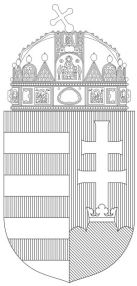
Annual Report of the National Authority for Data Protection and Freedom of Information (NAIH)

2013

National Authority for Data Protection
and Freedom of Information
Budapest, 2014



Introduction

According to a proclamation made by the Parliament in Hungary's new Fundamental Law, the protection of personal data and the guarantee of free access to data of public interest are rights that are to be supervised by an independent administrative authority. The National Authority for Data Protection and Freedom of Information (NAIH), as a new structure, provides more efficient public services. Its calling is to ensure a high level of data protection and transparency of public institutions for citizens in Hungary. This annual report highlights the results and main tendencies of past year's activities, which is the second in the Authority's existence.

Our first year was the year of construction and consolidation. After that, 2013 provided us with a lot of feedback from which we can resolutely draw grounded conclusions and expertise. Besides the success of our market-based data protection audit service, the ability to use our reinforced administrative competences, allowing an improved protection of the constitutional interests of data protection, was a prominent feature of the past year. When coming across serious infringements on data protection law, we make a resolute yet not excessive use of the prerogative to impose fines. Their amounts are set after careful consideration of all present and surrounding circumstances. We trust that the use of this tool is effective especially in serving vulnerable data subjects' interests. A striking illustration of this statement was the 6 million HUF fine imposed on various online dating services when our investigations showed that several thousand of their registered users were children, whereas those websites were supposed to be accessible to adults only.

2013 was also the year when we launched our first long-term project. Focusing on the protection of children's rights in an online environment, the end result of our « Key to the world of the Net! » study was the production of a report on our findings addressed to adults, and of an informational colour booklet for children. This is still an ongoing project, as we are striving to raise a wider audience's awareness of the Internet's dangers and pitfalls, through the use of selected means such as television advertisements, sensitisation publications, and cooperation with relevant civil society actors.

The data protection scandals that occupied and « shocked » both national and international public opinions proved the need to invest greater attention to the interwoven matters of data protection and IT security. We have therefore highlighted the importance of data security for data controllers when taking part in professional conferences. Our aim is to prevent this type of risk.

Next to the data protection activities, our independent Authority has to leave enough room for freedom of information. We have requested the disclosure of data held by State or local government administrations each time we received an established complaint from a citizen. At the same time, we needed to take into the increasing amount of work and duties placed on administrations when facing cases of late or incomplete disclosure. A balance needs to be struck,

and we have strived to follow the middle way road between the protection of civil servants' private lives and the interests of transparency, especially when having to make a decision on the disclosure of staff lists, for example the lists of teachers.

Our conception of the future includes the correction a few deficiencies that are now present in the Privacy Act. At this point in the EU's data protection reform process, the debate on data protection registers is still open. Our professional standpoint is that the current, relatively bureaucratic, administrative notification process could be dropped for a more flexible, less formal register that would serve specifically as a tool to inform data subjects. Another important goal, one in which we would like to see improvements in our law, is to follow well-proven foreign practices by adopting of a system of Binding Corporate Rules as legal basis for data transfers to third countries.

As we have done in the past, our work shall continue to serve the citizens as our main value, by protecting and guaranteeing their rights to privacy. We will also keep working to ensure the State's transparency, keeping in mind that the State's ability to function depends directly on taxpayers' approval and money. Finally, we must always keep in mind that data protection may not be an obstacle to public interest. We may not hide behind it as an excuse to avoid fulfilling our various duties as citizens, such as consent to taxation.

Budapest, March 4th, 2014

Dr. Attila Péterfalvi

President of the National Authority for Data Protection
and Freedom of Information
Hon. University Professor

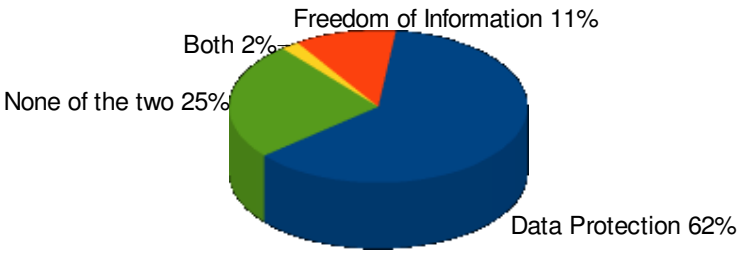
I. Statistics and highlighted items on the Authority's activities in 2013

1. Statistics

In 2013, the Authority received over 5700 postal and 11.222 electronic mails. We furthermore processed 11.686 notifications of personal data processings, of which 7420 arrived by postal mail, and 4266 by e-mail.

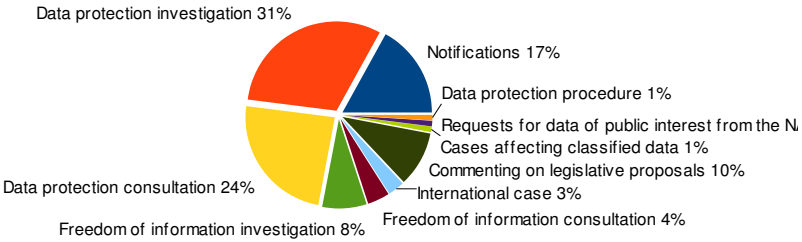
We opened 3280 cases in 2013, which represents a 9 % rise from 2012 figures. Among those cases, we launched 40 administrative procedures and 2481 investigation procedures. The remaining 759 cases pertained to other branches of our activity, such as international affairs or relations with data protection officers.

Only 370 investigation cases started in 2012 had to be continued in 2013. In January 2014, the number of unfinished cases from the previous year dropped to 341. We managed to complete 90 % of our procedures in 2013, which constitutes a significant achievement in a context of rising case numbers. We also dealt with 106 international cases.



Distribution of cases according to the branch of information rights affected

Distribution of cases by procedure types



In 2013 we processed 311 regulatory advisory procedures, which corresponds to a 33 % rise compared to 2012, and proposed 28 amendments.

We received 47 requests for data of public interest, all of which were processed within the 15 day legal deadline.

The NAIH had 167 media appearances - 408 on television or radio programs, 378 in the printed press, and 691 on the Internet. 1 % of these appearances concerns international media.

2. "Key to the world of the Net!": the NAIH's children protection project

In 2013, the NAIH launched its first long-term project. Its topic constitutes one of our top priorities: the protection of children's rights in an online environment.

The first step of this project was to realize a comprehensive study on young people's use of the Internet, the dangers they face in an online environment, and the relevant legal regulations both in Hungary and abroad. We conducted our study with the cooperation of various national and international partners. Our aim was to include in our work the help of experts in education, psychiatry, law, criminology and information technology, as well as

to gain information on international best practices. No less than 12 experts were involved in the writing and publication of a 122 page study, and an informational leaflet was designed for children and presented in several schools in Hungary.

This document was entirely translated into English, and a short summary was also made available in French. Both can be freely downloaded from our website www.naih.hu .

It is our aim to pursue this project with our international partners in the frame of an international workshop on digital education, under the leadership of the French Data Protection Commission (CNIL), and of a project funded by the European Union called “Introducing data protection and privacy issues at schools in the European Union“, under the leadership of the Polish Inspector General for Data Protection (GIODO).

3. Conference of Internal Data Protection Officers

Section 25 of the Hungarian Privacy Act provides for the organization of a national Conference of Internal Data Protection Officers (DPO). This conference has to be organised at least once a year. In practice, there are now two conferences a year. It serves as a regular exchange of professional expertise and experience between DPO's and the Authority. It helps ensure a uniform application of the Act. DPOs whose nomination is mandatory according to our Privacy Act are *ex officio* members of the Conference, but other DPOs may also register.

In 2013, the first conference was held on the International Data Protection Day, and the second one in June. The focus of the first one was on the entry into force of the new Labour Code and its consequences for personal data in relation to labour relations. The second one's main theme was the professional situation of DPOs in Hungary, and their place and status within data controllers.

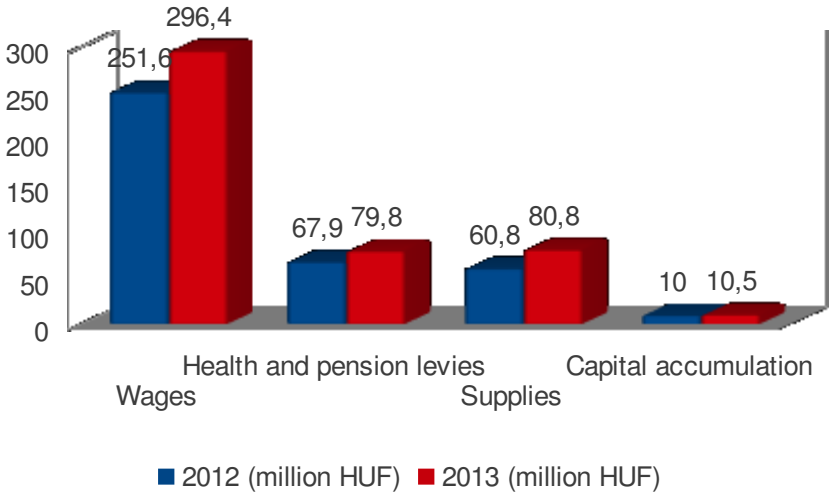
II. Budget, financial management and staff of the Authority

The Authority was allocated 59 full time equivalents. On average, in 2013, there were 56 people working at the Authority. This drop is explained by voluntary departures. Recruitments are expected to be completed during the first half of 2014.

This table summarises the main elements in the 2012-2013 budget:

Item / year	**2012**	**2013**	**2013/2012**
	× million HUF	× million HUF	%
Total budget	**390,3**	**467,5**	119,78
Operational budget	380,3	457	120,17
Wages	251,6	296,4	117,81
Health and pension levies	67,9	79,8	117,53
Supplies	60,8	80,8	132,89
Capital accumulation	10,0	10,5	105,00
Investments	10,0	10,5	105,00
Budgetary balance reserve for the chapter	12,1	9,5	78,51
Altogether	402,4	477,0	118,54

The following diagram illustrates the evolution between 2012 and 2013 :



In 2013, the Authority launched its Data Protection Audit service. Data controllers can, against the payment of a fee, ask for an audit that generates extra revenues for the Authority. During the first year of this service's existence, it generated 3 556 thousand HUF.

The enforcement of administrative fines is part of the Authority's responsibilities. These are the main figures of this activity in 2012-2013 :

Number of cases	47
Paid fines	20 677 478 HUF
Fines transferred to the Treasury	20 677 478 HUF
Fines pending payment	12 951 461 HUF
Devaluated demands	5 020 000 HUF
Devaluation altogether	1 502 000 HUF

III. International affairs

It has been several years now since the European Union launched its data protection reform process, and its issue appears still uncertain. The European Commission presented its plans for a new data protection regulation replacing the 1995 Data Protection Directive (95/46/EC) and for a data protection directive regulating the use of personal data for crime prevention and prosecution, on January 25th 2012 (the details of these reform plans are already presented our 2012 Annual Report). The Council, so far, has already discussed the Data Protection Regulation on three occasions. But no majority could be found in favour of the replacement of a directive by a regulation, and while most agreed with the "one stop shop" principle, it was found that more work was needed on the details of its practical implementation. Another element that according to the Council still needs to be reviewed, is the European Data Protection Board, which would be in charge of harmonizing implementation practices by data protection authorities or the Data Protection Regulation. The fate of national data protection registries remains unclear. The current proposal does not contain any provisions for such a registry, and as a consequence we are still unsure of what Member States' obligations will on this particular matter. Some of the European Parliament's committees have also debated these proposals. Interestingly enough, the Economic and Monetary Affairs Committee chose not to use its right to formulate an official opinion. The LIBE committee, however, voted to support the proposition on the 22nd of November, 2013. The text adopted includes several amendments : for instance, the principle of legitimate purpose was reinforced, the limit to data protection infringements related fines was risen to 5% of the data controller's turnover, and MEP's have subordinated the possibility for data controllers to transfer data to third country law enforcement agencies on the existence of bilateral cooperation agreements. Regarding the LIBE committee's opinion on the new Data Protection Regulation (on the use of personal data for criminal investigations), it should be noted that generally speaking, it shifted the text's focus from the notion of *accountability*[1] towards stricter enforcement of data subjects' rights.

In parallel to the European developments, the principle of accountability has been the cornerstone of data controller's increased call to responsibility in the English speaking world (mainly the US, Canada and Australia), during the past few years. While this principle has been around for about thirty years already, it has gained in strength significantly in the course the recent reform process. Its precise meaning is hard to grasp. Its very definition and translation into Hungarian are also problematic. In the private sphere, it is in practice primarily constituted by private actors' commitment to a set of rules set by themselves, which establishes clear responsibility statements that are followed by practice. Usually, the given undertaking compiles all its data protection rules, from the rules governing the processing

1 In English in the original text

of complaints to those that concern IT security matters, into one *privacy policy*[1]. This document serves as a guideline for the internal enforcement of data protection. It can be the source of confusion and mistakes if they are not updated, if they become out-of-date due for example to internal restructuration shifting data protection tasks to a different unit, if new challenges are incorrectly or incompletely analysed, or if internal rules of accountability are not laid down in a clear and explicit manner. As we can thus see, the accountability principle is not static, but is the base of a process that requires continuous attention and concentration. The American think-tank *Center for Information Policy Leadership* has been leading an international project called *Accountability Project* since 2008. Its main objective is to offer a discussion and debate framework for all stake-holders (legislators, data protection authorities and private actors). The following are the project's phases that can serve as a description of what the pillars of accountability are:

Setting out the essential elements of accountability ;
Demonstrating and measuring accountability ;
General and validated accountability ;
Data protection risks ;
Essential elements in distributed environments.

Concerning the NAIH's international affairs, the majority of 2013's 106 cases were consultations by European institutions, foreign data protection or freedom of information authorities, law practices, scientists or other individuals, requesting information about the interpretation of Hungarian law, the NAIH's case law and our opinion on concrete affairs. In 2013, we received many questions related to whistle blowing, as Act CLXV of 2013 on Complaints and Public Interest Disclosures, which entered into force on January 1st, 2014, brought significant changes. The general rule is that whistle blowing mechanisms do not have to be set up in the frame of social relations with employees, but if the employer decides to introduce such a system nevertheless, he must first notify it to the Authority's public data protection registry.

The NAIH sent questions to its international partners several times, aiming at gathering information on foreign practices and give relevant insights to our own cases and investigations. We sent out such questions for example on cases concerning anonymous job offers, the use of video cameras in personal vehicles, website registration and data processing, and contact keeping with Google. We also sent questions about the national security review of civil servants.

In 2013, we strengthened our relations with several Eastern European countries' data protection authorities, and especially with Macedonia, Montenegro, Moldova – thereby continuing the close relationship we enjoy since 2007 – and Russia, where although there is no specific data protection authority yet, but a government body in charge of data protection in the electronic communications' sector, and where Convention 108 of the Council of

Europe was ratified in 2013.

In the middle of the year, the TAIEX (Technical Assistance and Information Exchange instrument managed by the Directorate-General Enlargement of the European Commission) asked the NAIH twice to share its knowledge and experience with the Macedonian colleagues. The independent Macedonian authority started operating in 2005 and we received its president and two of his colleagues as guests between May 28th and May 30th, 2013. During the three days, we organized conferences and seminars on our work and on the material requirements. A special meeting was organizing between both our financial directors. We also discussed the differences between our procedural laws, the need to balance data protection with freedom of information, the data protection audit, some particular European norms, national and international legal proceedings, and Schengen experiences. A special visit was organized to the Constitutional Court.

Picture of the Macedonian delegation to the NAIH

Between the 25th and the 27th of June, 2013, we received a delegation from the Macedonian Committee on the Protection of the Right of Free Access to Public Data. Mr. Pece Tashevski, the president of the Macedonian Committee (the president, vice-president and three other members are elected by the Parliament for five year terms) reported on the fact that data protection and freedom of information are completely separate spheres in his country. The law on freedom of information was adopted in 2006. The Committee is in charge of the enforcement of this law, of giving opinions on bills, of processing appeals,

of cooperating with controllers of data of public interest, and of keeping their registry up to date. They place particular emphasis on people's education to freedom of information, and especially of those data controllers who are entrusted by law of the processing of public data. They imposed a fine only once since 2006. There are 1253 public data controllers in Macedonia. 87% of the complaints are lodged by NGO's, which shows the strategic importance of their activities.

The Hungarian colleagues held a conference on the concept of freedom of information, its historical development and its role in a democracy. Special attention was granted to the so-called *harm test* and its importance ("harm test" designates the cost-benefit analysis for society of a given data's publication). Our guests were particularly interested about the electronic publication of public data, as their work in Macedonia is considerably hindered by the legal obligation to communicate information on paper format (the cost of preparing and copying a document is fixed by a government decree at 1 MKD per page, which correspond to more or less 5 HUF). The other key topic was the relation between courts and freedom of information. Our guest lecturer, a judge from the Miskolc District Tribunal, gave detailed answers to technical questions on the anonymisation and publication of court decisions. Another judge, from Budapest's District Tribunal, told us about the relevant case law. The leaders of the Hungarian branch of Transparency International introduced us to their profile, activities and cases. On the re-use of public information, we insisted on the European directives, and prepared a detailed presentation on the University of Turin's scientific project called LAPSI (*Legal Aspects of Public Sector Information*), and on the E-PSI Platform website, which collects knowledge on this subject.

The Macedonian Freedom of Information delegation to the NAIH

Between the 19th and the 21th of November 2013, the NAIH's experts were invited to a one day seminar at the Data Protection Department of the Montenegrin Ministry of Interior and the Montenegrin Data Protection Agency. The Hungarian guests gave a lecture on the basics of European data protection law, on the European Court of Justice's case law, on the differences between data protection regimes and on the main elements of the 2006/24/EC Data Retention Directive (we mentioned the transposition and harmonized implementation roadblocks).

In the frame of Justice and Home Affairs cooperation, the European Union operates several databases containing personal data. Their aim is to contribute to cross-border cooperation in the prevention and investigation of fraud and criminal activities. National data protection authorities, like the NAIH, participate and cooperate in ensuring that these activities are not conducted in a way that would harm citizens' data protection rights.

The NAIH participated to Europol's Joint Supervisory Body, Schengen's Joint Supervisory Authority, and the Joint Supervisory Authority Customs (responsible for the Customs Information System's data protection). It furthermore conducted supervision over the Visa Information System and the Eurodac database, as each national authority is responsible for the data protection supervision of the information sent into the system by law enforcement authorities under their national jurisdiction.

In 2013, the NAIH carried out supervision controls at the national Sirene Office, the Europol and Eurodac national units, as well as at the Belgrade and Chisinau embassies. We concluded that the processing of data by these institutions provided adequate data protection safeguards according to both national and EU legislation.

In 2013, we received and processed 8 citizen requests involving the Schengen Information System.

Cooperation in the work of the Article 29 Working Party

Article 29 of the Data Protection Directive (95/46/EC) creates a Working Party composed by a delegate from each national data protection authority. Its main task is to promote harmonized interpretation EU-wide of the Data Protection Directive. Besides participating actively to the plenary meetings, the NAIH takes part in several of the Working Party's subgroups specialised on:

- Borders, Travel and Law Enforcement ;
- New technologies, Internet, Electronic Communications ;
- e-Government.

A highlight of last year's Article 29 Working Party related activities was

the participation of one of our experts to the four people delegation who travelled to Australia to undertake a comprehensive examination and control of the EU-Australia Passenger Name Record Agreement (PNR Agreement). The review took place between the 29th and the 31st of August, 2013, in Canberra.

International Working Group on Data Protection in Telecommunication

The International Working Group on Data Protection in Telecommunication (IWGDPT) was established by the Berlin Data Protection Authority. It includes members from the EU as well as from third countries, who work together to analyse the data protection impacts of new developments in Information Technology and telecommunications. Next to the publication of opinions, this working group keeps in touch with major data controllers who keep it up to date with the latest technical developments. In particular, this working group has published studies and opinions on hot topics such as big data, drones and webtracking. In 2013, the NAIH participated to the testing of the new Google Glass hardware, and analysed its data protection impacts. One of our main conclusion was that the device should indicate that it is recording not only to its user but also to people nearby, in order to avoid its use for spying purposes. Furthermore, we voiced our concerns over the centralisation of the data continuously transmitted by this device to a centralised data controller.

Accession to international organisations

In 2013, the NAIH joined the Global Privacy Enforcement Network (GPEN). Since 2008, this organisation, which was the result of an OECD proposal, has attracted 31 members. Its main objective is to contribute to international decision-making on data protection issues.

IV. Data Protection Cases

Compared to the total amount of cases, the proportion of data protection procedures is low, yet their significance and impact are high. The contents of the administrative decisions play a significant role in the expansion of our regulatory practices and case law. Indeed, contrary to the more supple investigation procedure, inspired by "Ombudsman"-type practices, data protection administrative decisions are legally binding on their recipients. As such, they can serve as a guide for all the other data controllers.

1. General introduction to data protection administrative procedures

Data protection procedures are initiated by the Authority's decision, whether they were preceded by complaints or not. In most cases, data protection procedures follow investigation procedures. The information gathered during the latter can be used in the data protection procedure.

The Authority has the right to judge in which cases it should launch a data protection procedure. The Hungarian Privacy Act also provides that such a procedure must be started if there are grounds to suspect the illegality of a personal data processing operation, and that the said operation concerns a large number of people, concerns sensitive data, and there is a risk to hurt the interests of many citizens in a significant way.

The Privacy Act and the Act CXL of 2004 on the General Rules of Administrative Proceedings and Services (Administrative Proceedings Act) together set the rules for the Authority's Data Protection Procedure. By law, such a procedure is not supposed to last more than two months, but the NAIH may extend this deadline upon procedural reasons. In 2013, we had to use this possibility in about 40 % of our Data Protection cases, due mainly to a lack of cooperation from the data controllers.

2. Selected procedural law matters

In 2013, next to those that were specified in our investigation strategy, our data protection procedures concerned the following topics :

- Personal data processing operations by estate agency networks ;
- Marketing databases ;
- Personal data stored on professional laptop computers ;
- Data processing operations by recruitment agencies ;
- Medical data disclosure ;
- Data breach incidents ;
- Anonymous job offers ;
- Telesales ;
- Data processing operations by winemaker and fruit grower syndicates ;
- Reports on crimes ;
- Publication of local deliberative bodies' decisions ;
- Real estate advertisements ;
- Organisation of courses ;
- Archives ;
- The processing of students' personal data.

Data controller's type	**Number of cases**
State body	1
Local government and its bodies	7
NGO's	2
Private commercial undertakings	31
Individuals	5

3. Decisions

In 2013, the Authority processed 40 Data Protection cases. At the time of the annual report's redaction, 4 of those were still pending. 35 of the 40 Data Protection cases result in an administrative decision. Some of the cases that were still pending by the end of 2012 were also ended in 2013.

Number of data protection cases ended by the end of the year (2013)	36
Administrative decisions	35
Terminated by orders	1
Pending cases	4
Total	40

The sanction that was used the most by the Authority were fines:

Fine's amount	Decisions
Minimal fine (100 000 HUF)	6
100 000 – 1 000 000 HUF	18
1 000 000 – 10 000 000 HUF	7
No fine	4

4. 2013's investigation strategy

The Authority designated three areas that are of particular importance, and which are stated as its priorities for 2013:

1. Data processing operations by websites, including the registration process from the point of view of users' rights. A strong emphasis was applied to the processing of children's personal data.
2. The electronic disclosure of information on local taxes.
3. Personal data processing operations by collection agencies.

5. Investigations of data processing operations by websites, registration processes, the enforcement of data subjects' rights on the Internet, and especially those of children (relevant cases)

During data protection procedures launched by the NAIH, some of which were started independently from received requests or complaints, the fixed goal was to undertake an overall investigation into data processing operations by websites. Among others, we wanted to evaluate the contents of information notices explaining data protection policies as provided by Art. 20 of the Hungarian Privacy Act, the registration processes, the scope of processed data, and finally the enforcement of data subjects' rights as provided by Art. 14 of the Privacy Act. In the frame of these procedures, the NAIH gave special attention to the processing of children's data.

The importance placed on minors as data subjects during our procedures was justified by the fact that, contrary to the former Data Protection Act, the new Privacy Act, in its Article 6 paragraph 3, provides that children over 16 have the right to consent to data processing operations independently from their legal guardians.

To determine the validity of legal statements and minors' consent to data collection, it is also necessary to take the Act IV of 1959 on the Civil Code (hereinafter: the Civil Code) into account. According to Article 12/C paragraph 1 of the Civil Code, only a minor's legal guardian, as his legal representative, may make legal statements in his name. According to Article 12/A, paragraph 2, of the Civil Code: "legal statements by minors enjoying limited legal capacity are valid only if accompanied by his legal representative's prior or subsequent consent, unless provided otherwise by other laws". Such a derogation is provided by Art. 6 paragraph 3 of the Privacy Act. By this provision, the legislator created special rules for minors between 16-18, but for minors between 14-16, consent by both the data subject and his legal guardian remains necessary, as provided by the Civil Code's main rule.

The NAIH encountered the case of a company operating several types of websites, including dating websites where it was usual to find registered users under the age of 16, who were able to register despite the absence of their guardians' either prior or subsequent consent. After this, the NAIH investigated several dating websites and observed that minors below 16 could frequently be found as registered users.

It is important to place the child's superior interests into highlighted account when examining their online activities and the data processing operations that concern them. This is particularly true in the case of social networks. Inside this category, dating websites represent the greatest threat. Indeed, unlike regular social networks where users communicate mostly with

known friends, the main function of dating websites is to meet new people. Given that services provided by dating portals to minors, and the data processing operations they infer, do not fall under the category of regular everyday acts that are usual and necessary to fulfil a child's basic needs, the NAIH believes that adequate consent can only be constituted along with the legal guardian's consent, and not only the child's one.

One must strive to enforce the above stated rules even if it is truly difficult to verify parents' consent. Otherwise, the website's owner or operator facilitates the availability of children for romantic or sexual relationships, which can contribute to their victimization.

We cannot close our eyes on the fact that children can appear on dating websites and be available on websites created to promote the establishment of new relationships. We cannot ignore, and thereby passively approve, such practices. This needs to be asserted even despite the knowledge that registration rules and processes can easily be circumvented. In that case indeed, the problem lies not in the data controller's behaviour, but in the field of child-parent relations, and becomes part of a larger social problem.

EU institutions also underline the importance of this theme (see the Article 29 Working Party's opinion 5/2009 on social networks, Recommendation 2006/952/EC of the European Parliament and of the Council of 20 December 2006, as well as the Commission's COM (2011) 556 report on children's protection in a digital world). It should be noted that Member States provide varying levels of protection. Only a small fraction of contents that are harmful for the healthy growth of children originate from Hungary. A far greater portion comes from other Member States and from outside of the EU. This renders the realisation of a unified protection strategy difficult. Until then, however, the NAIH wishes to enforce and achieve the maximal level of protection possible regarding data processing operations aimed at children, and also regarding the filtering of contents available to them.

This is why the NAIH investigated the registration processes of no less than 50 dating websites and tried to establish whether it was possible or not for minors to register without their parents' consent. Over the course of our test registrations, the NAIH was led to launch administrative data protection procedures against 18 websites. In total, about 4200 profiles[2] were found of minors below 16. The youngest user was only 10 years old. All of those profiles were available on-line, with the aim to help the establishment of relationships.

As a result, the NAIH imposed fines amounting to 2 900 000 HUF[3] in total (close to one million euros), and forced data controllers to erase relevant data and change their data protection policies.

2 If data from 2012 is also included, this figure is raised to 7700 profiles
3 If data from 2012 is also included, this figure is raised to 5 900 000 HUF

Over the course of the procedures, data controllers were globally cooperative, and deleted the illegally processed personal data, that is to say, the profiles of minors below 16. They modified their procedures and raised the registration age limit accordingly to our demands.

6. Common marketing databases

The NAIH investigated in the frame of an administrative data protection procedure the data processing operations of two companies operating marketing databases. The source of collected data was registration of the companies' websites. The two companies transferred shared the collected data between one another, and sent emails and SMS messages to the registered users. Telemarketing activities were conducted at a sub-contractor's call centre. Their aim was to advertise various banking and insurance products. Their partner would call people using the company's identity, to promote their own offers or that of others to people registered in either of the two companies' databases. Personal data was therefore received and used by the call centre, and not by the original data controllers collecting the data.

The NAIH established that the investigated operations did not comply with the adequate information requirements, and that the operation's indicated purpose ("marketing purpose") was too vague. There was a total lack of legal basis, for instance the data subjects' consent, for the transfer of personal data by both companies to a partner that was not even named in the general terms and conditions. Both data controllers also failed to provide adequate and precise information and ask for deliberate opt-in. Furthermore, the notification sent to the NAIH for prior registration purposes failed to mention all the involved agents.

Given the established infringements, the NAIH decided to impose a fine, request the adaptation of privacy policies and data protection practices to the Privacy Act's requirements, and require the deletion of illegally collected data.

Based on the above, it was also possible to establish that one of the companies working on the grounds of a data processing contract was not a data processor according to article 4 of the Privacy Act, but in fact a data controller.

7. Failure to comply with data security requirements – establishment of a data controller's responsibility following a hacker's attack (case number: NAIH-559/2013/H)

A company kept the data it had collected in the frame of a lottery game in order for direct marketing purposes, with the data subjects' consent. A group of hackers intruded on the server where the data was stored. They uploaded the stolen data on several websites, including names, e-mail addresses, phone numbers, dates of birth, city names and in some cases, the password. This data breach concerned more than 50 000 people.

Given the economic size of the data controller, the NAIH considered it to be its responsibility to implement the most efficient data security measures. This charge was aggravated by the fact that internal audits already brought attention to the fact that especially in the face of remote access, these data were not adequately protected.

The company ordering the realisation of the game and the sub-contractor both asserted that the other party was the data controller. Therefore, their respective roles had to be clarified before the NAIH could decide on each party's responsibility and thus on the fines it imposed.

V. Commenting on draft laws

The Hungarian DPA has been keeping statistics on its legislative advisory activity for years, which allows to draw comparison. Like last year, this annual report will include key figures on this branch of the Authority's activity. Some of the NAIH's competences are not mandatory, but practice has shown us that it is necessary to act and use them for the interests of data protection and freedom of information. This chapter will present the key elements of these activities in 2013.

1. Consultations

As an independent administrative authority, the NAIH collaborates with government authorities in the legislation drafting process. The Privacy Act provides for the possibility for the NAIH to comment on bills affecting data protection or freedom of information. The NAIH can also publish opinions calling for legislative amendments. This advisory function is particularly important because laws are of general application and affect the lives of all citizens. It is important for the NAIH to attract the legislator's attention to potential issues before legislation affecting informational rights is approved. The administrative advisory function can in many cases be a helpful tool to protect fundamental rights. However, in some sectors of legislation, and for various reasons, it does not always prove to be sufficient.

One such example is the large-scale development of IT infrastructure, for instance in the frame of e-government services. The decision to launch such projects is usually an executive decision, and the legislative process creating the adequate legal basis for it takes place at the same time as the technical work. Due to the volume of these investments, it is at that stage too late to amend legislative proposals in a way that affects strategic technical decisions.

Another example is the preparation of international treaties. Once the ratification instrument is submitted, it is too late to make any changes to the international commitment that was made.

The time constraint can also be observed in the quick pace of technical progress that keeps bringing new challenges to the legislator who must ensure the state's safety and the fundamental rights of the citizens, including informational rights. In the context of sharp market competition, IT R&D cycles become shorter, bringing ever quicker changes. The legal "R&D" cycle has to keep up with this pace if it wants to effectively regulate IT. An example of this was how it was recently necessary to step up legislative efforts to reinforce the security of governmental servers.

The above examples show that there are times when the NAIH's

opinion may arrive too late in the decision-making process. This is why it can be necessary to have new methods of cooperation with the decision-makers, earlier in the process. Consultations are one of the answers.

As an independent administrative authority, the NAIH is not compelled to take part in consultations and meetings about legal norms below legislative level, but it has so far accepted all the invitations when it was justified based on its domain of activity. For example, it took part in the preparation of the national IT security rules in the work groups led by the National Cybersecurity Coordination Council.

2. Monitoring the legislative process

In 2013, 181 bills were tabled by the government, while 257 were MP's bills. The majority of these bills were not preceded by social or administrative consultations that would have helped striking a balance between competing social interests. It should be stressed that a portion of these bills concerned very heavy, complex and large-scale legislative projects. This explains why the NAIH decided to monitor the legislative process very closely, which enabled us to forward our comments to the Parliament in a timely manner.

3. Publication of opinions on draft legislation

Since July 2013, the NAIH publishes its opinions on draft legislation on its website (www.naih.hu), in order to ensure the transparency of its advisory activity. We also believe that the availability of our opinions can be useful for government bodies seeking advice on informational rights in the frame of a decision-making process.

Statistical figures on comments of the legislation in 2013:

Legal instrument / year	**2011**	**2012**	**2013**
Act	85	49	86
Government decree	75	60	89
Ministerial decree	104	70	92
Government resolution	26	12	28
Other (parliamentary resolution, order…)	10	16	15
Total	300	207	310

VI. Investigation cases related to data protection

The main task of the Department of Investigations is to investigate incoming complaints. Besides this, it replies to the consultation requests it receives to help the enforcement of data protection guidelines. Last year, this department processed more than the two thirds of the NAIH's cases. These cases are then distributed among the three units of the department: data protection, freedom of information, and the new data protection audit unit. This chapter summarizes the main activities.

1. Political marketing

National elections and prior campaign periods have great significance also from data protection point of view, since personal data of millions of citizens can be transferred to the possession of political parties, nominating organizations and candidates in relatively short period of time.
The year of 2014 is special from several aspects: this is the year when not only the parliamentary but also the local self-governmental and the European Parliamentary elections will take place. This year will also bring the first proof of the new Act XXXVI of 2013 on Electoral Procedure (new Electoral Act) accepted in the framework of the reform of the new election system in Hungary.

The NAIH wishes to continue the tradition of the Parliamentary Commissioner for Data Protection and Freedom of Information to call publicly the attention of all the actors of the political campaign to respect the data protection requirements. From data protection point of view two special areas can be distinguished: the nomination process and the political campaign.

One of the novelty of the new system is that voters have the right to recommend not only one but more candidates. The name of the recommending voter, his personal identification number, his address and his mother's name shall be entered on the recommendation sheet, which shall be also signed by the voter by his own hand (Section 122 of the Electoral Act).
The election office – upon payment – shall hand over the recommendation sheets to the applicant without delay but not earlier than on the 48th day before the voting in the requested quantity. (Section 121)

Recommendations may be collected – without harrassing the citizens – by representatives of the nominating organisation or by the voter who wishes to stand as a candidate anywhere. The exceptions are precisely listed in the Electoral Act such as at workplaces, at service posts of the army and of central administration bodies, on means of public transport, in the official premises of the state or local self-governments, in educationial institutions, on the premises of healthcare providers. (Section 123)

The NAIH wished to draw the attention of the prospective candidates, the nominating organizations and all the participants who are taking role in the collection of the recommendation sheets to the following:

- There is no legal obligation to register the data processings with the purpose of the collection of recommendations to the data protection registry since this activity should be already registered by the election bodies. The exemption does not apply to preparatory data processings such as prior checking of phone contacts etc.

- Collection of the recommendation sheets shall be performed in a way which maximally respects the privacy of the citizens.

- No advantage shall be granted or promised to voters for providing a recommendation. No advantages shall be asked for or accepted by the voter to provide a recommendation.

- The data on the recommendation sheets shall be exclusively used for nomination purposes. The sheet shall not be copied and no duplicate registry shall be created upon the information of it.

- The recommending person shall not be named publicly. His personal data shall be kept confidential.

- The recommending citizen shall be granted the possibility to be able control the identity of the person who is collecting his recommendation sheet (through which the voter's personal and sensitive data will be also collected).

- Candidates and nominating organizations shall keep an accurate and up-to-date register in regard of those persons, who participate in the collection of the recommendation sheets in order to be able to inform the voters correctly or to clarify the possible infringements.

- The voters are firmly advised to control the recommendation sheet prior to signature. In case of any obligatory item in particular the serial number and the stamp of authentication put by the election office or the name and signature of the collector of the recommendation sheet is missing, it is reasonable for the voter not to sign the sheet.

The new legislation enables supplying personal data of the voters from the electoral register but it shall only be used for direct political campaigning purposes. Other use, copying and handing over to third parties shall be forbidden. The name and address of voters in the polling district electoral register shall be supplied upon request to the candidate by the election office operating alongside the election commission with competence in registering the candidate, or on request to the nominating organisation putting forward a list by the National Election Office. The supplied data shall be destroyed on the day of voting at the latest, and the record of the destruction shall be delivered to the election office that supplied the data within three days. (Section 153 and

155)

However, in accordance with the principle of the right to informational self-determination voters are granted the possibility to prohibit any release of their personal data by election bodies. In their request, voters may also limit or prohibit releasing their data pursuant to the Act LXVI of 1992 on Records of the Personal Data and Addresses of Citizens.

This regulation shall be also applied to political direct marketing methods.

According to the provisions of section 160 (2-4) of Act C of 2003 on Electronic Communications subscriber directories and address registers (e.g. phone books) may only contain as much data of a subscriber as is essential for the identification thereof unless the subscriber concerned clearly approves, on a voluntary basis, to the publication of more of his/her data. Each subscriber shall have the right to require the service provider, free of charge, to:

a) be left out from the printed or electronic directory;

b) 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;

c) indicate his/her address in the telephone books in part only.

Telephone calls directed to randomly selected numbers are only allowed, if the database of the provider serving as basis for the calls contains the data only of those selected subscribers, who gave their explicit and informed consent to the use of their data for such purposes. During the communication the concerned person must be informed about the data processing.

The NAIH wished to draw the attention of the prospective candidates, the candidates and the nominating organizations to the following requirements regarding data processings in connection with the political campaign:

- In case the candidates, the prospective candidates or the nominating organizations wish to forward campaign materials to the voters by the use of the central electoral register or of the records of the citizens' personal data and address the voters shall be informed about the source of information regarding their names and addresses.

- From public subscriber directories only those subscribers' data shall be used for contact purposes, who have previously given their consent to it. The consent regarding to the approval to publicising their data and to no disapproval of the use of their personal data for direct marketing purposes is supposed to be incorporated in the original subscriber contract.

- The use of telephone call systems generating automated and randomly selected numbers (including secret numbers or the phone numbers of those

subscribers, who have not consented to be contacted for direct marketing purposes) are not allowed to call since it may seriously infringe the privacy of the voters.

- A telephone call system generating automated and randomly selected numbers may be used if it is based upon and contains exclusively those subscribers' actual and public phone numbers, who have given their consent in the subscriber's contact to make their numbers public and have not prohibited the use of their personal data for direct marketing purposes. Such system may be also used in case of those supporters of the political party, who have previously and voluntarily provided their personal data for such a purpose to the data controller (political party, prospective candidate, candidate, nominating organization). Even in this case the possibility of interrupting the call shall be granted to the subscriber.

- Campaign materials shall be forwarded via e-mail or mobile phone exclusively to those voters who have given their prior and explicit consent to the use of their contact data to the prospective candidate, candidate or nominating organizations for this purpose.

- Prospective candidates, candidates and nominating organizations are obliged to apply to the NAIH for having their personal data processing for the purpose of political campaign registered in the Data Protection Registry. A clear distinction shall be indicated between a general data processing within the political campaign and a specific, distinguished campaign activity.

According to a traditional interpretation publicised personal data shall not be used freely for any further purposes.
Personal data may be processing only for specified and explicit purposes, where it is necessary for the exercising of certain rights and fulfillment of obligations (Act CXII of 2011 on the Right of informational Self-determination and on Freedom of Information, Section 4).
It means that further data processings shall always be carefully examined on a case-by-case basis to control whether the original purpose is in compliance or in contrast with the new purpose of the data processing. Furthermore, a clear distinction shall be made whether the original purpose of the publication of personal data was in connection with the data subject's private life or public life (public position, profession, business activity etc.)

The NAIH wished to draw the attention of the candidates and the nominating organizations to the following requirements regarding the use of public personal data for further political campaign purposes:

- It is forbidden to use registries containing data of private entrepreneurs and public registries of experts (e.g. registry of auditors) for political campaign purposes.

- In case of a direct mail sent via an intermediary the legal environment shall be thoroughly evaluated.

A frequently used (business and political) marketing tool for recruiting new clients, members or supporters is to contact a person who has already been in the register (first addressee) with the claim to recommend further persons (second addressees).

The NAIH wished to draw the attention of the candidates and the nominating organizations to the following requirements regarding the use of personal data of volunteers and supporters:

- Only those applications should be exclusively accepted which originate from a person who has already been registered in the own data base of the nomination organization or the political party.

- It is forbidden to maintain a „negative list" of those persons, who either explicitly refused to provide consent to the processing of their personal data and or simply did not confirm the contact message of the candidate or of the nominating organization.
The first addressees should be made aware of the requirement that transferring the second addressee's personal data is only acceptable if the data subject has been adequately informed and has given his consent to the data transfer.

Finally, one of the main principles of the Electoral Act is the publicity of the procedure (Section 2 (1) f))
The data processed by the election bodies are public only with a few exemptions regulated in the Act.
In the period between the calling of an election and the results of the election becoming final, the provisions of the Act CXII of 2011 on the Right of informational Self-determination and on Freedom of Information shall be applied by election bodies with the exception that requests for public information and for data public on the grounds of public interest shall be fulfilled without delay, but no more than in 5 days.

2. The NAIH's opinion on voice recording

Last year, the NAIH noticed an increased trend in complaints related to voice recording activities. According to the Privacy Act, voice recordings constitute personal data insofar as they can be linked back to the data subject.

Several laws provide for the mandatory recording of voice conversations. Act CCXXXVII of 2013 on Credit Institutions and Financial Enterprises provides that such institutions have to record telephoned

complaints. Insurance companies are bound to the same obligation, according to Act LX of 2003 on Insurance Institutions and the Insurance Business. These two acts indicate that data subjects must be given the opportunity, if they wish, to hear the recording of their voice. Data subjects can also get access to the minutes that were written based on the conversation, free of charge. However, this does not exclude, according to us, the general application of the Privacy Act.

The NAIH's official opinion is that both parties have the right to access the voice recordings. The data subject's access to them must therefore also be ensured. He must be able to hear the recording, and get a copy of it. Data controllers have 30 days to fulfil such a request. Copies must be given free of charge, unless this is not the first request by the given data subject for this specific data [see Section 5 Paragraph 5 of the Privacy Act]

3. Requests for access to personal data made by public authorities in the frame of criminal investigations

As was already the case in the times of the Data Protection Commissioner, the NAIH saw several cases in which data controllers rejected police requests for personal data.

Many plaintiffs complained about the absence of the prosecutor's authorization for the transfer of sensitive medical data. In another case, the complaint was about the request's scope. The police wanted access to all medical data from between 2008 and 2013 pertaining to data subjects born between 1970 and 1986. This plaintiff also requested a full opinion from the NAIH on the rules governing police requests for access to personal data.

The legal ground for police requests is that the legislator has granted police authorities such powers under Act XXXIV of 1994 on the Police, Act XIX of 1998 on Criminal Proceedings and, concerning medical data, Act XLVII of 1997 on Processing and Protecting Health and Connected Personal Data.

In Section 71 paragraph 3 of the Act on Criminal Proceedings, the legislator provided that personal data can only be disclosed to police institutions in the limit of what is strictly necessary for the request's purpose. The request must contain its specific purpose and the precise scope of requested data. According of paragraph 4 of the same section, data that has been collected through a request for personal data made by police forces, that is not strictly necessary for the set purpose, must be immediately deleted. The principle of purpose limitation must be enforced over the whole course of the data processing.

If the data controller deems a police request for personal data incomplete, the NAIH advises him to ask for further information and grounds.

They should further bring the police's attention to the fact that, in compliance with section 74 paragraph 4 of the Act on Criminal Proceedings, all transferred personal data unrelated to the proceeding must be immediately erased.

4. On CCTV's in condominiums, on access to documents held by co-ownership syndicates, and on notaries' new powers

Like in previous years, the NAIH received in 2013 numerous complaints related to the installation of closed-circuits television cameras (CCTV) in their buildings. In these complaints, plaintiffs often argued against the rules governing the use of these video cameras, the decision-making process, or the violation of data protection laws.

The Condominium Act provides the procedure for the implementation of CCTV systems in condominiums. The NAIH has observed that often, CCTV systems were implemented without the necessary 2/3rds of shares supporting the motion (which can take place through the written procedure of section 40 of the Condominium Act), and furthermore, the data protection policies are very often lacking.

There are also many cases when condominiums do not work as such, and where most of the provisions of the Condominium Act are not implemented. For example, no general assemblies of the co-owners are held, or there is no appointed common representative. In such cases, it is hard for the NAIH to intervene efficiently. Indeed, CCTVs can only be set up in such buildings if condominium rules are first implemented, which is something the NAIH's mandate does not extend to.

Like in previous years, the NAIH received a lot of requests for access to documents related the functioning of the condominium. The NAIH's official opinion however is that such documents are not personal data. As condominiums are not public bodies, these documents do not fall under the categories of information of public interest or of public information on grounds of public interest.

5. Investigations on data controlled by waste management public services

In 2013, like before, a significant portion of received complaints concerned the excessive collection of personal data by waste management public services. The NAIH handled these cases by examining whether local by-laws governing these services complied with the Privacy Act and with Act CLXXXV on Waste. The NAIH often found applicable by-laws to be worrying, for several reasons. In many municipalities, local governments still base their by-laws on waste management on Act XLIII of 2000, which has been abrogated by the currently applicable Act CLXXXV on Waste. Furthermore, many of the examined by-laws failed to address data protection issues. One of the municipal governments even tried to regulate waste collection and management via contract instead of regular regulatory acts. Based on Section 57 of the Privacy Act, the NAIH formulated opinions and advices to local governments concerned by these cases, to promote compliance with data protection requirements.

6. Data that can be stored for the use of electronic access control systems

Several complaints arrived last year regarding electronic access control systems implemented by mayor offices. Such systems are regulated under both the Privacy Act and Act CXXXIII of 2005 on Persons and Property Protection and on the Activity of Private Detectives. Under these provisions, property guards can ask customers to show their identification documents. In accordance with Section 32 of the Act it is possible to register the name and address of the person, but only to protect the entrance to buildings restricted to authorised personnel for security purposes. However, collecting the serial numbers of identification documents goes beyond the purpose of the personal data processing operation in question, and is therefore illegal. Furthermore, the NAIH reminded data controllers that they must adopt internal rules on data protection including information on the legal basis of the operation, its purpose, scope and time frame, the name of data processor and his contact information, as well as a limitative list of the persons who may access collected data.

7. Biometric systems

Some of the cases on biometric systems were consultation requests by organisations contemplating the introduction of biometric locks or entrance systems. Following its usual standpoint, the NAIH stressed that, given the provisions of Section 4 of the Privacy Act, it is necessary for the use of biometric systems to be adequate, relevant and proportionate to the fixed purpose. This infers the requirements for the necessity of the use of such data, its proportionality, and the strict evaluation of whether or not it would be

possible to achieve the same goal by other, less stringent means. Furthermore, the NAIH continued to base itself on the conclusions contained in opinion 03/2012 of the Article 29 Working Party on the development of biometric technologies, and especially those related to how the proportionality of such processing operations should be evaluated. According to such principles, a continuing concern are projects by schools to introduce biometric entrance systems. Indeed, such systems are not indispensable to either the safety of interested parties or that of school property. Finally, the desired purpose of such a system can be attained by less invasive means from the point of view of civil liberties.

The NAIH also examined cases where undertakings wished to implement a fairly common device, a fingerprint reader, on cash registers, to limit their access to authorized personnel. The NAIH reminded such companies that according to Section 10 paragraph 1 of the Labour Code, “only declarations or data relevant to the establishment of labour relations, the carrying out of this relation, or its termination, can be requested from an employee, and only as long as such requests do not violate his civil rights”.

According to the Labour Code, there are two conjunctive conditions that the employer must fulfil so that he can process his employee's personal data. Among the two, the fact that such a processing must not violate his civil rights is the most important one. If this condition is unfulfilled, then the other criterion becomes irrelevant. In examining whether or not civil rights are respected, one must take into account Section 9 paragraph 1 of the Labour Code, which provides that subjects of this law must have their civil rights respected. The rights of an employee may only be restricted if it is directly and without doubt necessary in the frame of the labour relations. Employees must be informed prior to the implementation of such restrictive measures.

Article 9 of the Labour Code provides for the general rules and main principles on the scope of employees' civil rights in labour relations, and on their potential restrictions. In order to protect such civil rights, the Law provides for two strict procedural obligations employers must respect. This procedure must be exclusively and directly tied to the employer's proper functioning. It may not exceed these boundaries. Even the notion of proper functioning is to be strictly interpreted. The employer may only decide to undertake such a procedure if it is obviously and objectively necessary. From this point of view, it is indeed relevant to take into account the employer's interest in making sure only authorized personnel is able to access cash registers and the money it contains. Controlling access to cash registers therefore fulfils the objective criterion of legitimate interest. But beyond this criterion, the Labour Code also enforces the criterion of proportionality. The Article 29 Working Party issued guidelines in this regard.

Based on the above, the NAIH established that the implementation of fingerprint readers on cash registers was not proportionate, as the purpose it fulfils can be attained through less invasive means in terms of civil rights, like cash registers with increased safety that could only be opened by the use of a

special code, given by the employer to its authorized employees.

One of last year's novelties in Hungary was the introduction of voice recognition as a biometric system. This technology is being actively developed. The Data Protection Working Party observed that “testimonials published by manufacturers report that, by implementing such technology, financial services companies have increased fraud detection rates and enabled a faster service to settle genuine claims.” This practice hasn't really taken roots in Hungary yet. Most service providers and producers are still working on introducing their products and services on the local market. In any case, the NAIH is keeping an attentive eye on further developments.

8. Official document copying practices of financial institutions

Every year the NAIH (first the Data Protection Commissioner, now the NAIH) receives complaints about financial institutions making copies of their customers' official identification documents.

All personal data processing operations must have an adequate legal basis and respect purpose limitation. Copies of identification documents do not constitute valid identification documents, voiding the purpose for which they were made. Asking customers to prove their identity with valid official documents is compatible with data protection rules, but making copies of these documents is not, as it violates the principle of purpose limitation.

Act CXXXVI of 2007 on the Prevention and Combating of Money Laundering and Terrorist Financing provides that financial institutions have to verify the identity of their customers when establishing contact with them. The financial service provider has to register a certain number of personal data on his customer, such as his name, address, type and serial number of identification document, citizenship, etc... However, this law does not allow financial service providers to make copies of official identification documents, and therefore, it does not constitute a legal basis for the processing of such personal data. It does not allow the collection of the customer's picture either, which can be found on such official documents. Copying the identification document, or taking photo from the customer, does not fulfil any legitimate purpose a financial institution, therefore violated the principle of purpose limitation.

Finally, copying official identification documents is a practice that should not be encouraged, in the interest of the protection of official documents. Indeed, such a practice represents a danger for the document's safety. Identification documents constitute "A" category official documents. Their illegal use or handling can violate administrative and criminal investigation interests.

This opinion was communicated in a letter to the secretary-general of the Hungarian Banking Association.

9. Personal data processing activities on the workplace

The number of complaints received on data processing operations related to labour relations increased between 2012 and 2013. This is due to the entry into force of the new Labour Code (Act I of 2012), which provides a possibility for employers to control technical tools (such as a computer or a cellular phone) used by employees in the frame of their work. The implementation of this new rule often raised data protection issues. Unfortunately, practice has shown that the wide interpretation of this provision by employers very often leads to the violation of the right to privacy and data protection of employees.

One type of recurrent complaint concerns the use of CCTV surveillance on the workplace. In the past few years, the tools at the employer's disposal to keep tabs on his employees has grown significantly. For example, it is now possible to track vehicles using a GPS-based technique, or to geolocate the user of a mobile phone using cell data.

Given the nature of the new Labour Code's provisions, on January 23rd 2013 the NAIH published a guide,on the basic requirements for the use of surveillance systems on the work place.

Often, employers fail to set out rules on the use of the professional email addresses, and yet still try to control their use and the content of messages during or after the end of a work relation with an employee. This can happen for example if the employer wants to investigate the alleged violation of a regulation by the employee. Another frequent type of case concerns the control of the employee's computer, including sometimes the copy of a computer's contents without the employee's consent.

Employees do not loose their right to privacy on the work place, but this right has its limits. The processing of some of his personal data by the employer can be justified in the frame of a labour relation. Employers must, however, abide by the data protection principles of the Privacy Act. Therefore, the control of technical devices lent by the employer to an employee for professional purposes, as provided by the new Labour Code, must be proven to be necessary to protect the employer's legitimate interests, and be proportionate to its purpose. This means that such a control can only happen if its purpose cannot be fulfilled through a less privacy-invasive mean. The NAIH encourages employers to fix rules in a preventive and proactive way in order to avoid later legal debates on the use of electronic communication devices by their employees for private purposes.

Instead of controlling the browsing history of their employees, employers are encouraged to implement preventive measures such as the implementation of Internet filters.

Employers must also inform employees of the rules governing the use of professional mobile phones. They may decide on their own of the purpose for which they offer employees the use of such mobile devices. As such, they may decide to allow, limit or forbid the use of these phones for private purposes, especially given the fact that they are paying the bills. The Labour Code allows the employer to perform controls over the use of professional mobile phones and related expenses. The NAIH's official opinion is that employers can ask mobile phone providers the user's bills provided that the last digits of the phone numbers be obscured.

It is particularly important to stress that controls are only legal if the data subject has been informed beforehand. Controls may only be performed in accordance with the provided prior information notice's content, and must restrict themselves to the professional activities of the worker. For instance, any communication or activity taking place outside of working hours (especially on weekends) pertain to the private sphere.

10. Data security trends

The data security principle is contained in section 7 of the Privacy Act. This principle provides that data controllers must take the necessary technical and organisational measures to protect access to personal data. Personal data must be safe from intrusion, illegitimate or accidental modification and erasure. Such data security measures contribute to the principle of purpose limitation. Natural persons should also take measures to protect their personal data. However, the Privacy Act does not apply to personal data processed for personal purposes.

A certain degree of leeway is given to data controllers to let them choose the type of security measures they want to implement. The Privacy Act does not provide for specific measures. Instead, it states data controllers are responsible for the security of the personal data they process, and if they have a choice between two or more protection measures, they should choose the safest one.

The NAIH has observed that in the past few years, data controllers have granted data security matters increasing attention. An example of this trend is provided by hard drive producers in the way they handle defective products sent back to the factory in the frame of customer warranties. If the product cannot be repaired, customers are sent a new model for free, while the producer keeps the old one. The problem with this practice is that, with the use of the bill and the warranty arrangement, it is possible to keep the link between the hard drive (and its stored data) and the data subject. Therefore, data found

on those hard drives are personal data. It is the NAIH's opinion that undertakings having access to the hard drives inform their owners about the way they will handle access to personal data and ensure compliance with the data security principle provided by section 7 of the Privacy Act.

A common data security flaw is when data controllers operating websites store user passwords in clear. This can be a problem in case of a data breach, especially considering the fact that many people use one password for several or all of their web services. Passwords must be protected not only from third parties, but also from people working for the data controller, who, generally speaking, do not need to know this password.

11. Data protection audits

Section 69 of the Privacy Act entered into force on January 1st, 2013, bringing a new duty and procedure to the NAIH: the data protection audit. Data protection audits are organised at the data controller's request exclusively. Data protection audits do not restrict the rest of the NAIH's competences, and the NAIH may refuse an audit if due to its limited resources, it would impede on the rest of its duties. Despite significant interest shown in this new service, only a few data controllers have come forward with requests. In 2013, 6 agreements were signed for data protection audits, 5 of which were completed.

Over the course of these audits, the NAIH observed that compliance with the formal requirements of the Privacy Act was acceptable, but a lot of worrying practices show that there is still a lot of room for improvement.

The most important shortcoming concerns data protection notices to data subjects. Documents examined by the NAIH showed that data controllers usually produce documents that only fulfil the formal requirements of the law and are often slightly edited copy-pasted excerpts from the Privacy Act. The NAIH produced examples of data protection notices that data controllers can use and that contain more and better information for data subjects.

The NAIH has come to the conclusion, from the experience gathered through these audits, that data controllers, when designing their processing operations, rarely take data protection matters into account. These considerations arrive only at a later stage of development, and are second priorities compared to profit or security. In some cases, reflection on data protection was not even included at all during the development process. This lack of planning reflects into the lack of knowledge on data protection of the involved agents. There is also a lack of internal documentation.

Another trend that could be observed during the audits was that more and more data controllers outsource their IT operations, including the processing of personal data, to external undertakings. Data controllers must ensure that data processors do not get into a position where they can make decisions on the data processing's purpose or the main characteristics of the technical operations, because if it were to be the case, then the data processor would need to be requalified as a data controller exercising joint controller together with the original controller. Finally, data controllers frequently forget to include the elements provided for by section 10 paragraph 4 of the Privacy Act defining the duties and responsibilities of the data controller and data processor.

One of the positive conclusions from the data protection audit is that data controllers requesting such an audit cooperate in a helpful manner with the NAIH and diligently implemented proposed improvements.

VII. Freedom of Information

1. Individual requests for access to information

Unjustified high fees for the duplication of documents; justified and unjustified elements determining these fees

Section 29 paragraph 3 of the Privacy Act provides the legal basis for charging fees covering the costs of duplication. Public bodies *may* charge such a fee, but this fee must not exceed the costs of making the copy. The Privacy Act does not mandate the setting of a fee, but only grants the possibility to do so. Indeed, freedom of information is best helped if public bodies abstain from charging a fee to citizens requesting access to information of public interest or public on grounds of public interest.

Despite the above, the NAIH has observed a trend, especially at local government level, where public bodies charge exaggerated duplication fees to try and hamper freedom of information.

Pursuant to the Privacy Act's provisions on requests for information, in conjunction with the Data Protection Commissioner's and then the NAIH's interpretation, duplication fees can only comprise the costs of materials. Citizens cannot be charged the costs of labour, energy or value added tax (VAT). This means that duplication fees are necessarily below market prices.

The NAIH determined, when asked in a concrete case, that for county seats and cities with county rights, copying a 100 page document does not constitute a significant work load. A 160 HUF per page fee was definitely exaggerated and constituted an obstacle to the exercise of the right to freedom of information. It is not legal to charge other costs than the strict costs of copy materials, and VAT is not of application.

Increased fees due to the scanning of documents

The Privacy Act does not make a difference between paper or electronic disclosure of data of public interest or data public on grounds of public interest. Only energy consumption costs may arise during the scanning of documents, which the Privacy Act's strict interpretation does not allow to be charged. However, it is possible that smaller public bodies do not possess the adequate material to carry out the digitalisation of documents. In this case, the public body in question may have to give the task to a private undertaking that will do the work for a fee. The Privacy Act allows to take these costs into account when determining duplication fees.

It is important when determining fees for the copy of documents to

take the scope of the request into account. With no or only small fees, it is possible for a public body to produce the copy of a small document of a few pages. But in the case of a particularly voluminous or complex request, it may be justified for a public body to charge a fee not only for paper but also for digital copies. Judicial case law states that market prices can serve as a guide to determine the fee. The Central District Court of Pest, in its decision of 9 May 2012 (case 10.P.87.319./2012/4), fixed the scanning fee for public information disclosure at 9 HUF per page in case of voluminous requests for information.

The absence of procedural rules pursuant to requests for information

The non-fulfilment of requests for information is often explained by the absence of procedural rules. It is often unclear, in an organisation, who is responsible for their handling. As a consequence, requests can be rejected simply because the public body in question does not possess the demanded information or document. In the absence of a clearly identified official in charge of access to documents, it is also difficult for a citizen to find out who he must turn to.

This is why the NAIH believes it is necessary to modify internal rules in order to identify who is responsible for freedom of information requests. In the absence of such rules, services and civil servants from a public body must communicate with each other proactively in order to collect and disclose the requested information in accordance with the citizen's request.

2. Complaints regarding compliance with electronic publication obligations

Like in 2012, many citizens turned to the NAIH in 2013 to complain about the fact that some public bodies failed to comply with their obligations as provided under chapter IV of the Privacy Act on the dissemination of data of public interest by electronic means. Such complaints mostly concern small local governments. Despite the fact that many of them operate websites while they have no legal obligation to do so, due to the absence of persons responsible for their maintenance and update, data published on them is often lacking, out of date, or unreliable. It would be a solution for such small local governments with limited resources to upload their data of public interest onto the www.kozadat.hu central open data portal. This operation does not call for particular technical skills. Yet this solution is often disregarded, sometimes even despite repeated calls by the NAIH to do so.

Websites

The Privacy Act does not mandate municipal governments to operate their own websites. Therefore, they may choose between several solutions in order to fulfil their duties on the dissemination of data of public interest by electronic means. For example, besides choosing, despite having no obligation to do so, to operate their own website, they can upload the data to websites operated by local government associations, to the central open data repository www.kozadat.hu or to the relevant Government Office's portal (see www.kormanyhivatal.hu). If data is uploaded on common websites, each municipality's data must be clearly and visibly separated.

The Local Government Regulation Database of the National Legislative Database

Pursuant to Government Regulation 338/2011 on the National Legislative Database, on June 30th local government regulations became freely accessible on-line, 2013. It is the responsibility of the Government Office to transmit local by-laws to the National Legislative Database.

The NAIH welcomed the introduction of this new system which significantly improved freedom of information in Hungary.

3. Transparency of public finances

Generally speaking the transparency of public finances lies at the core of freedom of information. In its 2013/21 (VII.19.) AB decision, the Constitutional Court declared the transparency of public finances to be a constitutional principal, based on the new Fundamental Law.

The NAIH had to examine several cases where the main difficulty was to determine whether commercial undertakings conducting business linked with national assets were public service providers under the provisions of the Privacy Act on freedom of information.

The Fundamental Law, in conjunction with section 7 of Act CXCVI of 2011 on National Assets, provides that the fundamental purpose of national assets is the provision of public services. The management of national assets must always be conducted in a way that makes the interests of public services, and public interest in general, the main priority.

The Act on National Assets provides that national asset operators must maintain a public register on the purpose for which assets are used, their value and their modifications. Only data that is to be classified under legal provisions are not to be published.

Pursuant to the Act on National Assets, State and local government

companies mainly provide public services. This is why they fall under the provisions of the Privacy Act on freedom of information, and must comply with requests for information from citizens. These companies must also comply with the obligations contained in the Privacy Act of dissemation of information of public interest through electronic means.

One of the most significant freedom of information cases involving the transparency of public finances was the access to the documents (notes, reminders) explaining the awards of a national tender on tobacco concessions. The K-Monitor Association of Public Interest turned to the NAIH in case NAIH-1169-2/2013/V to ask for an opinion on access to those documents.

Pursuant to Act CXXXIV of 2012 on Reducing Smoking among Minors and on the Retail of Tobacco Products (hereinafter: Tobacco Act), the Civil Code and Act XVI of 1991 on Concessions, anyone can have access to the contents of the notes, and Sections 28 and 30 of the Privacy Act are applicable.

According to the NAIH [NAIH-1700-7/2013/V] and based on decision 21/2013 (VII. 19.) AB of the Constitutional Court, that freedom of information, which is a safeguard for the rule of law, the principles of sincerity of public life contained in the Avowal of National Faith and of good governance can only be a reality if the notes of public calls for tenders and concessions are published, and made available to the public in a public and detailed fashion. A summary on submitted bids, and the full and detailed justification of the award, must be communicated to the public.

The National Tobacco Non-Profit Zrt's website only contained general information on the selection criteria, from which nothing could be learnt on the reasons behind the award or the rejection of individual bids. According to the NAIH, this violates the legislator's wish to encourage transparency. Concrete data on the notes should have been published.

Several court cases were initiated regarding individual bids and the access to the relevant documents. Some decisions have already been reached, but they do not constitute final judgments yet. In its decision nr. 70.P.23.269/2013/7 of 13 November 2013, the Capital Court, referring to the NAIH's opinion, ruled that the Ministry of National Development must disclose the names of the jury's members to the bidder, as well as the documents containing the reasons for the award or rejection of the bid.

4. The collision of the two fundamental rights (personal data protection and freedom of information)

The NAIH has to handle every year many cases where the right to the protection of personal data is in conflict with freedom of information. In such cases, the NAIH has to strike a balance.

The most obvious example of collision is when the Law mandates the disclosure of personal data, on grounds of public interest. For example, there is a law providing for the publication of certain data pertaining to the activity of civil servants. Several requests aimed at the publication of lists of civil servants. However, the NAIH tries to limit these attempts, since they are often in contradiction with informational right principles. Legal obligations to publish targeted personal data relating to the activities of civil servants in the frame of their duties is not to lead to the disclosure of their private lives.

On June 21st, 2013, Section 26 paragraph 2 of the Privacy Act was amended, and now states the following (the new text is in italics):

> The name of the person undertaking tasks within the scope of responsibilities and authority of the body undertaking public duties, as well as their scope of responsibilities, scope of work, executive mandate and other personal data relevant to the provision of their responsibilities to which access must be ensured by law qualify as data public on grounds of public interest. *These data may be disseminated in compliance with the principle of purpose limitation. Provisions on the disclosure of data public on the grounds of public interest shall be regulated by Appendix 1 of this Act and the specific laws relating to the status of the person undertaking public duties.*

There are still pending interpretation matters.

For instance, it is not clear whether the new provisions quoted above are applicable to personal data made public by Law in cases other than that of civil servants. Several legal norms provide for the disclosure of data on individual entrepreneurs or on the executives of private companies.

Lists of civil servants

The Klebelsberg Institution Maintenance Centre (abbreviated KLIK in Hungarian) asked for the NAIH's opinion on the publication of personal data (regarding names, status, salary or education level, for example) of its 140 000

employees (mostly teachers).

The Privacy Act's intention is to implement safeguards to ensure that the rule of law remains a reality, and to provide for the transparency of public finances. However, one cannot consider the matter of teachers' wages – which are without any doubt unfortunately well below the quantity, quality and importance of their work – from the same angle as that of the KLIK's executives.

Disclosure of civil servants' personal data must comply with the principle of purpose limitation. Asking to access documents and information in order to gain insight on the financial management of a public body is in line with the principle of transparency of public finances, and is legitimate. However, the disclosure of all professional data on 140 000 employees brings the risk that this data could be used to libel, slander or harass them. The disclosed information on an individual teacher's career may also, in certain circumstances, put him at a disadvantage on the labour market. Therefore, it is the NAIH's official opinion that such a sweeping request for information constitutes an abuse of law, as it is an attempt to use a fundamental right for an illegitimate purpose.

Access to information on local government officials

a) Assets declarations

One citizen asked for the assets declarations of a mayor covering the last three years, in order to publish them on an online magazine he operates. The mayor declared that he could only offer individual access to this data.

Act LXV of 1990 on Local Governments makes it an obligation for a mayor to publish an assets declaration at the time of his election, and then on a yearly basis. Based on this law's provisions, this declaration is public, and if it was not published for example on the local government's website, the mayor is obliged to disclose it to any body requesting it.

b) Access to information on official meetings and negotiations

Another person turned to the NAIH with a request for information concerning the time, place and involved persons in meetings with a mayor.

The NAIH stated that freedom of information only applied in this case if the involved persons were officials. Data involving private persons are personal data, and may only be disclosed under the Privacy Act with the consent of data subjects. However, if the mayor met with other officials, then he must, upon request, disclose the time and place of the meeting as well as

the identity of the involved people.

c) Access to information concerning days off taken by a mayor

Another citizen requested data concerning a mayor's days off between November 2012 and January 2013. The mayor answered that this was data related to his private life, and that he had no obligation to disclose it. The NAIH supported this point of view. Indeed, the link between the mayor's holidays and his duties as an official are tenuous. Disclosing the requested information would undermine the mayor's right to privacy in a disproportionate way.

Information stirring public attention

The NAIH received several requests for information by people wanting to know whether or not there had been requests for pornographic websites from clients within the Parliament's IT network. The NAIH stated in this occasion that the notion of information of public interest contained in the Privacy Act is not equivalent to the notion of information that the public opinion is curious about and that furthermore, the requested data, in this case, did not qualify as data of public interest nor as data public on grounds of public interest.

5. Data processing operations by court administrations

The role of freedom of information with regards to judiciary proceedings

The National Office of the Judiciary and its predecessor, the Hungarian Supreme Court have contacted us many times for consultations concerning specific data protection and freedom of information issues in relation with the work of the courts.

The NAIH has to – just as before the data protection ombudsman had to – face the controversial characteristic of disclosure of court procedures. From privacy point of view it is quite absurd that the audience of a courtroom may enjoy the closest view into the most intimate sphere of a marriage during the hearing of a divorce including the sexual life, health problems, financial matters of the husband and wife. On the other hand it makes no sense that people get no information about decisions of historical importance or nation-wide interested cases. It happens too often that the press gives detailed information on a crime committed just some days or weeks ago but remains

absolutely silent when the criminal procedure enters into the judicial phase.

There has been a serious dispute whether the data protection ombudsman or authority has the relevant competence to deal with issues of data processing of the judiciary. A consensus has been reached so far: what is a data processing in the sense of data protection terminology is a procedural action from the perspective of the court. The procedure of the court is being regulated by special codes of conducts and other legal norms in detail. These are thus the primary norms ruling the judicial procedures. These specific provisions are considered as lex specialis compared to the lex generalis ruling of the Privacy Act. However, it does not mean that the court may injure the right to informational self-determination of the data subjects during its own procedure when the primary legal norm on the specific situation fails to rule the concrete procedural or material action.

Publicity supports the effectiveness of the classical principles such as trust in the existing judicial system, faith in the Rule of Law and the control function of the society

The European Court of Human Rights stated that publicity is one of the main requirements of the right to fair trial, no matter in which case, in which procedure, at which level. It does not only protect the parties of the procedure from „secret ways" and „secret judgments" but also strengthens the public trust in the work of the courts.

The principle of the Rule of Law sets the requirement that „*the whole legal system, as well as the parts of it and also the concrete legal norms shall be clear, countable and apparent to the addressees."* (Nr. 9/1992. (I. 30.) Decision of the Constitutional Court)

Real time publicity

As far as social demands concern there has been a gradual development from the „publicity of the moment" to the level of complete and whole publicity on the internet. A „real time communication" such as twitter-(https://twitter.com/USSupremeCourt) and other online forum user journalists keep asking why not to broadcast live reporting from the courtrooms in interesting cases? The OpenCourt project makes a step further: it is an experimental project run by WBUR, Boston's NPR news station that uses digital technology to make Quincy District Court more accessible to the public. Anyone with an internet connection will be able to see and hear what goes on in court. (http://opencourt.wbur.org/)

The real problem would not particularly be with the nonstop reporting of the press but rather with the leaking information of the audience since the sanctioning of such action is not simple. In a British case: two jurors have both been jailed for two months after being found guilty of contempt of court for misusing the internet during crown court trials. One of them posted a message on Facebook, the other one used Google to research the fraud case he was sitting on at Kingston crown court and dig up extra information about victims, which he was said to have shared with fellow jurors. Both cases were brought to the high court by the attorney general on the grounds that the men's actions interfered with the administration of justice.

According to the interpretation of the Hungarian Constitutional Court the publicity of the court hearing gives guarantee against partial or unfair procedure primarily for the parties of the judicial trial and not for the „outside world", out of the mentioned personal scope.

The Hungarian Constitutional Court emphasises that court procedure is a tool for making a right effective. To turn to court is not a question of choice in most cases: the person has no no other way to enforce his right because either he gets involved in the case out of his will (e.g. becomes plaintiff or accused person) or he sees no other legitimate way to practice his right or to protect his legal interest. In this meaning participation in a court procedure shall man voluntarily resignation of data protection rights.
Generally speaking publicity of the hearing shall not bring automatically the free and detailed reporting about everything what there happens without the consent of the parties involved. It is true in particular for the personal data as of the name of the accused person in a criminal procedure: the full name shall be always mentioned in the courtroom but it does not give authorisation to the audience to make it public outside the courtroom.

In our opinion it is the official duty of the judge to ask for the prior consent of the data subject whether he is willing to be named in a press communiqué of the court or in a report of a journalist. Without such a consent it is not clear whether the data subject agrees or disagrees to be mentioned.

It is worth to mention that the press has its own responsibility on the media contents produced by the press. Section 4 (3) of Act CIV of 2010 on the Press says that „*Exercising the freedom of the press shall not involve or constitute the commission of a crime or abetting the commission of a crime, shall not be contrary to public morality, and shall not violate moral rights or result in personal injury under any circumstances.*"

If the future regulation gives green light to microblog reporting, the concrete cases of the exception from publicity shall also be mentioned (e.g. protection of children, of victims etc.). The NAIH's opinion is that limitation should not exclusively be based upon privacy interests but should also protect

the integrity of the procedure or the objective decision-making of the judge.

Media coverage

In the system of judicial communication the present legal regulation guarantees privileges for members of the press. Due to the classical principle of the independence of the judiciary the judges must not report on their own single cases and decisions in order to avoid any improper influence. But the speaker of the court may give information about the official opinion of the court even on single cases.

It is the privilege of the representative of the media to make audio and visual recordings during the hearing. Since the appearance does not fall within the scope of public appearance the procedural rules order to get the consent of the parties (accused person) as a permission for the recording.

According to the Code of Civil Procedure „*with the exception of the public prosecutor audio or visual recording is only permitted upon the clear consent of the parties and other actors of the trial, including the legal representatives, the expert, the witness, interpreter and holder of the object of review."*

According to the provisions of the Code of Criminal Procedure: making audio or visual recordings of the court hearing with the aim to inform the public is only allowed with the permission of the presiding judge. Recording of any person present at the court hearing – with the exception of the the judges, the clerk of the court, the public prosecutor and the legal representative - is only allowed with the consent of the data subject.

The ruling is clear: making audio or visual recording of the parties at a court procedure is only lawful if they have given their consent to it. However, the procedural rules give no clear direction on the publicity of the names of the parties. Thus we shall apply the Data Protection Act and follow the relevant Constitutional Court decisions respecting the right to informational self determination.

There is a special situation when either persons performing public duties or bodies with public service functions are involved. In these cases the future regulation shall interpret the limitation of publicity in the narrow sense.

In the case of other public figures all circumstances of the situation shall be taken into consideration. In particular how this person became a public figure (for example in the case of an actor or an artist), what is the subject of the ongoing trial and so on. The right to informational self determination shall be highly respected when the private sphere of the public figure is involved (for example a divorce case). The media shall ask for his consent when reporting

about his private affairs.

On the other hand when the trial is in connection with his public duty (for example in fraud or corruption scandals) the right to informational self determination of a person performing public duty might be limited with certain data protection guarantees. The limitation shall be necessary and proportionate for the sake of exercising justified general control of the public sphere.

In accordance with Section 26 (2) of the Hungarian Privacy Act the name and rank as well as other personal data of the person in connection with his tasks within the scope of responsibilities of the given public body – including his picture and voice, as well as his statements - might be disseminated. In relation with his other personal or sensitive data such as place and date of birth, health status etc. the limitation of his privacy right would not be justified.

It is worth to mention that in relation to other persons involved in the court procedure beside the person with public functions the data protection rights shall be fully respected (for example the active briber who is giving the bribery money to the politician). It means that their personal data can only be made public upon their consent.

The disclosure of decisions and anonymisation

Different legal systems offer various legal solutions to fulfil publicity demands. In some countries the judgments are available – sometimes for a fee - in collections. In other countries – like in Hungary – everyone may have access to them on the Internet for free.

To simply copy one country's model would be too dangerous because it is influenced by many cultural elements including the freedom of information regime and the importance of privacy protection in the given country.

Those legal systems which highly respect freedom of information the guarantee to have free access to judgments either online and also on paper should be incorporated in an Act. The text of the disclosed resolutions should be indexed to guarantee easy search. The Hungarian collection, which is also available online cope with these challenges.

The function of the publication of judgments has little to do with the original case and its parties. The dissemination neither serves the interest of the original case, nor is the aim to create a „wall of shame" but the main function is to share information on the judicial practice in general.

Court resolutions may contain information which is not meant for the society of the internet users, even though this information might be part of the publicly declared resolution. That is why the text of the resolutions shall be carefully selected but special attention should be paid not to shorten the useful information of the content. The key to the problem of this certain conflict of interests is the anonymisation of the resolutions so that the information loses its direct connection to the given data subject. Anonymisation does not mean a pure deletion of the names and addresses but it means a careful selection of the text to prevent unlawful dissemination of personal data. The parties of the court procedure should be identified through naming their position e.g. the plaintiff, the witness etc. According to the law there is no need to delete the name and rank of a person acting on behalf of an organ performing public duties, the name of the legal representative, the name of the NGO or foundation, the name of its representative and all the information which is made public on grounds of public interest. There is no need to delete the name of the respondent party if he loses the suit in case the law guarantees the recourse of *„actio popularis".*

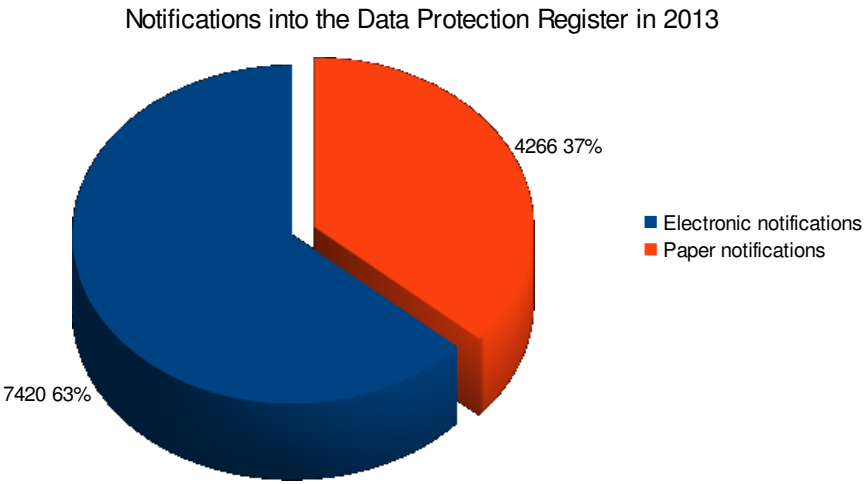
If the court session was partly or completely closed and the interest based upon the closure can not be otherwise guaranteed the resolution or part of the resolution shall be deleted from the collection. Classified data should also be protected but no other editorial revision should be carried out on the resolution. (780/K/2007)

VIII. Data Protection Register and Development of the NAIH's IT Infrastructure

1. Data Protection Register

In 2012, when the NAIH started its operations, it had to handle a large amount of pending notifications into the Data Protection Register inherited from the Data Protection Commissioner's Office. In 2013, the NAIH succeeded in closing those procedures and managed to bring back the processing time for each case to the legal deadline of 8 days.

Total notifications in 2013: 11686



2. The NAIH's IT infrastructure

The NAIH as a new autonomous administrative body (started functioning in 2012) is responsible for its own budget, functioning and all related duties.

In order to ensure the efficiency of our IT infrastructure, the Information Technology Department was created on February 1st 2013.

The National Assets Management Zrt (MNV Zrt) continued its renovation works on the NAIH's building. These works are expected to continue until 2014, but the third and second floors have already been fully renovated in 2013. However, some of the infrastructure development plans are dependent on lacking surrounding infrastructures. For example, the NAIH does not expect connection to the fibre-optic Internet network before 2015.

In 2013, the NAIH fulfilled its duties with its own independent resources and managed to hire personnel.

Besides their duties regarding the maintenance and operating of the NAIH's IT infrastructure, the IT Department supports the other departments with their expertises in investigations and data protection administrative procedures.

In May 2013, the NAIH launched project EKOP 1.1.7-2012-2013-0001 with the aim to modernise its IT infrastructure. The new infrastructure is expected to start operating towards the end of October, 2014. The new system is designed by bringing together functional and technical expertise in order to have it tailored to the needs of the NAIH's employees in exercising their duties. The NAIH will operate a new, modern website which will include customer service features, together with complex internal information, document and process management software. This software will need to be supported by adequate hardware infrastructure.

The new IT infrastructure is expected to replace the old computers inherited from the Data Protection Commissioner's Office and the quickly built, temporary website currently operating.

The following table gives a statistical insight on the visits on our website:

2013	Unique visitors	Visits	Visited pages	Hits	Downloaded content
January	5377	13560	60034	665147	20.97 GB
February	5026	9860	51083	566436	14.16 GB
March	5426	10659	47201	550115	14.85 GB
April	5632	9455	46622	599321	16.86 GB
May	5231	10698	39466	540804	18.19 GB
June	4630	8088	45786	523732	23.45 GB
July	4465	7965	58972	562285	34.13 GB
August	3971	6985	48276	477514	26.82 GB
September	4521	9536	58507	595929	36.02 GB
October	5263	9324	62796	659371	44.62 GB
November	5031	8960	187436	753708	49.44 GB
December	4099	7436	55072	524012	50.96 GB
Total	58672	112526	761251	7018374	350.47 GB

IX. Pictures, Conferences, Events

Attila Péterfalvi's presentation on Data Protection Day (January 28th, 2013)

The NAIH's press conference on its 2012 annual report int he Parliament's Gobelin Room (April 3rd, 2013)
Picture: Márta Hegedűs, Magyar Nemzet

Key to the World of the Net! – school presentation
Picture: Márta Hegedűs, Magyar Nemzet

Key to the World of the Net! – participation to a school's IT class

National Conference of Data Protection Officers, June 24th, 2013

Nemzeti Adatvédelmi és
Információszabadság Hatóság

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

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

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

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

ISSN 2063-403X (Printed version)
ISSN 2063-4900 (Online)