Annual report of the

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

2012

National Authority for Data Protection and Freedom of Information
Budapest, 2013

Introduction

„Herakleitos says, you know, that all things move and nothing remains still, and he likens the universe to the current of a river, saying that you cannot step twice into the same stream."

Plato: Cratylus, section 402a

Herakleitos' saying properly fits to the actual state of information rights taking into consideration the developments both in Hungary and worldwide. Not only the barriers between private and public spheres change but also the relevant technical means and regulations of data processing move and develop continuously – just think of the EU data protection reform process currently underway. I have also been watching the move of the stream personally for decades, what's more I have been striving to reinforce its sides for more than 25 years.

At the beginning of the '90s when I, as a young lawyer, was cooperating in elaborating the first data protection law of Hungary the challenges before the legislation were totally different. Following the system change from the dictatorship into the democracy the grounds of rule of law and, simultaneously, the institution of the data protection ombudsman had to be established.

As I was elected to data protection ombudsman by Parliament in 2001 I took over a well-functioning and publicly esteemed office from László Majtényi. Even at that time the organization indicated institutional tension frames since, due to the accession of Hungary to the European Union, the data protection law had to be amended and new authority competences, that are distinct from the classical ombudsman methods, had been conferred on the ombudsman. Slowly but surely steps were taken to set up a data protection authority and finally, in 2012, the National Authority for Data Protection and Freedom of Information **(hereafter: NAIH)** was established.

In 2011 the new Constitution recasted the system of fundamental rights. The new independent data protection authority, in compliance with the relevant international standards, could operate separately from the institution of commissioner for fundamental rights. Traditions and best practices from the former data protection commissioner's office may (and will) not waste; this is safeguarded not only by me and my fellow colleagues (the majority of lawyers now working for NAIH have previously worked at the data protection ombudsman's office) but also by the provisions of the new law. Besides the strong authority powers and competences (e.g. financial penalties, coercive resolutions) reflecting on serious data protection infringements the ombudsman-like, softer investigation methods remain operative; in the field of freedom of information exclusively, indeed.

The confidence of citizens keeps being sound; this is clearly displayed by the amount of incoming complaints and other petitions received by NAIH (altogether 2929 in 2012) or the increased interest from DPOs. In 2012 numerous European and EU committees of inquiry (Schengen expert group, LIBE, Venice Commission) scrutinized our operation and law and the final conclusions were always positive (what's more, the financial independence as well as the mighty authority powers of NAIH have been appreciated). Though, according to our findings, several provisions of the law could still be improved, the detailed proposes for amendment of NAIH can be found in the later chapters of the report. The infringement procedure brought by the Commission against Hungary before the Court of Justice of the European Union for removing the former data protection supervisor from office before time neither hampers nor restricts the domestic or

international functioning of NAIH, however, the final outcome of the procedure will render an important guidance for us, of course.
So, the year of 2012 passed, literally speaking, in the spirit of institution building, coping with a high workload and taking efforts to comply with strict international standards. I believe our Authority succeeded in overcoming these difficulties and I hope we will be able to perform our long-lasting strategies in a consolidated legal and technical environment in the coming years.

Finally, this way I would like to express my special thanks to the citizens and interested journalists for their attention and trust as well as to my colleagues for their hard work and support.

Budapest, 11th February 2013

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

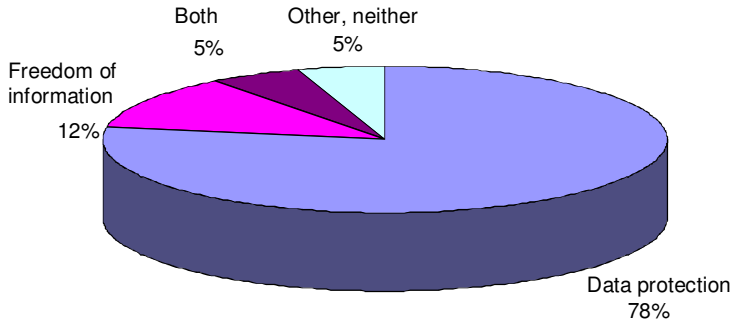
I. Statistical figures relating to the Authority

In the year of 2012 altogether more than 6500 postal and 8951 electronic mails were received by our client's office including documents received during investigations. Besides 1800 applications for registration into the data protection registry arrived; these applications were received to a separate email address. In the data protection registry 12.166 applications were processed in total.

3008 cases out of the overall incoming and internal cases were filed; 2929 investigation procedures as well as 33 data protection procedures were initiated. In comparison it is worth mentioning that the former Data Protection Commissioner received all in all 2274 cases to be investigated in 2011. An increase of 655 accounts for, partly, the takeover of files form the former Data Protection Commissioner that has already been examined by the NAIH.

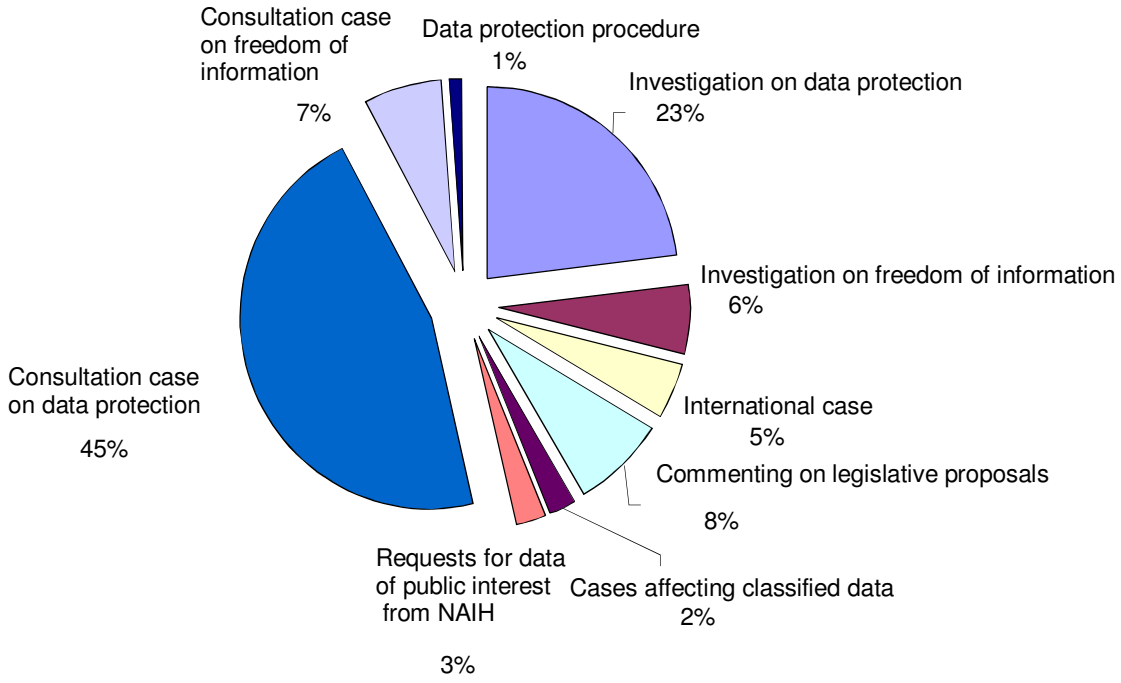
The scrutiny of 2550 out of 2929 cases completed until 31st of January 2013 thus a total of 379 investigations to be performed have remained in 2013 from the preceding year, consequently, 87% of cases could be settled in the first year.

Branches of information rights in 2012 complaints
(without applications into the data protection registry)



In 2012 investigated altogether 207 cases affecting legislative proposals and put forward wholly 46 legislative amendments. 35 submissions were transferred to the Parliamentary Commissioner for Fundamental Rights and other institutions. In the cases investigated we rejected 226 submissions affecting data protection and 14 submissions affecting data of public interest that is less than 8% of overall cases scrutinized.

Ratio of cases under investigation on the merits 2012



Investigations on the merits were carried out in 2152 cases, 1825 of them (85 %) affected data protection and 327 (15 %) affected freedom of information. Infringements were concluded in 514 investigations, 419 of them revealed breaches related to data protection and 95 of them exposed infringements (or its imminent danger) related to publicity of data.

1388 cases out of the total cases under investigations on the merits were consultation cases, that is to say, the petitioner does not require a concrete data controller to be scrutinized but requests information and guidance on the conditions and legality of an actual data processing activity. 1212 cases out of the total consultation cases affected data protection and, largely, the data protection registry as well as the conditions thereof, 176 cases in turn affected the disclosure of data of public interest as well as the obligation of disclosure.

The total number of international cases was 109, however, altogether 130 investigations with international relevance (involving foreign data controllers or processors) were performed. 56 cases affected processing of classified data.

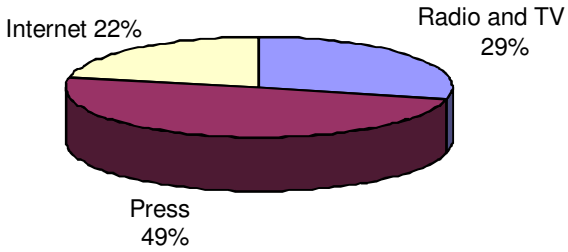
69 requests for data of public interest were received by NAIH, all of them were answered within 15 days set by law. This high number clearly indicates that a lively interest was shown towards the NAIH following its establishment in the first year. In comparison, the former Data Protection Commissioner received only 19 requests in 2011. The NAIH refused to disclose data of public interest only on one occasion, with regard to the nature of the data being part of a decision-making process, however, once the decision (the finalization of rules of data protection audit) had been made the request for data of public interest was, of course, performed.

In any event, it can be considered a success that the new supervisory authority, with a partly new legal background, on a new location and under different technical circumstances, succeeded in coping with the remaining files and cases taken over from the former Data Protection Commissioner and, simultaneously, was able to investigate the new incoming submissions. The increased number of cases clearly shows the confidence in NAIH, an organization dedicated to protect information rights, its recognition and reputation. In light of the above we can conclude the changes in the structure of institutions of fundamental rights did not result in a disruption, on the contrary: the protection of rights became even swifter and more effective. Detailed information on data protection, investigation, international and data protection registry cases can be found in the net chapter.

The presence of NAIH in the media between 1st of January 2012 and 31st of December 2012

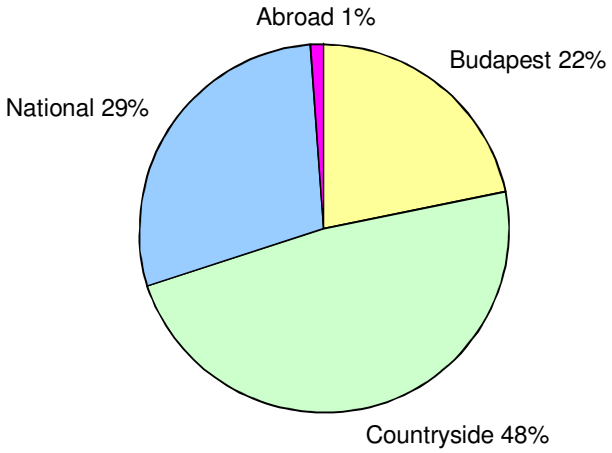
In the year of 2012 the Authority appeared totally 1238 times in the television, in the radio, on the internet and in the press (altogether in 133 media). These media appearances involved oral and written statements, interviews and communications as well. The Authority appeared in TVs and radios 356 times, in the press 278 times and on the internet 604 times.

Ratio of appearances by media 2012



(source: Observer)

Appearance in the media by territorial division in 2012:



(source: Observer)

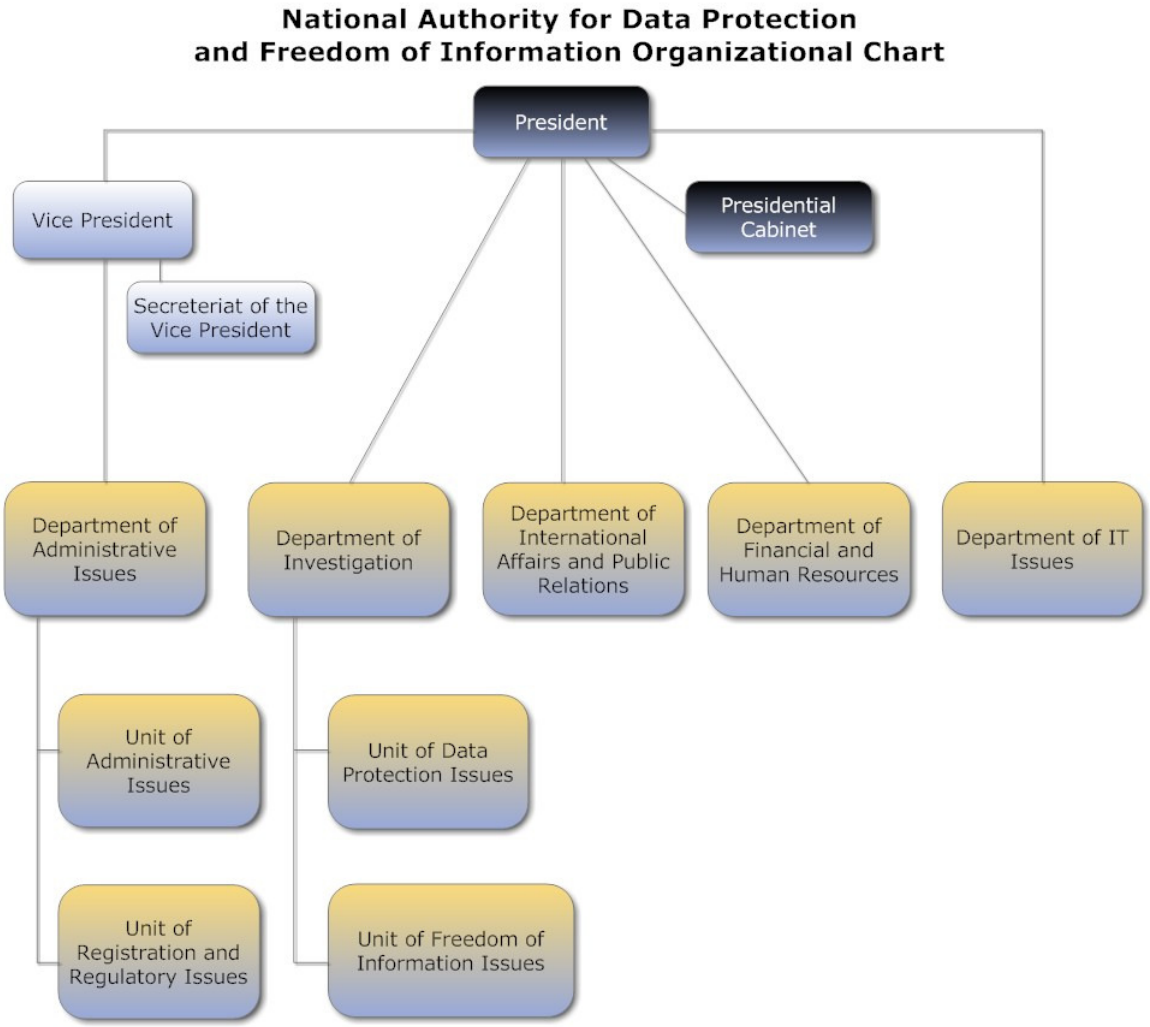
II. Budget, financial management and staff of the Authority

The total staff of the Authority of 59 was allocated only at the end of 2012.

Fulfilment of appropriations for payments on 31st of December 2012 (in thousand HUF)

Legal ground	Amended appropriations	Fulfilment of appropriations	Residual items with commitment
Personal wages	210 267	209 408	859
Employer's health & pensions levy	55 452	55 152	300
Supplies	89 372	77 298	12 074
Investments	35 120	29 971	5 149
Total:	**390 211**	**371 829**	**18 382**
Operating income	622	622	-
Subsidy	389 589	389 589	-
Total:	390 211	390 211	-
Altogether:	**390 211**	**390 211**	**-**
Budgetary balance reserve for the chapter	12 100	-	12 100
Expenditure savings:			18 382
Income shortfall:			-
Residual items with commitment:			**18 382**
Residual items without commitment (Budgetary balance reserve for the chapter):			12 100

The below chart illustrates the organizational structure of the Authority on 31st of December 2012.



III. International affairs

The NAIH dealt with more than 100 cases of international relevance in 2012. Besides cases filed we received various inquiries via informal and direct channels, e.g. through data protection conferences in Hungary, with respect to, principally, the transfer of personal data of employees abroad as well as whistleblowing systems. As of the 1st of January 2012, pursuant to the Act CXII of 2011 on Informational Self-determination and Freedom of Information **(hereafter: Infotv.),** it became possible to transfer personal data from Hungary to third countries not only by virtue of the data subject's consent but also to countries that ensure an adequate level of protection and respect the general data processing principles (thus abandoning the rule of the former DP law accepting exclusively the data subject's consent). However, data transfer to third countries failing to ensure adequate protection is allowed in a very little scope only. Both general contract terms and conditions elaborated by the European Commission and ad hoc contracts and BCRs were left out of legal bases as well as individual legal bases approved by the national DPA shan't apply. It is up to the Hungarian legislation to decide whether it is willing to settle this issue by means of a legislative amendment. It is also problematic that, pursuant to Section 10(2) of Infotv., it is forbidden to appoint another data processor – this provision contravenes the explicitly permissive regulations of Commission Decision 2010/87/EU.

The international organizations and colleagues from abroad (for instance Mr. Peter Hustinx EDPS at his visit in Budapest in October 2012) were enquiring primarily into the evolution of the new data protection authority. Due to the infringement procedure against Hungary for removing the former data protection supervisor from office before time the competences and operation of NAIH, established as of the 1st of January 2012, were scrutinized in detail by several European committees of inquiry (for example: LIBE, Venice Commission, Schengen Evaluation Committee) and the final comclusions have always been congruous: the provisions of Infotv. comply with the EU standards, the competences and powers of NAIH are to be considered broad compared to other DPAs and its financial independence, also in a European context, deserves a high rating.

Our Authority took part in numerous international surveys including, at first place, a research aiming at assessing the effectiveness of data protection redress mechanisms available to citizens coordinated by the European Union's Fundamental Rights Agency (FRA) seated in Vienna. In this survey the opinions and findings of all stakeholders concerned – DPAs, citizens, judges dealing with data protection cases, attorneys and NGOs – had been compiled by similar research methods in all 27 EU Member States. In Hungary the NAIH strived to support the international research by delivering statistical data, personal interviews and exploring citizens wishing to participate as well as by supplying prior evaluations on the results of the research.

Budapest Case Handling Workshop

As a confirmation of our inclusion into the international engagement was that the new Hungarian DPA hosted the regular expert meeting, focusing principally on practical challenges of privacy, of European DPAs in September 2012 (Budapest Case Handling Workshop, 3-4 September, 2012). Major items of the agenda prepared by a prior survey included the data protection procedures, the judicial revision of DPAs decisions as well as data protection audit though on the 2nd day of the conference, in alternative panels, roundtable discussions were going on the data processing activity of religious associations and the privacy issues of HIV infected

persons. Feedbacks from the 52 participants on the effectiveness of the workshop were positive, indeed.

Participants of the Budapest Case Handling Workshop (3-4 September 2012)

Schengen Information System

The NAIH, as the national authority with supervisory powers, was, by means of preliminary controls, monitoring the Sirene Office of the National Police Headquarters (ORFK) in charge of processing and transferring Schengen related data and the National N.SIS IT Central Office (KEKKH) at the beginning of the year. During the year we were inspecting the functioning of the SIS system at the Hungarian Consulates in Beregszász, Kiev and Moscow as well as the border crossing point at Beregsurány on the spot.

In 2012 we handled altogether 12 requests for information from individuals regarding SIS (mainly from foreign nationals, in several cases forwarded by partner DPAs) – this is a huge increase compared to the preceding year's figures. This remarkable interest may have been a consequence of a Schengen information campaign to citizens launched by the NAIH in March 2012 that had been realized in various forms of information leaflets (news sites, county dailies, NAIH website, on all Hungarian foreign representations' and government websites and in paper format as well) in Hungarian and English language.

In the fourth month of its existence (which posed a "*special situation*" to experts as well) the NAIH could prove its craft and skills before a strict EU monitoring committee in the framework of a Schengen data protection evaluation mission between 17-20 April 2012 that was coordinated by our Authority. Representatives of stakeholders concerned – the NAIH, Sirene Bureau of ORFK, KEKKH and the Ministry of Foreign Affairs in charge of data processing of Hungary's foreign representations – responded to all questions, both at lectures and onsite inspections, that affected the adequate and safe operation of SIS from a data protection perspective. The experts

scrutinized the relevant legal background and the amendments of law, competence and powers of, the theoretical and practical operation of SIS, the redress mechanism, the rights of data subjects, complaints, the appropriate information of citizens (website and leaflets in Hungarian/English, information to consulates on the establishment and powers of NAIH), the results of preliminary NAIH investigations, the findings of the preceding 5 years (counted from the previous assessment), our engagement in international investigations. The committee final evaluation was positive; simultaneously it has been specifically highlighted that the new Hungarian DPA disposes of broader competences concerning the protection of citizens than those of the former Data Protection Commissioner (the rapporteurs encourage the recipients to make use of legal instruments provided by the new competences). Our information activity respecting SIS received an excellent qualification while the number of colleagues dealing with Schengen cases should be increased.

The issue of Schengen weighed the agenda of the legislation highly in 2012 since the SIS II Act and the relating government decree was adopted in the previous year. Several inter-ministerial task forces (legal, IT), to which the NAIH was also invited to be involved, had been set up to prepare the relevant legislation. The development of SISII, the 2nd generation of the system (its legal basis are SISII Regulation and SISII Decision), has been one of the most significant IT project of the EU. The new system will provide various additional services, compared to the currently operating one, including the capability of storing photos and fingerprints. The Hungarian law, transposing the EU Regulation and Decision, contains specific provisions on the application of the system for the purposes defined in Title VI. (formerly 3rd pillar) of the Treaty on the European Union (TEU). Moreover the law outlines in detail what categories of data (warning signals referring to persons or objects) shall be entered into the system for the purpose of promoting operative cooperation in criminal matters among law enforcement and judicial authorities furthermore the purposes of data inputs, the criteria of data inputs and data process as well as the authorities entitled to right of access. For the time being the practical testing phase of SISII is underway in Europe.

Finally we must mention that our Authority plays an active role in numerous expert groups both on international and EU level as follow:

- International Working Group on Data Protection in Telecommunications (IWGDPT)
- Joint supervisory bodies of the European Union (JSB Europol, JSA Schengen, JSA Customs and other monitoring groups)
- Article 29 Working Party (Art 29WP). The experts of NAIH are also actively taking part in the following subgroups of Art 29WP:

1. Future of Privacy subgroup
2. Technology Subgroup
3. E-Government Subgroup
4. Border, Travel & Law Enforcement subgroup

IV. Data protection cases

A novel procedure

The NAIH can rely on large scale experience regarding the investigation procedures of the preceding years because it can make use of findings of the former DP Commissioner. This practice is useful in the data protection procedures as well; however, different aspects have to be taken into account compared to the ombudsman-like protective attitude. Data protection procedures are based on clearing up the facts and acquiring evidences along with the proper application of procedural rules.

The NAIH has been expected to apply the rules of the new data protection procedure. Due to this novel course of action the NAIH have had to elaborate the proceedings, to evaluate the prior experience and to develop the future strategy in the 1st year of its operation. Furthermore it wished to apply all the authority powers conferred upon it and took firm actions in cases of data protection infringements.

In data protection procedures both the General Rules of Administrative Proceedings and Services (hereafter: Ket.) and the Infotv. are to be applied together or the Ket. shall be applied in compliance with Infotv. The joint interpretation of these laws raised several operative questions and legal problems. Numerous provisions of Ket. allude to other laws – e.g.: *„law may prescribe"*, *„in the scope determined by law"* – in these cases the provisions of Infotv. complement those of Ket.

Our Authority acted in the following matters during data protection procedures:

- Data processing related to real estate advertisements
- Storage of documents of companies dissolved
- Unlawful dispatch of electronic circulars
- Disclosure of personal data of dwellers in a condominium
- Data processing relating to money transfer
- Deny to access to health data of the data subject
- Data processing of the *„social consultation"*
- Organizing of product tours
- CCTV surveillance
- Data processing upon opening a "Start" deposit account
- Online disclosure of documents of an authority procedure
- Transfer of insurance secrets
- Sending unsolicited SMS messages
- Data processing concerning dwellers of government housing estates
- Inspection of a social registry
- Online registration, dispatching newsletters
- Data processing of a fitness centre
- Data processing of *„discount-card"* systems
- Disclosure of personal data of local taxpayers
- Data processing considering report into address records
- Data processing respecting online *„promotion"*
- Claim management
- Data processing of high school students

Statistical figures on official decisions

In the year 2012 we had 33 data protection procedures. The majority of procedures was launched as a consequence of complaints or submissions, 5 cases were initiated without preliminary petitions. 17 cases out of 33 were underway on 31st of December 2012.

7 proceedings began in the 1st half of the year while the remaining 26 cases started in the 2nd quarter (15 out of them in the last quarter) – that's why the examination of numerous cases expanded into the next year. In some cases the procedure lasted for months due to the difficulties having arisen out of the clarification of facts.

In the year 2012 we had 16 data protection procedures fully completed. 3 out of them was terminated by orders, (in 1 case an infringement could not be concluded whilst in 2 cases the facts, needed to issue a decision, could not be clarified). 9 cases could be concluded by a decision, 4 additional decisions were made in January 2013.

In the decisions data controllers, obliged to terminate unlawful data processing or to pay a financial penalty, involved 5 companies, 1 financial institution, 1 health fund, 5 state or local authorities and 1 private person.

Pursuant to Section 61(1) of Infotv. the majority of decisions required the termination of lawful data processing activities while in 1 case the NAIH ordered the deletion of personal data processed unlawfully.

11 out of 13 decisions include financial penalties. (We imposed the maximum financial penalty of 10 million HUF once while the minimum amount imposed was 100 000 HUF three times - in the remaining cases the amounts varied between the limits.)

Four decisions had been taken to court out of which in 2 proceedings the court ruled in favour of NAIH.

Final court rulings delivered in lawsuits that had been launched against NAIH decisions imposing fines

From the 1st January 2012 on the NAIH may impose fines in cases of severe breach of data protection regulations against which a judicial remedy is available. In 2012 two cases were brought before court where the court ruled in favour of NAIH and sustained the decisions imposing fines.

In one case (Capital Court of Budapest – 2. K. 31. 506/2012/8.) the data controller was keeping documents, containing both general and special personal data, of various companies in an open barn without supervision.
Our Authority imposed a fine of 5.000.000 HUF against the controller on failing to take security measures and ordered the controller to pass on the documents to the competent institutions. Though the controller took the case to court the final judicial verdict denied the action of the controller and sustained the financial penalty, imposed by our Authority, affirming the position of the NAIH that the breach of relevant data protection regulations may have affected a wide scope of data subjects.

In another case (Capital Court of Budapest – 26.K.32.704/2012/5.) the data controller – an insurance company – rejected the multiple requests of the data subject to disclose a medical

expert report, containing health data on the data subject in question, alleging that the document is dedicated solely for internal use. Thereafter the data controller was required by the NAIH as well to disclose the documents. Since the controller failed to do so a fine was imposed on it. However the case was brought before court the final judicial verdict denied the action of the controller and sustained the financial penalty, imposed by our Authority.

Disclosure of NAIH decisions

Resolutions of NAIH are generally made public on our website taking into consideration the relevant legal conditions stipulated by Infotv. and Ket. According to the Infotv. the decisions shall be made public if it is deemed necessary in the interest of data protection or a wide scope of data subjects.

The Ket. also stipulates that the resolutions shall be made public if more than 50 individuals are affected or more than 5 NGOs, acting in the field of human rights, are concerned or an imminent danger is foreseeable.

V. Commenting on draft laws

Activity of NAIH regarding the legislation

The NAIH is not a legislator but a law enforcement authority, however, it plays a vital role in the preparation of legal instruments including either commenting on draft laws in an administrative process or own proposals. This is envisaged in Section VI(3) of Fundamental Law which stipulates that protecting personal data as well as facilitating the exercise of freedom of information rights fall within the scope of NAIH. That provision also implies the involvement in drafting laws that affect these domains.

Even though, formally, the NAIH started to operate without a legal predecessor as a novel institution in 2012 its functions concerning drafting laws date back to the former Data Protection Commissioner's era. This enables us to illustrate the NAIH's functioning related to legislation in the dichotomy of constancy/alteration taking also into account the former Commissioners' positions.

Commenting on draft laws

The opportunity for the NAIH to comment on legislative proposals/amendments affecting data protection & freedom information has not varied.

Statistical figures of comments in 2011 and 2012 as follow:

Legal instrument/year	**2011**	**2012**
Act	85	49
Government decree	75	60
Ministerial decree	104	70
Government resolution	26	12
Other: (parliamentary resolution, order etc.)	10	16
Total	**300**	**207**

Adoption of the Act LXIII of 2012 on the reuse of public sector information was a cornerstone in the legislative process considering freedom of information issues. The Minister in charge of preparing the draft legislation asked our Authority, in the first weeks of its operation, to formulate opinions concerning the draft. The NAIH, supporting the proposal, put forward suggestions, in the course of multi-round talks, that were intended not only to comply with EU legal harmonisation requirements but were also advantageous in terms of data of public interest. It is essential that a clear distinction shall be made between the need for disclosure of data of public interest and the reuse of public sector information (PSI). If the petitioner does not explicitly indicates his/her objective of reuse of PSI then the petition shall be judged in accordance with rules applicable to disclosure of data of public interest even if the data concerned are categorized by law as being PSI. A crucial principle is that the petitioner may not

be obliged to determine the purpose of his request to disclosure therefore, in the absence of indication to PSI reuse, he may not be obliged to make a statement in this regard. During the discussions a consensus was reached that the enactment of PSI reuse might not lead to such an amendment of the Infotv. which would hinder or restrict the disclosure of data of public interest. In our view this legislative goal has been completely attained. (NAIH-1489/2012/H)

Initiation of a subsequent constitutional revision at the Constitutional Court

The former legal regulations had empowered the Data Protection Commissioner to initiate a supervision procedure at the Constitutional Court if some legal instruments were presumed to have violated the Constitution or international treaties. Following major modifications in this respect the currently effective Infotv. does not entitle the President of the NAIH to bring cases before the Constitutional Court. To overcome this deficiency two operational solutions occurred.

1. The President of NAIH has been authorized by law to, in a proactive/"soft" manner, propose recommendations still in the course of the legislative process. This option will be illustrated in the following chapter.

2. Due to the flourishing professional cooperation between the NAIH and the Commissioner for Fundamental Rights (CFR) we are confident that, temporarily, the President could turn to the CFR with the objective of launching a supervision procedure.

In the long run it were a possible solution if, by amending the Fundamental Law, the President of NAIH would be entitled to initiate a subsequent supervision procedure before the Constitutional Court. Alternatively the President would be entitled to turn to CFR suggesting him to appeal to the Constitutional Court in cases where privacy/freedom of information rights would be endangered. Should the CFR fail to do so he would be obliged to specify the grounds of rejection in his annual report.

Involvement in the work of committees of the Parliament

A new opportunity for the President of NAIH, compared to the preceding regulations, is that he has become entitled to attend and address the meetings of parliamentary committees. This is useful in influencing the legislative work respecting information rights. Below some examples where the NAIH intervened successfully.

- A draft bill on geodesy and cartography, according to the position of NAIH, would have restricted the access to such data of public interest. The NAIH emphasized that the disclosure of such data shall be made in a way easy to understand to everyone. Following the intervention of our Authority the proposer informed us he had revoked the bill (NAIH-4094/2012/H).

- Another bill intended to amend the Act LXVI of 1992 (Act on the Name and Address Records of Citizens – hereafter: Records Act) with a view to grant access to these records for the Government Control Office (KEHI). The amendment had anticipated the KEHI would be empowered to gain access to personal data to such an extent which could be equivalent to that of other law enforcement authorities (police, national security services etc.). Following the intervention of our Authority the passages of the bill in question were deleted (NAIH-6047/2012/V).

- Another bill, involving also data transfer to EUROPOL system, was modified as the subsequent recommendations of NAIH had been taken into account. (NAIH-4915/2012/H)

The NAIH scrutinized a bill on national security clearance numbered T/7961. The bill would have replaced the actual system of national security clearance carried out from time to time with a model performed continuously. As a consequence an intrusive method of security investigation would be put in place restricting the privacy of the data subject and his/her domicile as well as affecting thousands of individuals.

The proposed novel system would have enabled to perform security inspections for a longer period without appropriate objective thus creating an uneven information situation between the state and its citizens. This would have seriously exceeded the necessary restrictions on privacy rights. As a result of our inspections we had found that no similar regulations are in effect in other democratic European states. Security clearances, performed without a sound suspicion and for a longer period, are not in conformity with privacy rights and fundamental data protection principles.(NAIH-4867/2012/J)

VI. Data protection – the most important cases

Data processing of Google Street View

The investigation of Google Street View (GSV) service had been commenced by the DP Commissioner in 2009. The purpose of Google's photo taking is to enhance the service of Google Maps application. It shall be mentioned that during photo processing operations the faces of individuals and car license number plates are blurred so that privacy rights are not infringed. As the Commissioner was advised on the intention of Google to launch the GSV he recommended to suspend this activity for the lack of clarification on what constitutes sufficient legal basis, how data subjects can exercise their rights of consent, information and objection during taking photos by GSV. Following that Google interrupted its activity and initiated cooperation with the DP Commissioner's Office. Finally the Commissioner issued a statement in May 2011 with regard to GSV in which he stated that if Google fulfilled the data protection requirements set out in the statement the purpose indicated by Google could not be challenged.

In 2012 there were several discussions between the NAIH and Google in order to clarify the conditions of lawful photo taking operations. Our Authority also invited various mayors and city councils to formulate their positions on GSV. The local authorities surveyed expressed their full support to the introduction of GSV which was taken into consideration by NAIH at delivering its position on the case. On 23rd of January 2013 the NAIH delivered a final statement concerning GSV emphasizing that a prior consent from data subjects could be seen as an unreal expectation to be met by the service provider. Another ground for issuing a final statement was a judgement (C-468/10 and C-469/10 unified cases) of the Court of Justice of the EU (ECJ) stating that the Art. 7 f) of Directive 95/46/EC has direct effect.

The main feature of taking photos, from a data protection perspective, is a systematic photo shooting accomplished in public places which also includes recording information of natural persons. The core legal issue to be evaluated is the purpose of taking photos. Two services, as purpose of photo taking, were indicated by Google: to set up a database used for the map application and to improve other services as well as the provision of GSV. These goals may qualify as legitimate and comply with Hungarian data protection standards. A prerequisite for that is the elimination of possible negative effects on privacy. It shall be taken into account that the activity is not intended to use personal data further, however, it is inevitable that raw pictures – under specific circumstances – include personal data (e.g.: faces, vehicle license plates, behaviour of several individuals, their whereabouts).

Pursuant to Section 3 point 10 of Infotv. taking photos, recording voice and pictures as well as their disclosure qualify also as data processing. There is another interpretation as to taking photos of an individual qualifies as being data processing irrespective of to what extent the natural person in question can be identified or whether the purpose of data controller is to identify the person by his/her name or any other means. Reviewing the recordings we can conclude Google produces high resolution images of excellent quality to GSV, therefore, natural persons can be easily identified on the pictures. The GSV vehicles taking pictures would record photos (personal data) of passers-by. In accordance with the European and Hungarian legal practice the license number plates of vehicles may qualify as personal data if they can be attributed to a certain individual, that's why, in these cases this activity is to be considered as data processing.

Art 29WP outlined in its opinion 15/2011 that the consent is not the only legal base for lawful data processing. Section 7 of the General Data Protection Directive (hereafter: Directive) defines several legal bases that could justify data processing activity, however, not always the consent of data subject is the most appropriate legal base.

We shall pay special attention to Section 7(f) of the Directive in light of the judgement of the European Court of Justice (ECJ) delivered in the unified cases of C-468/10. and C 469/10. In this verdict the ECJ stated that Section 7(f) of Directive "has direct effect" as well as it "is a provision that is sufficiently precise to be relied on by an individual and applied by the national courts. Moreover, while that directive undoubtedly confers on the Member States a greater or lesser discretion in the implementation of some of its provisions, Article 7(f), for its part, states an unconditional obligation" (Par. 52 of judgement). While evaluating the legal base for data processing Section 7(f) of Directive was also taken into consideration by our Authority since it has been found that the data processing of Google (controller) was necessary for the purposes of the legitimate interests pursued by the controller and it was proportionate to the possible restriction of data protection rights of data subjects.

Section 6(1) of Infotv. shall apply in this context laying down that "*personal data may be processed also if obtaining the data subject's consent is impossible*", since Google, as a service provider, cannot take up contact with each person before taking photos; this would practically be unfeasible. As for the purpose of data processing, Section 6(1) b) shall be taken into consideration according to which "*for the purposes of the legitimate interests pursued by the controller or by a third party, and enforcing these interests is considered proportionate to the limitation of the right for the protection of personal data".* The law, stressing legitimate interests, embraces business interests as well, that is to say, business interests may be considered legitimate when these interests are proportionate to the restriction of rights of data subjects concerned. In the opinion of our Authority this provision prevails if Google takes all reasonably necessary steps to avoid the processing of personal data during GSV service as well as enforces the safeguards defined in this statement.

In the statement of the Authority the early blurring of facial images and license number plates takes priority from among the safeguards, as the longer they remain recognizable the greater the risk is for the information to be attributed to identifiable natural persons, or the images get into the possession of persons/authorities which were to process the images with the objective of identification. The storage of raw data has to be terminated as early as possible in conformity of enforcement of the above legitimate interests. From a data protection it would be desirable if the applied technology, already at the time of taking photos, enabled the blurring of data related to natural persons. The Authority expects that service providers of GSV make efforts to meet this requirement.

Data subjects, especially those living in detached houses, shall have the right to object, without difficulty, to the involvement of their estates in GSV images. Google, and other service providers, shall fulfil the requested erasure within five working days counted from the reception of the request.

It is also essential that the storage purposes of raw data shall comply with the legitimate interest referred to the statement, it shall be disclosed and the public shall be informed under what circumstances raw data may be transferred to organisations other than the service providers.

The Authority emphasized that recording in the course of GSV, upon fulfilment of all relevant prerequisites, cannot be contestable from a data protection perspective. The Authority, irrespective of the statement, reserves the right to exercise its investigation powers, conferred

on it by Infotv., in single cases and to take the crucial steps in order to provide proper legal redress. The Authority keeps on monitoring the project implementation process and the findings in the statement will be considered in case of similar services of other service providers.

Requirements to be fulfilled in the course of recording and processing GSV images:

- Service providers have to supply prior information to the public (at least one week in advance) with regard to taking photos in Hungary. This information shall be made available online in Hungarian as well. Simultaneously the Authority shall also be advised on circumstances of taking photos.
- It is advisable to take photos in a time when few persons stay on the streets thus reducing the number of data relating to natural persons in the recorded images.
- Service providers shall, if possible, refrain from taking photos in the vicinity of sensitive locations (hospitals, social institutions etc.).
- Photo machines shall be placed in a way that nobody gains insight into places which are intentionally locked to passers-by. If, nonetheless, such recording were made it shall be blurred either on perception of Google or on request of the data subject immediately.
- Submission of requests of data subjects for deletion shall be made possible both online and in writing.
- Requests for erasure shall be implemented within 5 working days.
- Personal data visible on recordings shall, as soon as possible, be blurred and raw data shall, as soon as possible, be deleted, in conformity of the legitimate interest of the service provider.

Observation and privacy, CCTV devices at workplaces and supervision, new provisions of Mt.

The Authority, prior to the 2nd DPO conference held the 28th of January 2013, reviewed the preceding practice of DP Commissioner and (as of 2012) the Authority in relation to data processing at workplaces. As a consequence the Authority investigated under what conditions, with regard to the latest legal changes (Infotv.; Act I of 2012 – Labour Act – hereafter Mt.; C-468/10. and C-469/10. unified cases of ECJ), CCTV observation is allowed at workplaces. The findings of these investigations had been summarized in a statement which was published at the conference.

In its position the Authority clarified primarily the legal bases of the employer's control. According to the preceding practice the legal base of the employer's control involving also data processing could have been – in the absence of a legal authorization – exclusively the employee's consent. This precondition resulted in, obviously, unrealistic situations since the freely given employee's consent – with regard to the hierarchy between the employer and the employee – was questionable.

Therefore the Authority, respecting the legal base, stressed that data processing activity relative to the employer's control function, in conjunction with the Mt. and the nature of labour relationships, is not subject to the employee's consent. The privacy of employees, in the course of employment and in the context of activities of the employer, may be subject to certain limited and well defined restrictions while upholding appropriate safeguards.

Data processing by assessing legitimate interests implies its limits as well:

- The employers' actions of control shall be lawful only to the extent pertaining exclusively to the employment relationship
- The employers' actions of control, and the means and methods used, may not be at the expense of human dignity and the private life of workers may not be violated
- Employers shall inform their workers in advance concerning the technical means used for the surveillance of workers [§ 11(2) of Mt., § 20(2) of Infotv.]
- Data processing shall be lawful if the employer complies with fundamental provisions of Infotv. including principles of purpose limitation as well as fairness.

Regulations of the Mt. provide general authorisation for data processing in the course of employers' actions of control, however, giving meaning to these rules it is conferred upon the employer. Detailed regulations on means and methods to be applied shall be elaborated clearly and precisely in internal rules in detail. To this end the employer shall pay particular attention to the requirement of proportionality with regard to each data processing purpose.

Beyond an appropriate legal base further safeguards for applying a CCTV device are to be identified as well.

The currently effective Mt. – similarly to the former one – does not contain detailed rules relating to the application of CCTV equipments. At legislative level one relevant sectoral law, the Act CXXXIII of 2005 on Security Services and the Activities of Private Investigators (hereafter Szvtv.), encompasses key provisions and safeguards on CCTV surveillance methods. In this act the potential purposes, the storage period of recordings, the conditions of transfers as well as several safeguards (including, among others, places that may not be subject to observation or the right for information of individuals) have been defined by the legislator.

Even though the provisions of Szvtv. are not suitable to cover all circumstances that may occur concerning CCTV equipments. Nevertheless the NAIH takes also into consideration the regulations of Szvtv. upon investigating the legality of CCTV observations unless a clear-cut set of rules, similar to those stipulated in the Szvtv., are enacted by the legislator with respect to CCTV surveillance operations in workplaces. With a view to the detailed rules and safeguards on CCTV observations be incorporated into the Mt. the President of the Authority appealed to the Minister for National Economy.

In the framework of safeguards the Authority laid down that CCTV surveillance systems with facilities for making sound and/or video recordings may be used with a view to the protection of human life and safety, the protection of personal freedom, the safeguarding of hazardous materials, the protection of trade, payment, bank and securities secrets, and for the protection of property. Thus CCTV observations may affect, for instance, hazardous facilities, working spaces (assembly plants housing high power machineries, specific production processes). When justified, for the purpose of protecting tools of significant value stored in the workplace, raw materials as well as other valuables vulnerable sites (primarily warehouses and corridors to them) may be subject to observation.

Respecting human dignity constitutes an absolute barrier to CCTV surveillance. As a consequence a camera that monitors exclusively the employee and his behaviour may not be placed. The usage of electronic surveillance systems aiming at influencing the behaviour of employees in workplaces can be regarded as illegal as well.

An additional basic principle of the application of CCTV surveillance systems is that no cameras may be mounted in rooms where the functioning of these devices could harm human dignity, e.g. in dressing rooms, shower rooms, lavatories or medical rooms and the connected waiting rooms.

Besides, in the view of NAIH, no CCTV surveillance systems may be used in rooms either which have been designated for the employees to spend their break-times in.

The principle of purpose limitation and the test of assessment of interests set the requirement that the employer shall adjust the cameras with a proper angle of view: this angle of view may exclusively be directed to the place subject to observation.

The employer shall render detailed information on the placement, angle of view and purpose of mounting of each CCTV device. Thus the employer is able to verify the necessity of observation to the employee. It is an unacceptable practice if the employer informs the employees only generally on the use of electronic surveillance system.

The NAIH shares the view that provisions of Szvtv. [§ 31(2-4)] on storage period of video footages made by CCTV equipments – in absence of other legal instructions – also apply. Consequently the employers are entitled to store the video recordings for three working days as a general rule. The employer is obliged to verify if a special position within the company requires the footage – in conformity with the principle of purpose limitation and the test of assessment of interests – to be stored for more than three working days. Besides, should any special circumstances listed in § 31(3-4) of Szvtv. exist the NAIH accepts that the footages are stored for thirty or sixty days.

The employer shall ensure that only a limited number of persons is authorised to gain access to the footages, exclusively those who are competent to pass legally binding decisions within the organisation. To this end fundamental regulations need to be enacted specifying the possible purpose and the frequency of inspection of the footages as well as the persons who are empowered to do so.

The Authority, in its statement, made it clear what items shall be included in the written notification given to the employees. The employer is obliged to verify (either by a confirmation in writing or by completing a questionnaire) that the information on electronic surveillance has been handed out to the employees, indeed. Employees already in possession of a labour contract at the time of issuance of the present recommendation may become aware of the above information by acknowledging it. As to newcomers, they have to be informed on the above mentioned circumstances prior to the appointment in a separate document that needs to be taken over by him.

The Authority, following the issue of the statement and relating to CCTV application at workplaces, will turn to the employers in order to find out whether and how the employers comply with the conditions set out in the recommendation.

Further to the investigations the Authority, based on the responses from the employers, intends to summarize its findings of the year 2013 and will publish it.

New legal bases of data processing

The earlier Act LXIII of 1992 on the protection of personal data and public access to data of public interest (hereafter: Avtv.), effective till 31st of December 2011, had to be complemented. Recent practice of the past two decades clearly illustrated that legal bases laid down in 1992 were not appropriate to regulate data processing activities performed in various fields. As a consequence the following novel legal bases have been introduced into Infotv. Below we will be examining only the most significant interpretations on these bases.

- Section 6(1) of Infotv. stipulates the following on a new legal base: *„Personal data may be processed also if obtaining the data subject's consent is impossible or it would give rise to disproportionate costs, and the processing of personal data is necessary a) for compliance with a legal obligation pertaining to the data controller, or b) for the purposes of the legitimate interests pursued by the controller or by a third party, and enforcing these interests is considered proportionate to the limitation of the right for the protection of personal data."* Since this rule may be applied in discretion cases its passages should be interpreted:

- Obtaining the data subject's consent is impossible

This provision cannot be interpreted against the will of data subject: the data controller may not claim that the data subject did not wish to consent to data processing therefore s/he applies the new legal base. This would obviously be contrary to the legislator's intention, that is to say, the essence of informational self-determination.
The wording *„impossible"* shall be applied in conjunction with the grammatical interpretation like legal expressions in general. So, in practice, obtaining the data subject's consent shall be impossible. A good example, in this regard, could be the street view services where the service provider cannot take up contact with all data subjects prior to recording, indeed, because it would be practically unfeasible.

- Obtaining the data subject's consent would give rise to disproportionate costs

Cases where disproportionate costs could arise shall be examined on a case-by-case basis. Considering disproportionate costs the possible benefits and costs, needed for obtaining the consent, shall be compared. If the costs prove to be disproportionate the referred provisions of Infotv. may be cited. In terms of proportionality or disproportionality of costs the time of deliberation of the controller shall prevail, the circumstances arising subsequently are out of evaluation.

- The processing of personal data is necessary for compliance with a legal obligation pertaining to the data controller

The legal obligation may be based either on a legal regulation or a contract. Most important is that the obligor shall be the person who, referring to the new legal bases, wishes to process personal data. Obligations arising out of legal regulations may encompass a wide range of legal relationships. The referred provisions may be quoted when the legal obligation is specified

accurately and it is beyond doubts that the processing of personal data of the data subject is inevitable for the purpose of exercising of rights and fulfilling obligations.

- The processing of personal data is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, and enforcing these interests is considered proportionate to the limitation of the right for the protection of personal data

When the law referring to the legitimate interest it obviously implies business interests as well. Therefore not only those legal bases shall be taken into account which are specified by the legislator but also those ones that are recognized and supported by law. This is also a novelty of Infotv. still without proper domestic practice. We call the attention, however, that this is a complementary rule and may not be referred to where sectoral laws already exist. In these cases sectoral rules shall be applied; e.g.: in the field of direct marketing or market research the sectoral regulations are to be applied.

- Declaration of a minor

Pursuant to Section 6(3) of Infotv. "*the statement of consent of minors over the age of sixteen shall be considered valid without the permission or subsequent approval of their legal representative.*"

Among novel legal bases we shall mention that a minor over the age of sixteen shall have the right to make a declaration on the use of his/her personal particulars without subsequent parental consent. This is a new provision since the formerly effective Avtv. did not determine the age threshold for making such a declaration. Consequently, under 16 years of age a parental, preceding or subsequent, consent will be required if the minor decides upon the processing of his/her personal data. Otherwise the consent shall be deemed to be null and void and the data processing shall be considered unlawful lacking a proper legal base.

- Legal bases and direct effect in the EU Data Protection Directive

In relation to legal bases specified in the EU Data Protection Directive and the Hungarian law the ECJ's decision[1], regarding a preliminary ruling procedure concerning Spain, affirming the direct effect of Section 7(f) of the DP Directive is crucial (as we have already referred to it in the Google Street View case.)

It shall be taken into account that, according to the grounds of the decision, the whole Art 7 has got direct effect. This anticipates a remarkable reform process in the Hungarian legislation in terms of legal grounds as well.

Conference of internal data protection officers (DPOs)

Section 25 of Infotv. stipulates provisions on internal data protection officers' conference. The conference of internal data protection officers serves as a regular professional exchange for the purpose of the uniform application of the law. Promoting uniform application of the law regarding personal data protection and access to information of public interest is a goal of the legislature. The Authority wishes to use the conference to give professional assistance to data processors. The mandatorily-named data protection officers are members of the conference,

[1] Unified cases of C-468/10. and C-469/10.

and the non-mandatorily-named officers may become members upon application. The Authority keeps a list of internal data protection officers in order to maintain contact with them.

Conference of internal data protection officers
June 2012

Viewpoints and description of the data protection audit

Pursuant to the provisions of Infotv. effective as of 1st of January 2013 the Authority may conduct a data protection audit at the data controller's request aiming at – through assessing the data processing activities performed and planned according to professional criteria defined and disclosed by the Authority – ensuring a high level of data protection and data security.

The year of 2012 passed in the spirit of preparing for the data protection audit. The Authority examined the domestic practice on DP audit and also assessed the procedures of other EU MSs DPAs. In the framework of the latter two colleagues of us participated in the audit procedure of the Irish DP Commissioner thus gaining valuable experience. By the end of 2012 the Authority elaborated the professional criteria of the DP audit inspection.

VII. Freedom of information

During 2012 in the field of freedom of information the most significant cases affected the issues of applications for disclosure of data directed to companies owned fully or partly by the state or local governments.

Companies owned fully or partly by the state or local governments as organs performing public duties

A cornerstone of creating the publicity has always been the task of defining the circle of organs performing public duties. Classification of persons and institutions created and, as far as powers and competences are concerned, specified by the law was always clear. Although there are institutions the categorization of which is predominantly questionable; these include typically companies established, directly or indirectly, by public funds.

The interpretation of the notion of "other body performing public duties" anchored in Section 26(1) of Infotv. posed remarkable difficulties also in the practice of the former Commissioner. Pursuant to Section 100/K (6) of the Act XXXVIII. of 1992 on Fiscal Administration (hereafter: earlier Áht.), effective as of 1st January 2010, companies under the majority influence of the state, a local government, a budgetary agency or a public endowment qualified, according to the law on public access to documents of public interest, as organ performing public duties whereas the person acting on its behalf qualified as a person performing public duties. The 14th August 2010 was this provision however repealed.

In the event of state-owned companies the sections 5(1) and 5(2) of the Act CVI of 2007 on State Property clarified the situation as follows.

All data that relates to management and disposition of State property, other than public information, shall be treated as information of public interest. Access to these data may be restricted by specific other legislation.
A body or person that is vested with powers to manage or control State property shall be treated as a person or body exercising public functions pursuant to the act on access to information of public interest.

Pursuant to Article 38 of the Fundamental Law of Hungary the properties of the State and local governments shall be national assets. National asset includes, among others, properties owned by the state or local governments, financial assets, valuable rights and interests, company shares. State- and locally owned companies, as set out by law, manage public property independently and shall be liable for legality, expediency and success.

This Article of the Fundamental Law set the requirement of transparency over the appropriation of public funds on constitutional level.

Provisions of the Fundamental Law and the transparency of public funds are supported by the Act CXCVI of 2011 (Nvtv.) on National Assets.

Consequently the *"defensive position"* of state- and locally owned companies has become irrelevant stating that they do not qualify as agencies performing public duties since they are not in possession of powers set out by law. (NAIH-4203/2012/V)

The Act on National Assets and the new provisions of the Fundamental Law a meant a turning point in the long-lasting case of Balaton Shipping Company Ltd.

Since the Balaton Shipping Company Ltd. is owned at 100% by local municipalities around the Lake Balaton, therefore it shall be deemed to be a „quasi" state-owned company, as a consequence any data referring to its assets shall be regarded as data of public interest and shall be disclosed.
There are some exceptions, however, where the above requirements do not apply and where publicity may be restricted or excluded. These cases include e.g. business secrets, classified data, documents composed in the course of a decision-making process as well as documents that are subject to intellectual property rights. (NAIH-2607/2012/V)

A local representative, wishing to get access to the copies of agency and business contracts concluded after 1st January 2011, turned to our Authority questioning whether the Erzsébetváros Media Nonprofit Co. might deny the request for data of public interest. In its response the Authority claimed that all data concerning the company's assets qualify as data of public interest since the Co. is 100% owned by the local government.

Numerous submissions were received regarding the disclosure of data of companies owned, directly or indirectly, by the Debrecen Municipality. In these cases the data requested by individuals in connection with companies, directly or indirectly owned or directed by the local government, qualified as data of public interest therefore they were subject to disclosure and our Authority passed its decisions accordingly, in favour of the requesting party.

Business secrets and publicity – The case of the 4th mobile telecom service provider

At the end of August 2012, respecting the case of the 4th telecom mobile service provider, our Authority issued a recommendation on the disclosure and publicity of companies' business data which companies are in possession of national assets or are managing thereof. This recommendation is available on our website in Hungarian.

Information in support of a decision-making process as an automatic obstacle to disclosure

Public agencies performing public duties are inclined to extend the sections 27(5)-(6) of Infotv to any pre-decision processes. In several cases we found that these authorities had denied the whole disclosure without reasonable grounds.

The Századvég case

The Ministry of National Development turned to the Authority inquiring whether analyses and studies created by business contracts concluded with the Századvég Foundation, Századvég Economic Research Plc. as well as Strategopolis Strategic Analytics and Communication Consulting Co Ltd. can be subject to disclosure. According to the Ministry these papers were governmental preparatory documents. Our Authority found that the documents in question had been prepared from public funds and to public authorities that's why they qualify as being data of public interest and data public on grounds of public interest (except personal data possibly contained therein).

The Authority emphasized that the restriction of disclosure over preparatory documents in a decision-making process must not lead to the exclusion of transparency. (NAIH-4442/2012/V)
The case ended up with a judicial procedure where the court ruled in favour of disclosure of the documents in question at first instance.

Data public on grounds of public interest

The scope of data public on grounds of public interest has always been a crucial issue regarding disclosure. The new Infotv. defines the difference between the privacy and public more precisely since, in Section 26(2), it specifies the data that qualify as data public on grounds of public interest.

Pursuant to Art. VI(2) of the Fundamental Law every person shall have the right to the protection of his or her personal data, and to access and disseminate data of public interest. It shall, however, be underlined that the personal nature of these data remains sound hence the most remarkable safeguard of data protection, the principle of purpose limitation, shall be kept.

The objective of this kind of data processing is to enable the control over the functioning of the executive branch and to ensure transparency of using public funds. Consequently these data may not be used unlawfully, e.g. for the purpose of personal intrusion which is not in line with his/her public duties. Those disclosures that are intended to insult others obviously contradict the protection of privacy, which can be described as "taking the law into one's own hands" in the information law, is illegal.

The wide scope of disclosure of data public on grounds of public interest may not lead to the exposure of privacy which is not in conformity with public duties. We have learned that several actors wish to acquire personal data under the auspices of access to data of public interest.

Section 179 of Act CXCIX of 2011 on Civil Servants (hereafter: Kttv.) defines the data public on grounds of public interest concerning civil servants: name, citizenship, name of the employer, the commencement of civil service relationship, the current type and the date of categorization, the scope of duties of the civil servant, the date of appointment to, and dismissal from, an executive position, information on granting of a title as well as the remuneration of the civil servant.

Besides the above, other personal data in connection with his/her public duties may qualify as data public on grounds of public interest – information on education and detailed functions of the civil servant – in accordance with Section 26(2) of Infotv.

Transparency and control – as public interests – are of utmost importance. Although the freedom of information shall be in line with informational self-determination, i.e. it shall be ensured the privacy will not be endangered. Allowances paid to executive officials regularly or on a case-by-case basis, either in kind or in cash, e.g. ransoms, rewards, substitution allowances etc. qualify as personal data occurred in relation to public duties, i.e., are subject to disclosure upon request.

Allowances and benefits, however, that are disbursed relating to solely private circumstances may be subject to disclosure by his/her name only upon the consent of the civil servant therefore, without his/her consent, the disclosure may take place exclusively in an aggregated form – as data of public interest in connection with the financial management. (NAIH-6351/2012/V)

The case of the PM delegation

An MP of the Hungarian Parliament had lodged a petition to the National Authority for Data Protection and Freedom of Information. The MP wished to find out whether the Prime Minister's Office (hereinafter referred to as PMO) acted lawfully as it disclosed the data of members of a PM delegation (to visit Saudi Arabia last year) only who have been undertaking public duties or who authorized the PMO to do so.

Consequently the name of PM delegation members who have been undertaking public duties within the scope of responsibilities of the organization qualify as data public on grounds of public interest and that's why these data shall be disclosed duly upon request in accordance with the prevailing regulations.

According to the relating practice of the Constitutional Court the right of information and communication can be derived from the freedom of expression as constitutional right. This right is essential to safeguard the transparency of different branches of power and to enable the citizens to gain control over the activity of state organs.

This principle is supported by the European Data Protection Supervisor (EDPS) as well who asserted that an optimal balance is to be achieved between the protection of personal data and the citizens' rights to gain access to Community documents.

Personal data of businessmen and the name of companies that were involved in the PM delegation qualify as data public on grounds of public interest as they attended the journey as members of a state delegation rather than private persons. Disclosure of the above data should contribute to the transparency of state activities.

To sum up the above the NAIH takes the position that both the names of attending companies as well as those of the businessmen involved in the delegation shall be made public upon request. (NAIH-4017/2012/V)

Our Authority has repeatedly to strike the balance between informational self-determination and freedom of information.

"Since Section 26(3) excludes personal data from among the scope of data public on grounds of public interest the employee allowances – broken down by names – are out of that scope. Data on employees may be disclosed only in an aggregated." (NAIH-6383/2012/V)

Performing requests to disclose data of public interest

Our Authority concluded that the disclosure of the above requests beyond the time limit determined by law happened due to the deficiency of internal rules governing these requests. In numerous cases internal regulations merely took over the wording of Infotv. without specifying the proper process thereof. The Authority called up the actors to modify their rules accordingly.

Detailed provisions of performing requests have been improved by the legislator in the new act thus enabling organizations with minor human and financial resources to have more time for disclosure.

Organizations performing public duties have been turning to our Authority continuously, as was the case in the era of the former Data Protection Commissioner, requiring the official position of the NAIH. They argued the overwhelming data requests had been making their daily operation impossible. In these cases we inform the data controllers that the requests shall be fulfilled only in respect to data that are processed exclusively by them, they are not obliged to create new datasets (NAIH-4205/2012/V). Questions affecting the aims, purposes, opinions or seeking replies to open questions and which are not directed to discover factual information cannot be responded to in all cases.

As the Act LXIII of 2012 on public sector information reuse entered into force the 1st of January 2013 as well as taking into account that the decrees governing detailed rules have not been adopted yet

the Authority stressed the opportunity of requests to data of public interest encompassing the creation of new data. (NAIH-4927/2012/V)

Pursuant to Directive 2003/98/EC (hereafter: PSI Directive) organizations performing public duties are not obliged to create new data exclusively for the purpose of fulfilling requests on data of public interest. If the data is not in possession of the controller then it may not be obliged to supply the information. If the disclosure would demand a higher workload or would imply greater expenses in comparison to average sources the state organ is not obliged by law to perform the request (however it may assume to fulfil the request for fee as a service). Otherwise the state organ is expected to fulfil the required data processing. Hence the controller should endeavour to render the information in an intelligible manner. (NAIH-4205/2012/V)

According to the law information shall be supplied by way of the technical means asked for by the requesting party, provided that the body with public service functions processing the information is capable to meet such request without unreasonable hardship. In these cases a compromise shall be made between the requesting and the requested party. In view of the Authority a scanning fee may not be required. (NAIH-4973/2012/V, NAIH-5811/2012/V)

As the body with public service functions shall anonymise the personal data before disclosing the data of public interest the occurring costs of anonymisation shall be borne by the requesting party, however, the notion of costs shall be interpreted narrowly, at requests for minor information it shall be omitted.

In accordance with the positions of the former Commissioner and the Authority the remuneration of the official in charge, the energy used and the costs of depreciation may not be charged on the requesting party. Consequently the costs may not pose an obstacle against the exercise of access to public information as a fundamental right.

Obligation of dissemination of data of public interest by electronic means

According to our findings lots of public bodies still failed to comply with the obligation of dissemination despite multiple notices from the Authority. It would be desirable to expand the powers of the Authority in this regard.

Generally local authorities fail to comply with the obligation o dissemination. They kept on referring to personal and financial shortages that prevented them from disclosure and explained that it seriously jeopardized the fulfilment of basic public duties if they would comply with this obligation. In these cases the Authority called up the municipalities that the required data may be disclosed in the central system of public information where no special skills are needed.

Third party intervention

1. Upon citizen's initiative our Authority launched an investigation because a petitioner had lodged an application with the Eötvös Loránd University requiring public information on financial management of the university. His petition had been denied. The Authority concluded that the student's self-government was actively taking part in decision-making procedures as far as financial issues and strategic procedures were concerned. Therefore the student self-government qualified as being a body performing public duties whereas its officials as persons as officials performing public functions. (see: case No. 1642/K/2008-3 of the former Commissioner).

The petitioner filed an action against the University for failing to disclose the required information where the Authority intervened in favour of the petitioner (Pest Central District Court 29.P.85.166/2013.). The case is still pending and a final judgement is expected to be delivered in 2013.

2. The Authority intervened in favour of the Hungarian Civil Liberties Union (hereafter: TASZ) in the litigation against the Gyöngyöspata Municipality Mayor's Office. The TASZ required data of public interest electronically.

Gyöngyöspata Municipality Mayor's Office rejected the request stating that the electronic way of communication is excluded in administrative procedures. During the judicial procedure before the Eger City Court (No.19.P.20.194/2012.) the defendant fulfilled the request.

VIII. Administrative proceedings for the control of classified data

Durig the year the NAIH performed three investigations which affected the classification of personal data of data subjects as well as the legality of restrictions on right to information:

In one case the classifier had declassified the data thus a further NAIH proceeding became unnecessary NAIH.

In another case a petitioner complained that the Constitution Protection Office (hereinafter: AH) denied to render information about him. The AH informed him only that data processing is carried out strictly in compliance with the relevant data protection rules. The complainant argued he had not committed anything that would make sense to process or keep in secret personal data about him at AH.

Our investigation revealed that the petition had been based on a misunderstanding. In the course of the investigation no information arose that would have confirmed the AH's data processing in connection with the complainant. The restriction of the right to information of the data subject does not mean that the AH factually processes classified personal data of the petitioner. Namely the AH is obliged to deny any request for information even if no data processing is ongoing relating to the petitioner otherwise consequences could be drawn from the fact of a data processing activity in progress which could violate national security interests. Hereby it shall be noted that, pursuant to Section 59(4) of Infotv., the report made by the Authority on the examination of the activities of bodies authorized for using secret service means and methods may not contain any data or information that may suggest any covert investigation conducted by these bodies in a given case.

A third application challenged the practice of telecom service providers in relation to rendering information on covert investigations. This case is still pending.

One petition requested the Authority to initiate a proceeding on the legality of classification of the so-called Gripen report. This investigation is still also pending at the time of completing the annual report.

A state agency demanded a preliminary statement on the establishment of an IT system intended to process classified information.

Finally an interesting case is worth mentioning. According to the factual background explored a company, taking over the substantial and procedural methods of the relevant law on the protection of classified data, introduced such an internal code on handling classified information by which documents containing business secrets and other corporate information to be protected have been marked similarly to those of specified in the law on the protection of classified information. This practice is not supported from several aspects. First, the categorization of classification shall be used only in documents determined by the law on the protection of classified information. Second, stricter rules apply concerning classified data compared to business secrets therefore the internal code deceptively suggests that classified data are being held I this case.

To sum up, we can conclude that in 2012 we received only few submissions respecting data processing of classified data. Our Authority bears serious responsibility in supervision the classification procedures affecting the informational self-determination and freedom of

information as, in accordance with the Infotv., only the NAIH is authorized to launch administrative proceedings against the classifier for the modification of the level or the expiry of the classification of data. For the sake of efficiency the NAIH will examine the legality of classifications on the basis of an investigation schedule ex officio from 2013 on.

IX. Data protection register

The Infotv. reformed the data protection register which already operates as an administrative register. Since the new provisions of the register entered into force on the day when the NAIH commenced its functioning there was no interim period to prepare to align to the new rules. A national state-of-the-art administrative register requires a reliable and modern IT system. The installation of the former IT system was impossible that's why the NAIH began immediately to set up its new IT system supporting the data protection register from internal sources. During the development of the new system the establishment of the online administration as well as the cutting down on the administrative burden of clients takes precedence.

Due to the shortages and weaknesses of the IT system the processing of applications into the register, initially, proceeded slowly and the average processing time, in many cases, extended well beyond the 8 days limit determined by law. By October we became able to process each application properly and to keep the deadlines. In 2012 almost 11.000 data processing procedures were recorded into the IT system and in 90% registry number were handed out.

The NAIH, in applying the rules on the DP register, strives to reduce the "red tape" provided it is not contradictory to the interests of natural persons. This intention is reflected in the exceptions as well. Pursuant to Section 65(1) of Infotv. the purpose of the register is to provide assistance to data subjects. For example in the case of customer relations [Section 65(3) a) of Infotv.] the following exceptions have been elaborated:

- data are collected directly from data subjects,
- the purpose of data processing is known for the data subject,
- the type of data to be processed, the duration of data processing (deletion) are determined in advance,
- data are used only in compliance with the purposes determined in advance,
- data are not removed from the controller's scope,
- data subjects are appropriately and thoroughly informed.

The application of the new regulations on the DP register does not induce unsolvable problems, however, some corrections and modifications would be welcome for the objective to reduce the administrative burden of clients. If the compulsory dataset to be registered would involve data on electronic correspondence as well as then the procedure could be simplified. Similarly it were useful if mandatory processing procedures would have to be registered by the competent minister rather than the data controller. In case of mandatory processing, ordered by several laws, even hundreds of registration applications could be received, however, the registration could be made by the minister himself as well. In this case a final decision could be made in a single administrative procedure.

X. Photos: conferences, events

Welcome speech of Dr. Attila Péterfalvi at the reception given by the NAIH honouring International Data Protection Day (27 January 2012)

Dr. Endre Győző Szabó, Vice-President of NAIH at the 34th International Conference of Data Protection Authorities, 23-24 October 2012

„Democracy walking" – presentation to students – April 2012

Session of the Budapest Case Handling Workshop (3-4 September 2012)

“National Authority for Data Protection and Freedom of Information medallion” instituted by the President of the Authority
/Created by goldsmith Tamás Szabó/

„Awarded to persons or organizations that achieved a high reputation and exemplary results in the field of informational self-determination and freedom of information or significantly contributed to such an achievement.”

Contents

Appendix of laws and abbreviations referred to the report

- Act LXIII of 2012 on the Reuse of Public Sector Information
- Act CLXXXI of 2007 on the Transparency of Subsidies Supplied from Public Funds
- Avtv.: Act LXIII of 1992 on the Protection of Personal Data and Public Access to Data of Public Interest (repealed as of 1st January 2012)
- Ávtv.: Act CVI of 2007 on State Property
- Infotv..: Act CXII of 2011 on the Right of Informational Self-determination and Freedom of Information
- Ket.: Act CXL of 2004 on the General Rules of Administrative Proceedings and Services
- Kttv.: Act CXCIX of 2011 on Civil Servants
- Mt.: Act I of 2012 on Labour Code
- Nvtv.: Act CXCVI of 2011 on National Assets
- Records Act: Act LXVI of 1992 on Records of Personal Particulars and Addresses of Citizens
- Szvtv.: Act of CXXXIII of 2005 on Security Services and the Activities of Private Investigators

AJBH: Office of the Commissioner for Fundamental Rights
BCR: Binding Corporate Rules
EDPS: European Data Protection Supervisor
EURODAC: Council Regulation 2725/2000/EC concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention
EUROPOL: European Police Office
FRA: Fundamental Rights Agency
GSV: Google Street View
JSA: Customs Joint Supervisory Authority – Customs JSA
JSB: Europol Joint Supervisory Body – Europol JSB
KEKKH: Central Office for Administrative and Electronic Public Services
LIBE: Civil Liberties, Justice and Home Affairs Committee of the European Parliament
MNV Zrt.: Hungarian National Asset Management Inc.
NAIH, Authority: National Authority for Data Protection and Freedom of Information
PSI Directive: Directive 2003/98/EC on the Re-use of Public Sector Information
SIRENE: Supplementary Information Request at the National Entry
SIS: Schengen Information System

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: ugyfelszolgalat@naih.hu

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