions shall, in line with the Act CXXXVI of 2007 on the Prevention and Combating of Money Laundering and Terrorist Financing (hereafter: Pmt.), be deemed as mandatory. Section 42 of Pmt., effective as of 1st August 2013, provides that the service provider must refuse to carry out transactions, following 31 December 2014, for customers with whom the business relationship was established before 1 July 2013 or for customers who failed to appear in person or by way of a representative at the service provider for the purpose of customer due diligence procedures by 31 December 2014 and if the outcome of the customer due diligence requirements specified under Sections 7-10 is not fully available on 31 December 2014.The consultation on personal data with volunteer mutual benefits insurance funds took place in 2014 accordingly.

A health insurance fund with a wide range of clients obliged its customers to make available their Social Insurance Number (hereafter: SIN number) on a client's sheet. The sheet was used in order for the data controller to comply with the due diligence obligation as set out in Pmt. On the sheet, however, a misleading notification stated that the collection of SIN numbers took place as per the requirement of the Pmt. The NAIH ordered the deletion of the collected SIN numbers.

The above case evidently shows that financial institutions shall divide the various data processing activities. In the event of direct marketing, market research or interbank data transfer they shall empower their clients to make statements on the different data processing processes exercising their rights properly.

We received nearly 30 petitions from individuals, who had re-entered the state-run pension insurance funds from private funds, complaining that their personal data were onward processed after the leaving of the private funds. An investigation of NAIH concluded that personal information of former clients can be lawfully processed by the funds until the limitation of enforceability of rights and obligations arising out of the legal relationship. In this regard the Act LXXXII of 1997 on Private Pensions and Private Pension Funds prescribes that such funds shall establish a data storage system capable of frequent retrieval of records specified by law to provide sufficient facilities to ensure that archived materials are stored for the period defined by legal regulation, or for at least five years following termination of the membership of the member to whom it pertains, and that they can be retrieved and restored at any time, containing safeguards to prevent the stored contents from being manipulated or corrupted.

In 2014 the NAIH kept on focusing on the compliance of financial institutions with the requirement of information, e.g. if clients have access to audio recordings of their conversations with the data controller. The NAIH performed several checks as for whether customers, as parties to life or health insurance contracts, receive the copy of the medical expert report or, when parties to property insurance contracts, have access to the damage report or to the expert report in the damage investigation procedure.

V. 4. Telemarketing

The NAIH received numerous petitions in 2014 regarding unsolicited SMS messages and phone calls.

According to Section 160-161 of the Eht. and Sections 22-24 of 6/2011. (X. 6.) NMHH 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.

The currently effective regulations are based on the concept that personal data kept in subscriber lists are freely available for further use. The legislation, however, made it possible for costumers to ban it. Section 160(4) of the Eht. provides that each subscriber shall have the right to require the service provider, free of charge, to be left out from the printed or electronic directory or to indicate in the telephone books that his/her personal data may not be used for the purposes of direct marketing, information, public-opinion polling and market research or to indicate his/her address in the telephone books in part only.

In addition, Section 162 of the Eht. prescribes that applying the automated calling system free of any human intervention, or any other automated device for initiating communication with prospective subscribers, for the purposes of direct marketing, information, public-opinion polling and market research in respect of a subscriber shall be subject to the prior consent of the subscriber. Additionally, no call serving the purposes of direct marketing, information, public-opinion polling and market research may be placed to a subscriber who has declared that he/she does not wish to receive any publicity matter; this prohibition also applies to direct marketing techniques falling outside the scope of Section 6 of Act XLVIII of 2008 on the Basic Requirements and Certain Restrictions of Commercial Advertising Activities (hereinafter referred to as: Grt.), and to any communication that is not treated as advertisement under the Grt.

From the above provisions follows that personal data kept in subscriber lists are freely available for further use, for instance for direct marketing purposes, unless the subscriber has objected to it. ECSPs keep putting a § mark next to the names of subscribers who do not wish to receive such direct marketing (DM) calls.

Pursuant to Section 6(1) of Grt., unless otherwise provided by specific other legislation, advertisements may be conveyed to natural persons by way of direct contact (direct marketing), such as through electronic mail or equivalent individual communications only upon the express prior consent of the person to whom the advertisement is addressed. Subsection (4) of the present Act states that direct mail may be sent to natural persons within the framework of direct marketing in the absence of the prior express consent of the person to whom it is addressed; the advertiser and the advertising service provider, however, are required to provide facilities for the person to whom the advertisement is addressed to unsubscribe at any time from receiving

further advertisement material, freely and at no cost to the addressee. Such unsolicited advertisement material may not be sent by way of direct marketing to the person affected.

The NAIH emphasized that in Hungary the sending of electronic advertisements is regulated by the Grt. and the Act CVIII of 2001 on Electronic Commerce and Information Society Services. According to Section 24(4) of Grt. the National Media and Infocommunications Authority shall have jurisdiction in accordance with the Eht. in connection with any infringement relating to advertisements disseminated by information society services, exclusive of voice telephony services, and by way of electronic communication.
According to the experience of NAIH several companies get access to potential customers by so-called "cold (random) callings" or machine generated callings with DM purposes even in the absence of a phone book. It is also possible that businesses applying DM techniques are not aware that clients might have banned the potential DM contacting options therefore there might be a § mark beside their names. As non-public phone numbers do not appear in phone books (suggesting that the customer has not consented to receiving DM calls) calling non-public numbers basically violates the information self-determination rights of the data subject even if the caller is not aware that the called number is non-public.

In accordance with the law each subscriber shall have the right to require the service provider (landline and mobile service provider), free of charge, to be left out from the printed or electronic directory or indicate in the telephone books that his/her personal data may not be used for the purposes of direct marketing. Although it is not possible for customers to make a general statement to all telemarketing companies that they don't wish to receive calls from any of them. This intention is indicated by the § mark which should be respected by all businesses.

V. 5. The publicity of documents of condominiums and housing cooperatives, the cases of default payment for maintenance fee and the judicial oversight of the notary over condominiums

Last year the NAIH received numerous petitions with respect to the publicity of documents of condominiums and housing cooperatives as well as enquiries under what conditions default payments for maintenance fee may be disclosed. The NAIH keeps on striving to enhance the awareness of fundamental rights of citizens in this regard as well.

In these cases the NAIH emphasized the following aspects. According to Section 28 of the Act CXXXIII of 2003 (hereafter: Tht.) the general meeting of the association shall have exclusive jurisdiction to approve of the association's annual budget and financial report. To this end, it is necessary for the general meeting to learn the figures and balance of the annual budget proposal as well as the contributions and backlogs of owners with their names. Hence, according to law, general meeting members (the owners) shall have the right to find out the default payment of the respective dweller. This information can take place either by inspection or by throwing a closed envelope into the post-box.

The owners, however, shall always respect the personality rights of their fellow dwellers, that is to say, they may not disclose the personal data of data subjects. The disclosure of such personal data contradicts the provisions of Privacy Act and also violates the personality rights. The disclosure of personal data of inhabitants with default payment for maintenance fee on a billboard or online is not authorised by law. Such disclosure would also contravene the principle of purpose limitation as defined by Section 4 of Privacy Act.

In addition to the above further documents of the condominium (invoices, certificates, contracts, agreements, decisions, other administrative or judicial documents etc.) do not fall under the data protection rights and freedom of information rights either because their contents do not affect the privacy and personality rights of the inhabitants.

With regard to the above documents Section 39 of Tht. states that the said papers may be viewed by condominium owners, that is to say, they shall have access to every contract, draft contract or any other document that refer to the whole condominium, particularly its financial condition as all owners are subject to the financial commitment of the condominium.

We shall underline, however, that only those documents (contracts, invoices etc.) may be viewed which relate exclusively to the financial management of the whole condominium. Though even in these cases the owner may have access to those personal and other information only that either refer to him/her or the whole owner community. Consequently all personal information must be covered which are not necessary to learn the financial background of the condominium. The provisions of Privacy Act only protect the personal information of individuals rather than those of legal persons.

The above regulations apply to the condominiums, the data processing in case of housing cooperatives are governed by the Act CXV of 2004 on Housing Cooperatives.

Considering CCTV cameras operated by condominiums it shall be noted that, as a result of the amendment of the Act as of 1st February 2014, judicial oversight of the condominium association's operations, condominium bodies and their operations shall be carried out by the notary. Judicial oversight shall not apply to cases where court or administrative proceedings may be initiated.

V. 6. Data processing of waste management service providers

We received several submissions in 2014 from individuals, companies and local governments relating to the data processing of waste management service providers (hereafter: WMSP). The most frequent enquiries concerned the conditions and scope of data processing by WMSPs. We faced numerous times petitions enquiring after municipal decrees as to whether WMSPs are allowed to obtain the personal data of local residents, and if so, under what conditions.

The public waste management services' shall mean waste management operations comprising part of the statutory public service, covering the acceptance, collection, transport and treatment of waste, and the operation and maintenance of waste management facilities affected by the public waste management services. In order for the WMSP to be able to collect the fees and to exercise the tasks, conferred upon it by the Act CLXXXV of 2012 (hereafter: Hulladéktv.) and local regulations subject to it, the company needs certain personal information from local residents. As a result, the WMSP is authorized to process certain personal data for the implementation of legal obligations on one hand and for the purposes of legitimate interests pursued by the controller (initiating the collection of debts exacted as taxes).

Pursuant to Section 38(3) of Hulladéktv., when so requested by the competent WMSP, natural person property owners shall give, from among their personal data, their forename and surname, home address, habitual residence and contact address. This provision shall be interpreted with point g) of Section 35 stating that the council of representatives of the municipal government shall establish in a municipal decree specifying provisions for the processing of personal data

(natural identification data and home address) in connection with public waste management services. Section 88(4) of Hulladéktv. authorizes the council of representatives of the municipal governments to decree the rules for supplying public waste management services and for access to such services, and the rules for enforcement of the provisions set out in Section 35.

To sum up the above, WMSPs are authorized to process the forenames and surnames, home addresses, habitual residences and contact addresses of data subjects, in that, detailed rules thereof shall be established by municipal decrees.

WMSPs may obtain the personal data directly from the residents, however, this could become difficult if residents fail to respond. In these cases the municipal government shall not obtain personal information instead of the WMSP and to set up a database of residents who failed to respond on behalf of the WMSP. The service provider may turn to the Register of Persons and Residences to obtain the personal information needed for the implementation of legal obligations and for the purposes of its legitimate interests.

V. 7. Data processing in the course of election procedures

From a data protection point of view the general parliamentary election and the preceding campaign is of high priority as, within short time, millions of personal data can be obtained by political parties and candidates. The year of 2014 was particularly remarkable as both national, local and European elections were held as well as the entry into forced of the new law, the Act XXXVI of 2013 on the Electoral Procedures (hereafter: Ve.), was a trial of strength. The NAIH upheld the traditional practice as to notifying the candidate organizations on the data protection requirements[2] to be taken into consideration, to this end, the NAIH discussed the issue with representatives of political parties for the first time with a view to pave the way for an appropriate data protection practice.

The NAIH investigated two topics in this regard: the data processing practice concerning electoral nomination and that of electoral campaign.

With regard to collecting nomination sheets the NAIH pointed out that the privacy of voters must be fully respected, that is to say, giving or accepting remuneration for nomination is prohibited, as is the utilization of nomination sheets for different purposes or photocopying them or creating duplicate databases. The identity of the proposer may not be disclosed. The NAIH acknowledged the legitimate interest of voters in overseeing whether or not the appropriate person is collecting their personal information. For this reason, on the one hand, people collecting nominations should verify their identities. On the other hand candidates and their organizations shall strive to keep an updated record on persons involved in collecting the nominations. A novelty of the NAIH recommendation is that data controllers shall not have their data processing registered with the NAIH carried out in order to collect nominations.

As regards data processing in campaigns, voters shall be notified if their personal data have been obtained either from the central voters register or from the register of persons and residences. In addition, from public phone books those personal information may be collected the owners of which consented to the publication of their phone numbers or who have not prohibited the receipt of submissions for the purposes of direct marketing, information, public-opinion polling and market research. The usage of a calling system applying a number generator is not allowed

[2] http://naih.hu/files/Valasztas-2014-Ajanlas-2014-02-04.pdf

as it may harm the privacy of voters. A calling system using public phone number database may be used only if the database contains only personal information of individuals who had consented to the publication of their phone numbers or who have not prohibited the receipt of submissions for the purposes of direct marketing, information, public-opinion polling and market research or the calls are made following the provision of phone numbers by supporters.

Data subjects shall have the right to interrupt the call. Campaign documents by virtue of e-mail or mobile phone can be sent to voters only who provided these contact details to electoral nominees or organizations with a view to be contacted this way as well. The utilization of databases containing private entrepreneurs or judicial experts for campaign purposes is strictly prohibited.

Unlike nominations sheets, data controllers shall have their data processing registered with the NAIH carried out in order to processing data for campaign purposes. Though a clear distinction shall be made between the general and the unique, special campaign activities.

The NAIH adopted guidelines concerning the contacts with nominee organizations and campaign volunteers. In the former issue the NAIH called on the nominee organizations to appoint a person in charge of contacting with voters regrading data processing. As for the processing of volunteers' data nominees should accept applications from persons only who previously registered in their own database. Those voters' personal data who objected to the processing of their personal information may not be processed in a "negative database". Finally, the primary addressees' shall be reminded that data transfer may take place only with the knowledge and consent of secondary addressees.

A novelty of 2014 has been that the NAIH, in the context of user-friendliness, launched a website prior to the municipal elections in order to facilitate the registry of data controllers. To this end, a template application form, a completion guide as well as a template list of candidates names have been published. Additionally, the NAIH called on the candidates and nominee organizations wishing to run for the municipal and national minority elections of 2014 to initiate the registering of their data processing activities, carried out with the purpose of political campaign, exclusively electronically.

VI. Investigation cases – Freedom of Information

VI. 1. The election procedure in light of freedom of information

Transparency is an utmost precondition of elections and electoral procedures. In the absence of transparency the election results can be doubted, the common belief of citizens vested in the notion of fair procedure will be ruined which, ultimately, jeopardizes the legitimacy of democratic states. Therefore the enforcement of freedom of information is of highest importance.

The novelty of Ve. is that point f) of Section 2(1) specifically mentions, among election principles, the notion of transparency. This an innovation because the former Ve. (Act C of 1997) did not mention it as a basic principle. Section 2(2) of Ve. generally establishes that information at the disposal of electoral bodies shall be, with some exceptions specified by law, public. Section 2(3) states that in the period between the calling of an election and the results of the election becoming final, the provisions of the Privacy Act. shall be applied by election bodies with the

exception that requests for public information and data public on the grounds of public interest shall be met without delay, within no more than 5 days.

The application of Ve. brought about several practical issues, among others the relation between the provisions of Privacy Act. andVe. concerning transparency, which had to be addressed by NAIH.

A municipal government turned to NAIH enquiring whether or not Ve. 2(3) applies to all requests for public information during the election period. The NAIH, in its response, referred to Ve. 2(2) establishing that information at the disposal of electoral bodies shall be, with the exception of personal data and other information specified by law, public. In light of transparency, according to Ve., the provisions of Privacy Act. shall be applied. With respect to request to public information the Privacy Act. functions as a general whereas the Ve. applies as a special rule. That's why Section 2(3) of Ve. is a special rule because the legislation set the short deadline for demanding public information in light of the short election period.

In another case an individual lodged a petition with NAIH alleging that the election committee denied to provide an electronic (scanned) copy of the election minutes. According to Section 204 of Ve. a copy of the minutes may be inspected at the relevant election office for three days following the day of voting. The election committee denied the info request claiming that Ve. contains special rules in this regard. The NAIH, on the contrary, stated that the only special rule is the shorter time period (3 days) and there are no effective provisions in the Act that would limit the enforcement of freedom of information. The NAIH stressed the crucial importance of inspecting the election minutes since these documents contain the final results of elections. Since the election committee didn't refer to the special circumstances as defined by Privacy Act. they denial of information requested had violated the right to freedom of information, therefore, the NAIH called on the electoral body to provide the requested information *(NAIH-973/2014/V)*.

The National Election Office (hereafter: NEO) enquired about the scope of public information, that is to say, whether or not election bodies shall disclose the names of candidate organisations taking over recommendation sheets. The NAIH stated that, pursuant to Section 2 of Ve., the data available to electoral bodies shall be public and electoral bodies shall oversee the legality of recommendations and elections, as a consequence, electoral bodies shall perform such data requests within the time period as defined by Section 2(3) of Ve. (NAIH-781/2014/V.).

We also received a submission concerning the application of provisions regarding pro-active publicity.

A citizen criticized the practice of the Vas County Electoral Committee (VCEC) for the latter failing to send him a resolution electronically initiated by the complainant. The VCEC sent the document solely in postal way and therefore, the applicant alleged, an important deadline for judicial supervision had not been met. In its response the NAIH referred to Section 48 of Ve. saying that the manner of direct communication of resolutions shall be chosen by the applicant and, failing that, in postal way. The decisions, except personal data, shall be disclosed as well though its means is not defined by law and by the National Election Committee (NEC) either. The VCEC informed the Authority that the applicant failed to provide an electronic contact details and the resolution had been disclosed on the billboard of the County Hall, too. As a result the NAIH stipulated there had not been a violation of freedom of information rights though, considering the tight deadlines for legal remedies and the state of the art e-government solutions, it would be advisable for the electoral bodies to disclose their resolutions electronically as well (NAIH-2203/2014/V).

We faced another case where the collision of the publicity of election procedures and the protection of personal data of candidates had to be removed.

A public notary approached the NAIH enquiring whether or not the home address of municipal election candidates may be disclosed. The NAIH referred to point b) of Section 46 of Ve. which says that the resolution on registration of the candidate shall contain the name and home address of the said candidate. Although, in examining the issue, the content of the ballot paper shall also be taken into account. Ve. stipulates that ballot papers shall contain the name of the candidates only. Consequently, the NAIH concluded that the disclosure of home address of independent candidates violated the data protection rights of data subjects (candidates) (NAIH-2666/2014/V).

The NAIH emphasized multiple times that Section 2 of Ve. refers to information processed by electoral bodies only which relate to election procedures. Provisions of Ve. on data processing not related to election procedures shall not apply, in this case the Privacy Act. and other regulations have to be taken into consideration.

VI. 2. Transparency and the funding of election campaigns

The Hungarian State Treasury (hereafter: MÁK) turned to the NAIH enquiring whether or not names of candidates and nominating organizations subject to the repayment obligation of financial support may be disclosed. In its response the Authority referred to the Section 27(3) of Privacy Act. saying that any data that is related to the central budget shall be deemed information of public interest and, as a result, not only the names of candidates (and nominating organizations) but also the exact amount subject to repayment shall be disclosed upon request. The MÁK, however, acts as data controller rather than as an electoral body therefore it shall disclose the requested data within 15 days instead of 5 days, as per the Privacy Act (NAIH-1153/2014/V).

A journalist made an enquiry as to whether the financial support paid to candidates and nominating organizations shall be disclosed. The petitioner claimed that the MÁK had denied providing information referring to Section 30(7) of Privacy Act. The NAIH concluded that information respecting financial support paid to candidates and nominating organizations shall be deemed information of public interest. In its reply the Authority cited the Section 30(5) of Privacy Act. saying that if, as regards the refusal of any request for access to data of public interest, the data controller is granted discretionary authority by law, refusal shall be exercised within narrow limits, and the request for access to data of public interest may be refused only if the underlying public interest outweighs the public interest for allowing access to the public information in question (NAIH-1448/2014/V).

VI. 3. Transparency as purpose and means; challenges in the transparent operation of state-owned or municipal companies

The NAIH attaches high importance to the transparent operation of public (state-owned or municipal) companies. In this topic the Transparency International Hungary (hereafter: TI) made a research with a view to explore the attitudes of CEOs (chief executive officer) of public companies to the notion of transparency.

As a result of investigations both the NAIH and the TI found that general managers and chief legal officers of public companies were reluctant to acknowledge even the importance of transparency with regard to the operation of public enterprises whereas the CEOs of private companies clearly supported the basic principle of publicity and the prevention of corruption. Consequently, the first and foremost prerequisite in expanding transparency among public companies is that their CEOs should recognize their being subject to freedom of information. This reasoning is confirmed by the Act CVI of 2007 on State Property (hereafter: Ávtv.).

In case of municipal enterprises we should go back to the provisions of the Fundamental Law (FL). According to Article 38 of FL the Property of the Hungarian State and of municipal governments shall be considered national assets. Article 39(2) of FL states that data relating to public funds or to national assets shall be recognized as data of public interest. Provisions of the FL are supported by the Act CXCVI of 2011 on the National Property (hereafter: Nvtv.). In conformity with the FL Section 7 of Nvtv. stipulates that the National Property is primarily dedicated to ensure the management of public services. According to Section 10(1) of the Nvtv. the Owner shall keep records on the assets of National Property. These records are, with the exceptions of classified data, public. This interpretation has been affirmed by the Resolution 25/2014. (VII. 22.) of the Constitutional Court expanding the notion of public enterprises to indirectly state-owned companies as well. The Constitutional Court confirmed that a subsidiary company under the direct controlling influence of a state-owned or municipal company shall also be subject to the obligation of freedom of information as a company performing public duties.

The NAIH also acknowledged that in certain cases the publicity may jeopardize the effective functioning of public, state-owned companies that's why, in cooperation with the TI, a balanced approach has been developed to ensure both the enforcement of transparency and business interests.

An additional open question is the setting up of a company website which could be useful for both the company and the public even though the Privacy Act. does not prescribe it as an obligation. We think that it would be advisable to establish an own homepage but in case of minor municipal enterprises it is also acceptable if they disclose their public information on the website of the relevant municipality or in the central public information system (www.kozadat.hu).

As for the question whether or not companies managing national properties shall use the same standard publication list as public administration bodies do the NAIH stated already in 2012 that those items of the publication list which do not refer to the activity of the company were not subject to disclosure.

According to Section 37(3) of Privacy Act the Act CXXII of 2009 on the More Economical Operation of State-Owned Companies (hereafter: Kgtv.) shall be deemed as a special publication list. Accordingly, the publicly owned company shall disclose the personal data of executive officers, the members of the supervisory board, executive employees and employees with the right to dispose of the bank accounts of the enterprise and employees with individual power of representation. The CEO of the relevant company shall be liable for the disclosure, the credibility and the continuous access of these information.

Consequently, business interests and secrets shall be limited with a view to ensure the fair financial management, the transparency and the freedom of information rights.

VI. 4. Investigation and law review relating to the extension of the Paks Nuclear Power Plant

Last year the NAIH focused on the publicity of information regarding the Paks Nuclear Power Plant (hereafter: PNPP) as well and, accordingly, criticized the adoption of regulations seeking to limit the enforcement of freedom of information.

The NAIH, as a member of the Aarhus Roundtable and in order to foster the transparency, the rights to access to environment information as well as the involvement in decision-making processes, highlighted the following points concerning Draft Bill No. T/2255.

In relation to the publicity of public information over the upgrading of the PNPP the subsequent international and EU regulations shall be taken into account. Principally the Convention on Access to Information, Public Participation in Decision-making and Access to Justice in Environmental Matters (hereafter: the Aarhus Convention) and the Directive 2003/4/EC on Public Access to Environmental Information. Preamble (24) of the Directive and point 6 Article 3 of the Aarhus Agreement both stipulates that the these legal instruments shall not affect the right of national legislations to maintain or introduce measures providing for broader access to information, however, the Draft Bill appears to limit these rights.

Section 5(2) of the Draft Bill contradicts both the Privacy Act. and the Aarhus Convention therefore, thinks the NAIH, it must be amended on several points.

Pursuant to Article 8(4) of the Council Directive 2009/71/EURATOM, as amended the 8th July 2014, Member States shall ensure that the general public is given the appropriate opportunities to participate effectively in the decision-making process relating to the licensing of nuclear installations. The NAIH, accordingly, recommended the differentiation of various rules governing the access to information, in conformity with the transposition obligation.

We can conclude that the disclosure of environment information do not fall under the Section 27(5)-(6) of Privacy Act. (information underlying a decision)since the preparatory feature is based not only on formal but also on substantial aspects.

In accordance with the practice of the Constitutional Court, documents containing principally drafts or opinions shall be deemed information underlying a decision but environment information do not fall under this term. A recent court decision concluded that an emission metering protocol (quasi advisory opinion) shall not be deemed as a preparatory document underlying a decision but information used to take a decision that's why it shall be public. In our view, in a pending administrative case such a data request for environment information shall be fulfilled.

The NAIH is of the view that the necessity for limitation of access to public information shall be assessed thoroughly. The respect for investors' interests cannot overwrite the right to freedom of information and environment information. In the course of such limitations the NAIH suggests that the provisions of the Fundamental Law as well as the EU and international rules shall be taken into consideration (NAIH-2782/2014/J).

VI. 5. The limits of freedom of information

We received numerous petitions concerning Section 30(7) of the Privacy Act. This provision deals with the so-called "*vexatious data requests*" where we can find several problems.

In case of some municipal governments with small staff it may be realistic that they cannot meet enormous data requests from individuals due to lack of sufficient infrastructure and capacity. In such cases the NAIH can accept the practice if the requested party grants access to inspection for the requesting party [Section 30(2) of Privacy Act.].

It can be concluded that the more government agencies strive to limit access to public information through publication lists the more and detailed info requests they will face. In light of this, and to foster the uniform application of rules, our Authority published a recommendation[3] interpreting Section 30(7) of Privacy Act.

The NAIH established in various cases that even if the data request affects the inspection of copies of invoices the application of Section 30(7) of Privacy Act. shall not be deemed as lawful, what's more, even in these cases Section 30(5) of Privacy Act. shall apply saying that if, as regards the refusal of any request for access to public information, the data controller is granted discretionary authority by law, refusal shall be exercised within narrow limits, and the request for access to public information may be refused only if the underlying public interest outweighs the public interest for allowing access to the public information in question.

Consequently, contracts concluded by a public body do contain public information and therefore, pursuant to Section 26(1) of the Privacy Act., shall be public (NAIH-2604/2014/V).

VI. 6. Compliance with data requests – anybody can approach public bodies with information requests

In the past years we investigated several cases where the requested parties demanded additional identification data from the individuals or, in case of non-governmental organisations (NGOs), the registration document was required so as to fulfil the data request.

According to Section 28(1) of the Privacy Act. there is no need for the requesting party to submit any document verifying his identity. The only requirement is that the requesting party shall submit his contact details in order for the requested party to fulfil the data request. In conformity with the law anybody may submit a data request without the need of providing grounds or his identity for it.

Section 30(4) of Privacy Act. affirms this notion by providing that *"a request for public information by a person whose native language is not Hungarian may not be refused for reasons that it was written in his native language or in any other language he understands."*

It may come up that the data request cannot be fulfilled because the requesting party has not provided any contact details. In each case the circumstances shall be examined thoroughly and sometimes the information requested can be disclosed electronically. Information shall be

[3] http://naih.hu/files/Ajanlas30--7-_V2.pdf

supplied in a readily intelligible form and by way of the technical means asked for by the requesting party.

To sum up, it is irrelevant if the requesting party is a registered organisation or not since the requested party may not verify the identity of the applicant.

VI. 7. Investigations concerning municipal governments

The negative trend as to the lack of sufficient personal resources and infrastructure affected adversely the enforcement of freedom of information continued in 2014. We found remarkable disparities in the practices of various local governments; some of them run quite informative websites whereas others are reluctant to disclose the most basic information on their financial background.

The Authority always respects the lack of resources and the enormous work burden of smaller municipalities which could prevent these bodies from complying with their disclosure obligations, however, even under these circumstances they should endeavour to disclose public information and to effectively cooperate with the NAIH. Where several local governments were unwilling to collaborate in enforcing freedom of information rights our Authority prepared a publicly available report and published it on its website[4].

In this report the NAIH emphasized that it was not mandatory for municipalities set up an own website; the disclosure of public information can also take place on the websites of local governments associations or on the homepage of government offices exercising legal supervision over municipalities (NAIH-4369/2012/V, NAIH-5724/2012/V, NAIH-1921/2013/V, NAIH-614/2014/V, NAIH-419/2014/V) etc.

[4] http://www.naih.hu/informacioszabadsag-allasfoglalasok,-jelentesek.html

VII. Cases concerning classified information

In cases affecting classified information the Authority conducts either an investigation proceeding or an administrative proceeding for the control of secret. Pursuant to Section 62 of Privacy Act. if the findings of an investigation launched upon notification or other evidence suggest that the classification of certain national security information is unlawful, the Authority may open administrative proceedings for the control of secrets. The provisions of the Act on the General Rules of Administrative Proceedings shall apply to administrative proceedings for the control of secrets, subject to the exceptions set out in this Act. Administrative proceedings for the control of secrets may be opened *ex officio* only, and it shall not be deemed to have been opened upon request even if the administrative proceedings for the control of secrets was preceded by the Authority investigation launched upon notification.

Usually the information provided by the petitioner at the beginning of the proceeding are not sufficient to render the unlawful classification of information likely as the additional information needed are not available to the petitioner. These data would become accessible to the Authority only during the procedure.

If the conditions for launching an administrative proceeding for the control of secret are not satisfied the Authority initiates an investigation procedure. The commencement of an investigation procedure is possible because, in case of an unlawful classification, an infringement relating to the personal data or concerning the exercise of the rights of access to public information or information of public interest, or if there is imminent danger of such infringement [Section 52(1) of Privacy Act persists]. Since the legal opportunities of citizens concerning a classification are weak the Authority always initiates an investigation procedure if there is even the slightest evidence suggesting the infringement of national classified information.

Here below you can find some excerpts from the 2014 files.

VII. 1. The Gripen case

The submission initiated the supervision of the classification of a Report concerning the purchase of Gripen jet fighters that was prepared by the then State Secretary for Defence in 2007. The NAIH, in the course of investigation, requested several documentary evidences and reports from the Ministry of Defence so as to clarify the facts.

Major findings

Competence of the classifier

The classifier of the Report was Mrs. Ágnes Vadai, then State Secretary for Defence whose classification rights were delegated from that of the Minister in conjunction with the then effective Act of LXV of 1995 on State and Service Secrets (hereafter: Ttv.).

The classification of the report from formal-procedural aspects

Compliance with the formal classification rules is of remarkable importance since these methods make classification easily recognizable. In the absence of these regulations only skilled experts could detect the classification of data. Though the legal regulations protecting classified information shall be observed generally even if somebody lacks proper expertise. Therefore it is inevitable from the perspective of due process of law to comply with the formal rules of classification. According to the general practice, followed also by the Authority, the data shall not be deemed as classified if the indication of classification is missing.

The classifier failed to indicate the country code MK/HU on the Report. In our interpretation the country sign MK/HU displays the country of origin rather than the secrecy level of the document. Section 5(8) of the Act CLV of 2009 on the Protection of Classified Information (hereinafter referred to as Mavtv.) does not prescribe the use of such country indication that's why the missing country indication does not constitute an invalid classification.

The formerly valid Ttv. distinguished the terms "state secret" and "service secret" which clearly pointed to the classification level of classified information. Classified information could not be created without the "state secret" mark. The classifier failed to indicate the "state secret" mark on the Report hence, the NAIH found, the classification shall be deemed as invalid and no secret information had been created.

As for the Appendix of the Report, it not only lacked the "state secret" mark but other indications, as per required by law, were also missing making the whole classification invalid. Since the classification of both the Report and the Appendix were formally invalid the NAIH did not initiate an investigation on the merits of the documents.

Review of the Report

The successor state secretary of the Ministry re-examined the Report and the Appendix and, as a result, modified the classification into "Top Secret". However, as the former classification was unlawful, consequently no classified data had been created, the subsequent classification modification could not be valid.

Actions of the NAIH

Our Authority concluded that due to unlawful classification of both Report and the Appendix an imminent danger of the enforcement of rights to access public information took place. Therefore the NAIH called on the successor State Secretary to advise those recipients whom the documents had been transferred on the unlawfulness of the classification.

Although the unlawful classification of both Report and the Appendix does not imply the validity of those information the classification of which took place earlier and where the classification were carried out lawfully. Those information require a separate legal assessment. If it can be found that the data are still classified data then those information shall be handled in accordance with the provisions of the Mavtv.

The NAIH called on the successor of the classifier that in case of a request for public information concerning the Report and the Appendix the request shall be fulfilled in a summarized form where the classified information are unrecognisable to the requesting party.

VII. 2. The lawfulness of classification of data public on the grounds of public interest

A citizen turned to the NAIH claiming that his information request over contacts details of executive employees of the Ministry of Foreign Affairs and Trade (hereinafter KKM) had been denied on the grounds that the requested information were classified as secret.

The NAIH found that the requested information were data public on the grounds of public interest because executive employees of the Ministry are persons with public service duties. Pursuant to Section 26(2) of the Privacy Act the name of the person acting on behalf of a body with public service functions shall be considered information of public interest, including his job description and responsibilities, title and other personal data that may be of interest relating to the public function, as well as all other personal data that is to be made public by law. According to point I.3. of the Appendix 1 of the Privacy Act the name and title of the executive employees of the body with public service functions and its departments, including contact information (telephone and fax number, electronic mail address) shall be disclosed electronically.

We had to examine whether or not the KKM acted lawfully when data public on the grounds of public interest had been classified as secret and, as a consequence, the information request was denied.

In accordance with Section 26(1) of the Privacy Act. any person or body attending to statutory State or municipal government functions or performing other public duties provided for by the relevant legislation (hereinafter referred to collectively as “body with public service functions”) shall allow free access to the public information and information of public interest they have on file to any person, save where otherwise provided for in this Act. In accordance with Section 28(1) of the Privacy Act information of public interest shall be made available to anyone upon a request presented verbally, in writing or by electronic means. Access to information of public interest shall be governed by the provisions of this Act pertaining to public information. In accordance with Section 27(1) of the Privacy Act access to public information or information of public interest shall be restricted if it has been classified under the Act on the Protection of Classified Information.

Based on the above provisions the same rules (concerning access, classification etc.) apply to data public on the grounds of public interest as to data of public interest. However there are no clear regulations in the Privacy Act whether or not data of public interest may be classified.

The investigation revealed that point I.3. of the Appendix 1 of the Privacy Act prescribes an immediate disclosure obligation. Neither the Mavtv nor the Privacy Act authorizes the classifier to ignore the legal rules for disclosure. If the data has been published it may not be classified. So, the KKM unlawfully denied the disclosure of the requested information. However, in the meantime, the data was published on the central government website hence the NAIH did not have to take actions (*NAIH-2378/2014/T*).

VII. 3. The application of spywares for intelligence purposes

An individual approached the NAIH and alleged that, based on press sources, Hungarian intelligence services had installed spywares on IT appliances of each Hungarian citizen with a view to control their email correspondences.

Since there are no legal regulations governing the use of spywares we had to draw up a model depicting the functioning of such a mechanism which consists of a target system, a spyware and the intelligence service operating a spyware programme (static model). The dynamic model of the system is made up of the following elements: preliminary (external) approval, the installing of the spyware, data collection and the termination of the application. The so-called data protection impact profile characterizes the effects of a spyware application on privacy the main items of which are the following:

- Spywares, compared to passive methods and means, enable a more intrusive insight into the privacy of individuals because they facilitate multiple use of information collected.
- Spywares enable a targeted data collection. This method considers the application of the purpose limitation basic principle limiting the data collection to the information strictly needed and requires an advanced application usage approach from the intelligence service. Passive appliances, in contrast, are likely to ignore the purpose limitation requirements and to use stockholding data collection means.
- Spywares are not suitable for widespread usage. The more spywares are installed on target systems the higher the risk is that target persons find them. From a data protection perspective this can be favourable as, given the limited capacity of spyware applications, users of these systems needs to consider carefully the usage thereof.

Our Authority, with a view to clarify the facts, took the following actions:

- Attending the closed session of the National Security Committee of the National Assembly twice and receiving information.
- Inspecting the application methods and procedures of covert investigation on the spot.
- Requesting detailed information on the use of spywares in the course of covert investigation from the Director General of the National Intelligence Service (hereafter: NBSZ).

Major findings of the inspection:

- The use of spywares is a covert investigation subject to an external approval. Legal regulations provide adequate safeguards for data subjects concerning the enforcement of their rights to privacy and data protection.
- During the review of the legal background in a different case the need for clarification of the Nbtv. came up: in the course of the external approval procedure the specific task at which the covert investigation would be directed should be specified in the proposal for the covert investigation with so as for the data controller to assess the purposes and methods.
- In view of the rapid technical development in the field of spywares the NAIH has to keep the pace and examine repeatedly as to whether the balance between technological novelties and the enforcement of privacy rights of individuals are harmonised. This is of crucial importance as covert investigations, carried out secretly, prevent citizens from

assessing whether, and if so, to what extent these operations comply with democratic legal requirements.

- Concerns that Hungarian intelligence services are carrying out widespread surveillance operations by means of spywares are unjustified. The NBSZ performs its duties in full compliance with point a) Section 8(1) of the Nbtv. During the inspections no signals suggesting possible infringements were raised.

The report of the NAIH on spywares can be found on our website (*NAIH-1904/2014/T*).

VII. 3.1. The covert intelligence operation of the NSA in Hungary

Similarly, a citizen approached the NAIH, based on press sources, that the National Security Agency (hereafter: NSA) of the United States (USA), in the course of its worldwide intelligence mission, might have collected information on him as well. The NAIH investigation has not confirmed these allegations but, in such cases where foreign intelligence services are involved, this cannot be verified. However our Authority has been aware of the Snowden case revealing a mass information gathering activity of the NSA by compromising global IT networks and companies and, thus, affecting a huge scope of individuals. Although, given the enormous range of potentially affected data subjects and the vast impact of such an operation could have on privacy rights, we could not verify the punctuality and reliability of these information an investigation procedure was launched.

The premise of the investigation was that the Hungarian law did not allow any foreign country to gather information about individuals in Hungary secretly therefore such an activity shall be unlawful. However we shall point to the fact that Section 2(1) of the Privacy Act refers to data processing carried out in the territory of Hungary. The Authority does not have jurisdiction over data processing activities carried out outside Hungary. Though the operation of the NSA, according to press sources, targeted primarily global IT companies in the USA and submarine optical cables. According to the Hungarian law the NAIH has powers only to take action in case of data processing operations carried out in the territory of Hungary, for instance if a foreign intel service were to collect information from a server or located in Hungary.

The NAIH does not have investigative powers and lacks the capacity to uncover the alleged covert intelligence activity of a foreign secret service in Hungary. Therefore our inspection aimed at examining whether the competent Hungarian defence intel authorities prevented such actions and performed their duties.

The NAIH, in order to clarify the relevant facts, requested copies of documents and information from the National Security Committee and from the Speaker of National Assembly. In this regard we found that the competent Hungarian authorities had done everything they could to examine the situation and to clarify the facts. No signals emerged suggesting the possible impact on, or inclusion of, the petitioner in such intelligence operations. We would like to mention that our Authority received remarkable and useful support from the National Security Committee in providing all necessary documents (*NAIH-46/2014/V*).

VIII. International and public relations

VIII. 1. Conference on drones

The NAIH decided to organize an international conference over the data protection and privacy implications of remote controlled flying objects (drones). Both in Hungary and the European Union these interesting appliances are expanding in military, law enforcement, commercial, scientific and private fields though lacking sufficient national and EU legal bases. The main purpose of the conference was to project the best practices to legislations, authorities, business entities, government organizations and private persons in order to hammer out solutions that respect privacy and data protection principles in the Single European Market.

Privacy and legal experts, aviation experts, business and industry representatives, researchers and non-governmental organizations attended the conference.

The conference's topic was of particular importance given that the relevant legislation on the civil use of drones, both on national and EU level, is currently in a preparatory phase. The NAIH opts for a statutory-level regulation as well.

Our Authority published its detailed recommendation on drones on the 14th November 2014 which can be downloaded from http://naih.hu/files/ajanlas_dronok_vegleges_www1.pdf.

VIII. 2. The international engagement of NAIH

VIII. 2. 1. The 36th International Conference of Data Protection and Privacy Commissioners (ICDPPC)

The yearly held International Conference of Data Protection and Privacy Commissioners was organized on the 15-16th October 2014 in Mauritius last where the leaders of the NAIH also participated. The conference dealt with surveillance, e-health, internet neutrality, PET technologies and the topic of "*big data*". The attendees of the event adopted various statements including: smart devices, "big data" issues, the integrity of privacy in the digital age and on the international cooperation. The 36th Conference, in order to facilitate the international cross-border collaboration and to foster the enforcement of data individuals' rights, adopted the Global Cross Border Enforcement Cooperation Arrangement and urges all data protection authorities (hereafter: DPAs) to get involved. These documents are available on http://www.naih.hu/nemzetkoezi-adatvedelmi-konferencia.html.

VIII. 2. 2. The Conference of European Information Rights' Commissioners

In November 2014 was held the European Conference of Information Rights' Commissioner in Edinburgh with the participation of NAIH. At the event the presentations and roundtable discussions addressed the ratification process of the Tromsø Agreement, the publicity of environment information and the enforcement of the Aarhus Agreement. The participants decided to establish regular meetings and create a European-wide network of information rights organizations.

VIII. 2. 3. The International Working Group on Data Protection in Telecommunications (IGWDPT)

The NAIH was actively involved in the work of the IGWDPT in 2014 as well. This working party, which also includes DPAs outside Europe, dealt with numerous evolving themes and a memorandum was adopted on the issue of "*big data*". This notion encompasses huge amount of data accumulated at multinational companies and used to create detailed profiles about individuals without their knowledge and consent. As a result, the enormous anonymous and pseudonym databases give rise to threats to the privacy of people, especially if conclusions will be drawn and collected, for certain purposes, from individuals or groups of people. The NAIH also supported the adoption of the memorandum.

In addition, the IGWDPT analysed the topics of appliances used for work (Bring Your Own Device), the theme of Wearable Computing as well as the biometric technologies and video analytics.

The NAIH, during its involvement in the IGWDPT, learnt the "privacy survivor kit" joint project of the Portuguese DPA and the University of Porto aimed at restoring control over personal data that internet users disclose during internet surfing.

VIII. 2. 4. JSB Europol

The Joint Supervisory Board of the Europol (JSB Europol) held 4 meetings in 2014 where Hungary was represented by the NAIH. The JSB dealt with the following hot topics: data protection supervision of Europol, the impact of the USA national security programme on the data processing of Europol, third country (e.g. Russia) relations as well as the appropriate data processing practice in the course of combatting human trafficking.

Between the 3rd and 7th of March 2014 the 16th Europol review was held in The Hague. The review committee consisted of 9 experts including one from the NAIH. The review summary report was adopted by the JSB Europol on the 2nd October 2014.
In 2014 the JSB Europol kept on debating over the draft Europol Regulation. In this regard the JSB reiterated its concerns, in an opinion, over the prospective Europol review scheme putting the EDPS into the core point of supervision which contradicts the opinion of the JSB. The NAIH was also involved in drafting this opinion.

The JSB Europol debated over the opinion of the European Parliament (EP) over national security programme of the USA. In this report the EP called on the JSB Europol to review whether or not the Europol was processing personal data (including data transfers to the USA) achieved from national intelligence agencies. The JSB Europol published its summary report over this theme on the 2nd October 2014 which did not reveal any serious infringement regarding personal data obtained from intelligence services and processed by the Europol, however, in order to get a more detailed insight the national Europol offices should also be subject to a review.

Special attention was paid to the relations with third countries. In this regard we should mention the negotiations carried out with Russia under the aegis of the Europol cooperation. Previously the Europol expressed its concerns stating that the level of data protection in Russia did not comply with the adequate European standards. Following several rounds of discussions among the parties and some amendments to the Draft Agreement the final wording and content of the Agreement will be subject to a review by the JSB Europol.

The JSB Europol invited representatives of third country DPAs, which concluded memoranda of understanding with the Europol, to its meeting of 16th June 2014. During these discussions, among others, the parties decided to facilitate and improve their cooperation.

The JSB Europol debated over the potential impacts of the ruling of the Monaco Supreme Court taken relating to the Monaco DPA as well as the possible accession of the Europol to the SELEC (Southeast European Law Enforcement Centre).

The plenary session of 16th June 2014 adopted the Opinion on EU Most Wanted List whereby the JSB Europol expressed that, in its view, such disclosure by Europol would not comply with the effective rules.

The JSB Europol, together with Europol, organized an awareness raising event on the issue of human trafficking in 2014. The topic is of crucial importance as there are always disputed items and problems on the agenda. During the joint session the stakeholders felt the most problems and misunderstandings occurred due to lack of information and, therefore, they determined to promote the theme with their own means.

The JSB Europol welcomed the adoption of the new AWF Handbook in the second half of 2014 that was a huge step forward after several years of delay.

VIII. 2. 5. SISII CSG

The Regulation1987/2006/EC of the European Parliament and of the Council on the establishment, operation and use of the second generation Schengen Information System (SIS II) foresaw the establishment of a coordinated supervision group (CSG) which commenced its operation in 2013. The high priority themes where the NAIH was actively involved were, among others, the following: efforts to be made to enhance the safety of SISII following the data breach incidence of 2013, the elaboration of uniform methodology for data protection checks, the review of the new Schengen evaluation mechanism (hereafter: Scheval) mechanism, specific issues relating to vehicle warnings and practical guidance on the enforcement of data subjects' rights.

During the year the SISII CSG made several efforts to improve the safety of SISII and, to this end, included the EU-LISA agency into the process. It became clear that Member States have distrust both towards each other and to EU institutions. Therefore the SISII CSG developed concrete recommendations to national supervisory authorities with respect to the review of the safety of SISII. By using these schemes Member States will become able to review their national systems and to avoid data protection incidences in case like the one happened in Denmark in 2013.
The SISII CSG commenced to develop uniform methodology for data protection checks and, for this purpose, set up two subgroups. The NAIH acceded to the legal issues subgroup.

The SISII CSG was active in the development of the new scheme of the Scheval prepared by the European Commission. In this regard the NAIH insisted multiple times that the independent data protection module should be maintained, what's more, data protection experts should be delegated into other modules as well, for instance into the N.SIS+SIRENE and VISA systems.

The SISII CSG, following numerous complaints, endeavoured to review the data protection implications of vehicle warnings in the SISII. These petitions suggested that SISII warnings placed by other Member States become apparent only at the time of the purchase or change of ownership. During the time of clarification of the origin and nature of the SIS warning, which can last for years, the owner may not use the car and even if he uses it within the Schengen zone he may become subject to police inspection or even apprehension. With a view to clarify the question the NAIH issued a recommendation in 2014.
The SISII CSG adopted the practical guidance on the enforcement of data subjects' rights (Guide of Access). It was agreed upon that the Guide should be distributed in the widest possible scope.

VIII.2.6. JSA Customs and CIS CSG

In 2014 the JSA Customs discussed the conclusions of the 2011 review report on the Customs Information System (hereinafter referred to as CIS) and, in order to follow up its recommendations, set up a questionnaire. Additionally it dealt with the information leaflet distributed to authorities using the CIS.

The Coordination Supervision Group of the Customs Information System (hereafter: CIS CSG), consisting of experts of the Member States' DPAs and the European Data Protection Supervisor (EDPS), negotiated the findings of the examination of central and national CIS units.

In addition, the CSG discussed the preparation process of the information leaflet on data subjects' rights and the relating survey as well as the work programme for the years 2014-2015. In this regard it was argued that the utilisation rate of the system had been quite low. According to some sources there are only 200 data on file which received very few queries and, as a result, the necessity of the system can be questioned and, in this form, it does not comply with the basic conditions of purpose limitation. Consequently the CIS CSG will inspect the issue shortly and, if appropriate, will consider recommending the cancellation of the system (which would be unprecedented in its kind).

VIII.2.7. The Eurodac CSG and VIS CSG

The Eurodac CSG discussed the implementation of the so-called "*advanced data erasure"* which had to be put in practice due to the accession of Croatia but various Member States failed to carry out. In this topic also the NAIH approached Hungarian government agencies.

The Eurodac CSG called on the European Commission (hereafter: EC) that, following the entry into force of the new Eurodac Regulation, a new IT infrastructure will have to be established to meet the query demands of police authorities. In this regard the data protection implications of the new system have also been examined where the access rights of law enforcement authorities, the data subjects' rights, the tagging of personal data, the methods of coordinated supervision as well as the public information proved to be of crucial importance. The NAIH here highlighted the review of "special queries", the deletion of data in a proper timely manner and the enforcement of rights (complaints, appeals) of data subjects.

In 2014 the Coordinated Supervision Group of the Visa Information System (hereafter: VIS CSG) negotiated the issue where it had been revealed by the Spanish DPA that Spanish consular officers, in the course of visa procedures, had utilized data retrieved from the SISII. The Spanish DPA condemned the process of the Spanish Foreign Affairs Ministry and imposed a financial penalty on the ministry.

The VIS CSG discussed the data protection implications of outsourcing of visa procedures with special regard to the legal basis, the supervision, the enforceability of contractual obligation, the data retention and the applicable law. The NAIH stressed that the EU-level protection of personal data shall be ensured even in those receiving countries where law enforcement agencies, with a view to combat terrorist and other serious international crimes, have access to all electronic data systems.

The VIS CSG adopted the questionnaires prepared with respect to the listing of authorities having access to VIS, to the access of law enforcement agencies to the system as well as the exercise of data subjects' rights. The VIS CSG emphasized that, in view of the questionnaires, the synergy of the VIS, SISII and the Eurodac shall be sought. The NAIH called for the extension of investigations into the Local Consular Cooperation since important data processing is carried out on this level and both Member States and the EC are involved.

The VIS CSG discussed the reports suggesting that Russian authorities had kept on exercising pressure on EU national authorities to disclose data concerning certain visa procedures. The VIS CSG urged for a firm and joint action to tackle this.

During the year the VIS CSG followed up the current situation and future plans over the VIS roll-outs. In this context it has been concluded that the biggest deficiency in the VIS had been the

implementation of the principle of proper data quality whereby the impact on biometric data is of particular concern.

VIII.2.8. IMI CSG

The first session of the Internal Market Information System Coordinated Supervision Group (IMI CSG) was held on the 6th May 2014. The IMI was developed by the EC in order to facilitate the fast and effective communication among EU and EEA Member States' administrations. This web platform enables Member States and other users to collaborate practically and daily upon implementing single market regulations. Users include ministries, national authorities, various chambers and other authorities. The IMI is used in 7 different areas (professional qualifications, services, posting of workers, euro-cash transportation, SOLVIT, patients' rights, e-commerce) and can be accessed by 7.396 authorities and where 6.000 data exchanges happened in the first half of 2014. The IMI is supervised by Member States' DPAs (involving the NAIH as well) and the EDPS jointly in a Coordinated Supervision Group.

The IMI CSG, in its first session, discussed the major data protection topics with special regard to the freely given consent, the proper access of authorities, and the information given to the public as well as the basic rights of data subjects. It was concluded that the public information on IMI was quite ineffective, what's more, the users of the system proved to be uncertain over how to operate the IT structure therefore it is of crucial importance that national DPAs, by issuing guidance and recommendations, assist in exercising data subjects' rights and facilitate the information of the public. The NAIH emphasized the significance of the monitoring of exercising data subjects' rights, the utilization of the system for purposes other than intended originally as well as the proper information of the public.

VIII.2.9. Cyber security

The NAIH attended two conferences and held presentations: the one organised by the Law School of Masaryk University in Brno on 28-29th November 2014 with the title "Cyberspace" and the other held in Budapest and organized by the French Institute on the 19th November 2014 with the title "*Protection des données et cybersécurité, systems compares et enjeux."*

VIII.2.10. International delegations

In the framework of his program in Hungary, H.E. Mr. Nils Muiznieks, Human Rights Commissioner of the Council of Europe paid an official visit to the NAIH on the 3rd of July 2014. Attendees of the program reviewed the history of data protection in Hungary and the current institutional structure. Afterwards the Commissioner raised the issues of supervision of data processing activity of national intelligence authorities, the recent remarkable rulings of the CJEU (data retention, right to be forgotten), the discrimination of the Roma, the special rules on the processing of sensitive personal data and the certain points of jurisdiction. During the discussion other issues, which received considerable media coverage, were also raised like the statements of a judge from the Gyula Tribunal, kuruc.info website, data processing concerning the Budapest Pride in connection which the President of the NAIH presented the position and practice of the NAIH.

A delegation of 3 from the Moldavian DPA, led by Mr. Director Vitalie PANIŞ, visited our Authority in the course of a study tour on 5-6th May 2014. Members of the delegation discussed the operation and structure of the NAIH, the situation of data protection in Hungary, the pending investigations and the conclusions thereof as well as the issues relating to complaints.

A delegation of 5 from the Georgian DPA was received on the 27th November 2014. The purpose of the visit was to get to know the operation and structure of the NAIH and to gain experience and information which they can utilize in their domestic work.

On 9th May and 12th September we received delegations of judges. In the course of these study tours they paid a visit to the NAIH as well. The experts of our Authority delivered presentations about the operation and structure of the NAIH and our findings during our work.

The purpose of the "*Civil Servant Mobility Program"* (CSMP) is to provide further education on the Hungarian experience of EU accession to civil servants coming from the countries of the Eastern Partnership. The project is supported by the foreign affairs ministries of the Visegrád Countries including the Hungarian Ministry of Foreign Affairs and Trade. The focus topic of the Georgian delegation, visiting the NAIH between the 24th and 28th November, was data protection. During the program they were received by various government agencies where experts delivered presentations and offered consultations to the delegation. In this context the experts of the NAIH delivered a lecture with the title "The relation and contradiction between data protection and freedom of information.

VIII.3. The Arcades project

The European Commission adopted in July 2014 the "*ARCADES" („Introducing dAta pRoteCtion AnD privacy issuEs at schoolS in the European Union")* project which aimed at raising awareness in schools in the European Union about data protection and privacy and in this way reinforcing children's protection of personal data in the online environment. The project consortium consisted of the NAIH, the Data Protection Commissioner of Slovenia (IP) and the Research Group on Law, Science, Technology and Society (LSTS) of the Free University of Brussels (VUB) and was led by the Polish DPA (GIODO).

Project partners are experienced actors on the data protection arena and prepared several education materials in the theme. The project started officially on the 3rd of November 2014 and the cross-border joint work aimed at raising and enhancing awareness in data protection will last prospectively for 18 months till May 2016.

The project's aim is to actively reach out to schools, by organising a two-day seminar for teachers and involve them in the initiatives (contest) which will provide them and their pupils with an elevated view and understanding of data protection and privacy issues.
The project has been co-financed by the Fundamental Rights and Citizenship Program of the European Union.

VIII.4. The Article 29 Working Party

The Article 29 Working Party (hereafter: 29WP), consisting of the Member States' DPAs and acting independently in an advisory status, adopted numerous documents and formed positions in several issues during 2014. Legislative and decision-making bodies of the EU regularly

approach the 29WP for consultations therefore the party became an essential player on the European privacy arena.

A detailed presentation on the operation of the 29WP would exceed the limits of the present report that's why we can highlight only the most remarkable documents and events. Beyond the plenary sessions of the 29WP the NAIH is involved is different subgroup activities as well. The Technology Subgroup deals with the relation between privacy and new technologies, in the Borders, Travel and Law Enforcement (hereafter: BTLE) Subgroup the NAIH is actively involved. We are represented also in the Future of Privacy subgroup which examines mainly strategic issues regarding the data protection law and reform on EU level.

The plenary session of 29WP adopted opinions, among others, on the following topics: the necessity and proportionality concepts and data protection within the law enforcement sector, the surveillance of electronic communications for intelligence and national security purposes, the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. The 29WP also issued statements on the ruling of the CJEU invalidating the Data Retention Directive and on the impact of the development of big data.

The Statement of the 29WP issued in the framework of the Data Governance Forum on the 8th December 2014 was of particular importance. This document analysed the relation between security and privacy and was released before the Paris terrorist attacks. Particular attention was paid to, due to the scope of affected persons and its international aspect, the so-called Google ruling which established the legal responsibility of internet search engines.

VIII.4. 1. The Google ruling – the responsibility of search engines for data processing

On the 13th May 2014 the CJEU delivered a judgement, in a preliminary procedure, relating the data processing by internet search engines. In the main proceeding a Spanish national (hereafter: Petitioner) lodged with the Spanish DPA (hereafter: AEPD) a complaint against La Vanguardia Ediciones SL, which publishes a daily newspaper with a large circulation, and against Google Spain and Google Inc. The complaint was based on the fact that, when an internet user entered the Petitioner's name in the search engine of Google, he would obtain links to two pages of La Vanguardia's newspaper on which an announcement mentioning the Petitioner's name appeared for a real-estate auction connected with attachment proceedings for the recovery of social security debts.

The CJEU has already stated that the operation of loading personal data on an internet page must be considered to be such 'processing' within the meaning of Article 2(b) of Directive 95/46. The operator of a search engine is the 'controller' in respect of the data processing carried out by it since it is the operator that determines the purposes and means of that processing. The search engine provides, from a privacy perspective, a sensitive service as it can establish a more or less detailed profile of the data subject. The CJEU concluded that the fact that publishers of websites have the option of indicating to operators of search engines that they wish specific information published on their site to be wholly or partially excluded from the search engines' automatic indexes does not mean that the operator of a search engine is released from its responsibility for the processing of personal data that it carries out in the context of the engine's activity.

According to the judgment Google Search does not merely give access to content hosted on the indexed websites, but takes advantage of that activity and includes, in return for payment, advertising associated with the internet users' search terms, for undertakings which wish to use

that tool in order to offer their goods or services to the internet users. The Google group has recourse to its subsidiary Google Spain for promoting the sale of advertising space generated on the website 'www.google.com'. This makes the service of the search engine profitable. That being so, it cannot be accepted that the processing of personal data carried out for the purposes of the operation of the search engine should escape the obligations and guarantees laid down by Directive 95/46.

The Court has already held that the provisions of Directive 95/46, in particular the right to privacy, must necessarily be interpreted in the light of fundamental rights. Considering the applicable provision of the Directive 95/46/EC ("balance of interests", the directly applicable point f) of Article 7 in the Directive) the competing interests shall be harmonised: the protection of individuals' privacy, the business interests of the operator of the search engine and the information rights of internet users. The CJEU, analysing the former interests, came to the conclusion that "*the data subject's rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in finding that information upon a search relating to the data subject's name*." The judgment added, however, *"that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of inclusion in the list of results, access to the information in question."*

It follows from the rights to privacy and data protection of the individual that "*even initially lawful processing of accurate data may, in the course of time, become incompatible with the directive where those data are no longer necessary in the light of the purposes for which they were collected or processed."* The NAIH, in its statement, welcomed the decision because the ban on eternal publicity follows from it, that is to say, not the privacy shall take a step backwards in light of the technological and business considerations but, on the contrary, the technological and business solutions shall be aligned with the protection of privacy. The NAIH also shared the opinion of the CJEU stating that the data subject, playing an active role in the public life, may not ask for the restriction of information available on him.

The 29WP, in light of the practical application of the ruling, held consultations with the search engine operators. As a result the 29WP provided a guidance to national DPAs for handling incoming submissions and adopted a common position in the question. It is also expected from search engines that, in order to protect the privacy of data subjects, information shall be deleted from the *".com"* sites as well.

The NAIH has been continuously receiving complaints from individuals claiming that requests for deletion of certain items in the listing have not been fulfilled. The examination of such submissions is carried out in close European cooperation and in the coming years we are expecting a significant rise in legal cases.

VIII.4. 2. Our engagement in the subgroups of the 29WP

The Technology Subgroup prepared the Opinion on Anonymization Techniques which, beyond providing theoretical inputs, delivers practical guides to data controllers in order to facilitate anonymization. The subgroup prepared the wording of the Opinion on Personal Data Breach Notifications as well that presents, through practical examples, the major aspects to be considered in the evaluation process of such incidents. The subgroup, after long lasting consultations, drafted an opinion on how to interpret the provisions of the ePrivacy Directive concerning creating fingerprints by computers (device fingerprinting). A specialty of the Opinion is that its content has been consulted with the national info communications authorities. The subgroup was also actively involved in the elaboration of the Opinion on Internet of Things which deals with the impact of fast developing technologies on data protection. Another important task was to harmonize the collaboration of EU DPAs in remarkable cross-border privacy issues. In the framework of the Technology Subgroup the respective data protection experts had the opportunity to inform their counterparts on investigations concerning the Google, Facebook, LinkedIn and Microsoft.

In 2014 the BTLE Subgroup took up the following topics: Draft Opinion on the Electronic Communication Monitored by National Intelligence Services, Draft Opinion on Necessity, data protection implications of data processing activities carried out according to the Cyber Security Agreement, the processing of travellers' data, the so-called Smart Border Package, the Data Protection Reform Package, the Recommendation on Drones, the Statement of the 29WP issued in the framework of the Data Governance Forum of 8th December 2014 as well as the implementation of the court ruling relating to Data Retention Directive. The NAIH acted as rapporteur in cases of the travellers' data and the drones.

VIII.5. The Draft 108 Convention

The Convention was opened for signature in 1981. Since then it has been considered as a reference document in 43 states and this is the only binding international instrument which protects the individuals against abuses and can be applied worldwide.

Any country of the world may access to the Convention provided that they comply with the data protection regulations as laid down by the Convention and has a solid legal background to enforce the rights of individuals. The modernisation of the Convention is driven by the rapid technological developments and the globalization of data processing that bring about challenges to privacy protection. It has been widely agreed that the general and technologically-neutral nature of the Convention shall be upheld and, in addition, its openness shall be maintained to other legal systems in order to remain a universal and generally respected legal instrument internationally. Due to the technological developments and with a view to develop a more harmonised international data protection law the commencement of the modernisation shall be done in a timely manner.

The above objective is supported by the fact that articles relating to the privacy and data protection have not vanished from the front pages of newspapers. The technology is booming and we are facing that the purchase of goods and services is made by using personal data. This refers mainly to the online world: from bank services to travel and to social networking sites. The use of personal data is important in order to ensure the safety of society as well. The more than

30 year-old wording of the Convention is, taken into account the rapid technological changes, timely. For this reason the new draft wording of the Convention will be discussed on two level (CAHDATA, T-PD). The NAIH proposed that a reference should be included to the basic principle of necessity in Article 5 of the Convention as this is at least as important fundamental principle as are proportionality and purpose limitation that's why it is essential to declare them on the same high level. The amended wording of the Convention is expected to be discussed by the Council of Ministers in the first quarter of 2015.

CONTENTS

Nemzeti Adatvédelmi és
Információszabadság Hatóság

1125 Budapest, SzilágyiErzsébetfasor 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: ugyfelszolgalat@naih.hu

Published by: National Authority for Data Protection and Freedom of Information
Publisher: Dr. Attila Péterfalvi, President
ISSN 2063-403X