National Authority
for
Data Protection
and
Freedom of
Information

Summary Report

2012

Table of Contents

Introduction

According to Act CXII of 2011, Section 38 (4)(b), the National Authority for Data Protection and Freedom of Information (NAIH) must publish a report each year by 31 March and submit the report to Parliament.

The transitional provision of the Fundamental Law, Section 16, calls for the mandate of the former Data Protection and Freedom of Information Commissioner to come to an end simultaneously with the entry into force of the new Fundamental Law, which is to say that the mandate terminated on 1 January 2012. It was also on 1 January 2012 that Act CXII of 2011 on Informational Self-Determination and Freedom of Information (the Act) came into effect. Pursuant to the Act, the NAIH, through monitoring and promotion, ensures the protection of personal data, as well as the freedom to access data in the public interest in Hungary. The establishment of the Authority can therefore be linked to related constitutional and legal reforms.

When the law took effect and work began at the newly formed NAIH, it brought with it the professional experience of the Data Protection Commissioner's office. Although the data protection authority is not, in the technical legal sense, the successor to the former Data Protection Commissioner, we can speak of legal continuity as far as fundamental rights protection issues are concerned, because the new authority took over data protection cases from its predecessor and continues to handle the same data and cases. Despite all this, it is impossible to ignore the European Union infringement proceedings that arose as a result of the abolition of the office of the Privacy Commissioner, the legal situation brought about by the transitional provisions of the Fundamental Law, and the professional and political debates that started before the actual creation of the NAIH. It is not, however, the responsibility of the Authority, of course, to take a position or form an opinion on these issues. The responsibility of the Authority is to promote and oversee the right to protection of personal data, as well as the right to access data in the public interest and data made public on the grounds of public interest, as provided for by the Fundamental Law. It must do this as an independent, impartial organization, free from external influence. The traditional Hungarian approach of unified supervision of information rights therefore remains unchanged. Every employee of the

Authority is committed to the protection of information rights through maintaining the high national legal standards and acquis, and are ready to prove this to the EU.

The Authority intends to utilize the experience gained during the period of the ombudsman, and looks forward to working with both governmental and nongovernmental actors in order to ensure a smooth transition and enable the NAIH to carry out its responsibilities.

This report is only a snapshot of the first months of a newly formed organization. It covers the development of a staff shown to be capable of performing under the previous structure and how they are developing and meeting new challenges under the new one. In light of the current situation as described in this report, the NAIH cannot be considered to have been formed in a vacuum without previous experience, but was built on existing foundations. Thrown in the deep water, it was able to start and continue work as an essentially already well-known legal protection organization. The expectations, hopes, challenges and the inherited tasks waiting to be completed all determine the future of the Authority. The diversity of what lies ahead promises to be challenging, but will hopefully not present anything insurmountable. Either way, it will all be measured in the reports of forthcoming years.

Dr. Attila Péterfalvi
President

I. The Formation of the Authority, Its Organisational Structure and the Hiring of Its Personnel

1. The formation of the Authority

The need to strengthen legal guarantees in the field of data protection has been recognized years ago in the professional community. In 2011, the Parliament decided, when they voted on the Fundamental Law, that they would replace the former model, composed of four separate ombudsman offices, by electing one parliamentary ombudsman and two deputy-ombudsmen, and by discontinuing the post of the Data Protection Commissioner. In parallel with the shift to the one-ombudsman model, it created a new authority tasked with the responsibilities related to data protection and freedom of information.

Article VI of the Fundamental Law of Hungary states that anyone has a right to the protection of its personal data and a right to know and disseminate data of public interest. An independent authority guarantees these rights, introduced by a law that was passed by a qualified majority. The Fundamental Law set up a new model and, unlike the previous ombudsman system, chose the form of an authority for the execution of the tasks described above. According to the Fundamental Law, a law passed by a qualified majority shall regulate the law concerning the new authority. This law is Act CXII of 2011 on Informational Self-Determination and Freedom of Information (Act), which was adopted by the Parliament on 11 July 2011 and entered into force—together with the Fundamental Law—on 1 January 2012. The Authority is named the National Authority for Data Protection and Freedom of Information (NAIH or DPA), and the detailed rules regarding its functions and operations are outlined in Chapter V of the Privacy Act (passed by a qualified majority).

The DPA is independent and subordinate only to the law, and is responsible for the supervision and support of the execution of the right to the protection of personal data, the right to access data of public interest and data made public on the grounds of public interest. According to the Privacy Act, the DPA has more power than the previous parliamentary

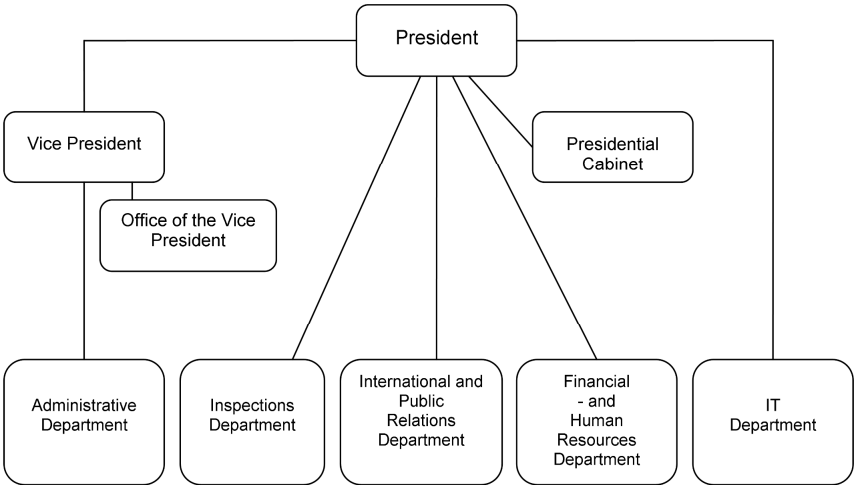
commissioner, as it also has the right to impose fines. The setup of the new DPA is one of the structural changes introduced by the Fundamental Law. The legislature has incorporated several guarantees regarding the DPA's independence. In this way, Hungary has fulfilled the obligations imposed by European Union legislation. From 1 January 2012, the DPA represents Hungary at EU institutions and working groups dealing with data protection.

The DPA is led by the President. On 15 November 2012, the Prime Minister recommended dr. Attila Péterfalvi for the position of President of the DPA, who was nominated at the end of November by the President of Hungary for a period of nine years. The President of the DPA is assisted by the Vice-President, who is appointed for an indeterminate period. From 1 January 2012, the post of the Vice-President is held by dr. Endre Győző Szabó.

2. The organizational structure

The new Authority is allocated a staff of 59. This number is somewhat larger than the staff available during the prior operation of the Data Protection Commissioner's office. The ten-person difference is due to the fact that earlier, the prior Data Protection Commissioner operated within the Parliamentary Commissioners' office, which provided shared services to the multiple commissioners. Since the data protection and freedom of information roles have been moved out of the ombudsman framework, the Authority had to make up for some previously available services (IT, operations, human resources, etc.). This accounts for part of the expansion of the work force. A further reason for the increase lies in the fact that the Act introduced the data protection audit, a new type of task, thereby justifying the increase in the number of experts. Within the organization of the Authority, the President and Vice President are assisted by a Presidential Cabinet and the Vice Presidential Secretariat, respectively. The Operational and Human Resources Department, as well as the Information Technology Department are responsible for supporting the work of the Authority.

The NAIH organizational structure



The organizational chart also illustrates that the professional core of the Authority consists of the following three main categories: the Administrative-, the Inspections- and the International and Public Relations Departments. The Administrative Department is naturally responsible for administrative procedures. These include, beyond data protection, the responsibility over matters concerning the data protection registry, legislative opinions and oversight of qualified information. The Inspections Department is responsible for conducting the investigatory-type procedures, which generally means that they provide consultation in order

to answer submissions. The International and Public Relations Department plays a dual role: it builds the Authority's international relationships and cooperation, by preparing for the Authority's participation abroad; and it maintains relationships with domestic actors to strengthen awareness of the law, playing a key role in getting the Authority's message out. The data protection audit to be performed from January 2013 will put an as yet undetermined load on the Authority, therefore it is premature to speculate how much effort it will have to expend. However, it is likely that the additional tasks arising from the audit will be dealt with within the framework described.

II. The NAIH Budget and Financial Management

Values are given in million HUF

Chapter 1, title 21: National Authority for Data Protection and Freedom of Information	Planned Expenditures	Income	Subsidy	Authorized staff (persons)
Revised statutory appropriations for 2011				
Changes by legal grounds:				
Tasks taken over from an organization in same or another budgetary chapter	362,4		362,4	49
Additional personnel salaries and wages	18,5		18,5	10
Additional employer's health and pension levy	4,1		4,1	
Additional supplies	8,5		8,5	
Additional capital expenditures	8,9		8,9	
Revised appropriations for 2012	402,4		402,4	59
Of which budgetary balance reserve	12,1		12,1	
Appropriations available:	*390,3*		*390,3*	*59*

The passed budget contains the following appropriations split by legal grounds:

Chapter 1 title 21: National Authority for Data Protection and Freedom of Information	Expenditures	Income	Subsidy	Authorised staff (persons)
Total budget for 2012:	402,4		402,4	59
Split by legal grounds:				
Operating budget	380,3		380,3	
Personnel wages and salaries total:	251,6		251,6	
Employer's health and pension levy	67,9		67,9	
Supplies	60,8		60,8	
Capital budget				
Investments	10,0		10,0	
Budgetary balance reserve administered by chapter				
Budgetary balance reserve for the chapter	*12,1*		*12,1*	

III. The NAIH Website

National Authority for Data Protection and Freedom of Information

Home Page

NAIH responsibilities and remit

Organizational Structure

Access to public data

Information, Announcements

Laws

Data Protection Registration

Schengen Information System

Contact

News, Events, Notices

In English

Dear Visitors!

On 1 January 2012, the National Authority for Data Protection and Freedom of Information came into being. The Authority, which is independent and only subodinate to the law, is responsible for promoting and supervising personal data protection, and the right to know data of public interest as well as data public on grounds of public interest.

The Authority, under Act CXII of 2011, regarding the right to informational self-determination and freedom of information, has had its powers expanded, relative to those of the earlier ombudsman's office. For example, the Authority now has the right to impose fines. The establishment of the new authority forms part of the organizational changes enacted in the Basic Law.

The legislature included several guarantees of operational independence built into the Act, through which Hungary fully complies with the required EU standards in this area. From 1 January 2012, the NAIH represents Hungary at EU bodies working in the data protection field as well as at working groups.

The Authority hopes to use the experience acquired during the ombudsman period. The NAIH will take action in future cases of data protection or freedom of information violations. The new Authority hopes to work together with both governmental and non-governmental actors in the pursuit of its responsibilities.

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

H-1125 Budapest, Szilágyi Erzsébet fasor 22/c Tel. +36 (1) 391-1400 e-mail: ugyfelszolgalat@naih.hu

General Information

Welcome to the Hungarian National Authority for Data Protection and Freedom of Information

Who we are

The Hungarian National Authority for Data Protection and Freedom of Information is responsible for supervising and defending the right to the protection of personal data and to freedom of information in Hungary. Our responsibilities extend to cover both the state and private sectors.

The National Authority for Data Protection and Freedom of Information is regulated by Act CXII of 2011, on Informational Self-determination and Freedom of Information, which was endorsed by the National Assembly on 11 July 2011. The Act is comprehensive in scope, and concerns all data control and data processing activities undertaken in Hungary. The Act defines these activities as those which relate to the data of a natural person, as well as data in the public interest and data made public on the grounds of being in the public interest.

What we do

Compared to the former system, the new regulations confer the Authority with broader competency to pursue violations of both informational rights. In particular:

- Anyone is entitled to **request an investigation** from the Authority on the grounds of infringement of data protection law.
- The Authority is **entitled to launch an official data protection procedure** if it is presumed that the illegal processing of personal data concerns a wide scope of persons; concerns special data, or significantly harms interests or results in the risk of damages.
- The Authority may decide to

  a) Order the correction of inauthentic personal data;
  b) order the blocking, deletion or destruction of illegally controlled personal data;
  c) prohibit the illegal control or processing of the personal data;
  d) prohibit the transfer of the personal data to other countries;
  e) order notification of the data subject, should the controller have unlawfully refused to do so;
  f) impose a fine ranging from 100,000 HUF to 10,000,000 HUF;
  g) order the disclosure of their decision in the interest of data protection or to protect the rights of a greater number of data subjects.

- The Authority registers data processing undertaken in respect to personal data in a **data protection file or registry** in order to facilitate access to information for the data subject.
- The Authority is authorised to launch a **confidentiality review procedure**, should, pursuant to information received, it may be presumed that national classified information has been illegally classified.
- The Authority provides a **data protection audit** as a service to those entities that request it. This audit is designed to provide

IV. Description and Evaluation of the New Provisions of the Act

1. Justification of the new provisions

For several years now professionals in the data protection field have been calling for for the creation of an independendent supervisory body with strengthened powers and a broadened reach. In spring 2011, the Parliament decided on a single-ombudsman model, enshrined in the Fundamental Law. After the establishment of the single-ombudsman system, the creation of a data protection authority and its separation from the ombudsman's office was inevitable.

Before introducing the new law in detail, it is worth briefly commenting on the reasons for the amendments to the former data protection laws.

The ombudsman model did not provide adequate legal protection against risks for those affected who sought such protection. One of the big achievements of the Act is that the organizational model of the Authority enables the state to intervene in a way commensurate with the dangers and abuses threatening the public. In severe cases, where people encounter abuse and errors that perhaps affect their lives significantly, the Authority is duty-bound to intervene effectively.

The earlier data protection laws governing the legal grounds for data management were also ripe for review. The need to update the law regarding the legal grounds for data processing arose from our membership in the European Union: it was necessary to make changes in line with the standards set by the data protection directive.

The rules pertaining to public information requests that were set down in the prior data protection law have mostly withstood the test of time. That said, a need for a revision of these rules that reflected the experience of the past two decades was apparent.

Maintaining a good relationship with those responsible for internal data protection also proved to be a weak spot in the former ombudsman system. It was therefore necessary to make up for this deficiency.

2. The legislative intent as apparent in the law

A comparison of the Act with the old data protection legislation shows that one of the most important intentions of the legislature was to form an effective institution. The legislature found that this purpose is best served by the establishment of an authority. An authority is better equipped to act in cases of transgression, and therefore it serves as a better deterrent. The law shows clear legislative intent to give the Authority a stronger role than that of the former Ombudsman.

3. Summary of the new rules

3.1 Introduction of new concepts

The Act introduces a few new definitions. The concept of data subject is formally new, but as this was previously simply a part of the definition of personal data, the new wording does not entail substantial change. But special attention should be given to the change in the concept of personal data: in addition to the above-mentioned separation of concepts, Section 4(3) states that

> Throughout the data processing, personal data shall be classified as such until its connections with the data subject can be restored. The connection with the data subject can be restored if the data controller has the technical conditions required for restoration at his or her disposal.

It might seem that the new definition of personal data is in fact narrower than it formerly was, and therefore fewer types of data processing are under the Act's remit. However, the law's applicability is influenced by the purpose of the data processing, and because of this, all actions which aim to draw conclusions or take decisions in connection with a person will be covered by

the Act. In addition to the above, the Act introduces a few conceptual innovations of smaller practical importance.

3.2 New legal bases

According to Section 5(1)(a)(b) of the Act ,

> personal data may be controlled if the data subject agrees to it, or it is provided by law, or – on the grounds of authorisation of law, within the scope defined in that law – by or pursuant to a local government decree for a purpose based on public interest.

A novel aspect of this wording is the clear effort to separate data control by state and local governments and by those performing public functions from the commercial processing of data, which is subject to other appropriate rules.

The new legal ground for data processing in Section 6(1) of the Act is relevant to the latter type of data handling:

> Personal data may also be controlled if it is not possible to obtain the consent of the data subject or even if the cost of doing so is excessively high and the personal data a) must be controlled to fulfil legal obligations applicable to the controller, or b) must be controlled to enforce the rightful interests of the controller or third parties and the enforcement of such interests is proportionate to the restrictions pertaining to the right to the protection of personal data.

The introduction of this new legal ground raises several questions of interpretation. The impossiblity of consent, the "cost of doing so is excessively high" phrase, and the concept of "legal obligation" of the data handler all require interpretation. We can expect clarifications from the practical application of the law. The phrase "rightful interests of the controller" includes legal and honest business interest too. In the

interpretation of the new legal ground, the new "proportionate interest" concept will have to be weighed as well.

Regarding the new legal grounds, we must note that minors may give consent to the processing of their personal data from the age of 16. The marriage age is 16, and employment is possible at even younger ages. In the era of social networks, it really does not seem reasonable to maintain 18 as the age of consent.

The area of national regulation related to the legal grounds of data processing is fundamentally affected by the European Union Court's decision of 24 November 2011. In the preliminary decision proceedings regarding Spain, the Luxembourg body stated that, among the legal grounds enumerated in the data protection directive, Article 7(f) has direct effect, which implies that anyone may directly cite this section in member states' courts. While the proceedings concerned Article 7(f), the justification handed down implies direct effect of the other sections too. The decision therefore has a deep impact on the regulations of those countries, such as Hungary, where the legal grounds of the data protection directive have not yet been fully implemented. The Authority, as the enforcer of the law, must be cognizant of this circumstance.

3.3 About the rules governing the National Authority for Data Protection and Freedom of Information

The Authority is independent, operates subject only to law, is not subordinate to any direction regarding its remit, and may only be assigned tasks by law. Within the national government, it is an organisationally separate, central budgetary organ with its own appropriation chapter in the budget. Its income and expenditures may not be decreased but by Parliament. The independent Authority is headed by the president, who is appointed for a term of nine years. Unlike in the earlier law, under which the Commissioner was appointed by the Parliament based on a nomination by the President of the Republic, now the appointment is made by the President of the Republic based on the nomination of the Prime Minister. The President of the Authority is assisted by a Vice President, appointed by the President for an indefinite term.

The ombudsman-like investigative process remains in regards to the actions of the Authority. If the Authority does not launch an official procedure, it may nevertheless ask the court to enforce its findings.

The Authority is now empowered to instigate an official procedure, which is carried out according to the rules of administrative proceedings. The procedure may only be initiated *ex officio*, if the Authority finds that justified. The decision of the administrative proceedings is binding on the data processor. In the decision, the Authority may impose fines ranging from a hundred thousand to ten million HUFs. As an administrative decision, the decision of the Authority may be challenged in court.

3.4 Conference of internal data protection officers

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, 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.

V. Handover to the NAIH of the submissions and current cases

According to the provisions of the Act, the Authority will process current cases based on submissions that were lodged with the Data Protection Commissioner before 1 January 2012. Therefore the cases, which mostly consist of citizens' complaints, have been taken over by the Authority from the Data Protection Commissioner's office. Although the President of the NAIH was ready to work together to accomodate the handover, the NAIH was unable to take over the cases in the legally-required, itemized format. The conscientious efforts of the commissioner's staff enabled an orderly transfer of the cases to the new Authority to take place. The new Authority

made significant effort in order to be able to complete the current caseload and be able to take on new submissions.

The Authority's remit focuses chiefly on the handling of complaints, but due to the changes in the legal environment, consultative submissions are also receiving priority in the transitionary period in order to help form a unified interpretation of the Act. Upon surveying the case traffic of the first three months (approximately), we can already say that the time spent on dealing with each case has perceptibly decreased. Due to our efforts to streamline the process, the effectiveness of the operations has improved.

There were additional difficulties with handling those petitions for registration in the data protection registry that were still in process.

The NAIH has taken over the electronic database of the Data Protection Commissioners' office, along with the data for the finalized years (1996-2011). Based on this database, the number of incomplete cases was 4256 in the time period 2009-2011. Of this, there are 3777 petitions for registration in the data protection registry, and 479 other cases.

Based on the state of the database as of 31 December 2011, 5461 cases were submitted to the data protection commissioner in 2011. These consist of 3162 petitions to register in the data protection registry, 1011 complaints, 797 consultative requests, 65 cases initiated *ex officio*, 290 requests for opinion on legislation, 112 international cases, and 24 other cases (protection of classified data, freedom of information requests, others).

The number of cases taken over by NAIH in 2012, i.e. the number of incomplete cases, was 2650. These consist of 2310 petitions to register in the data protection registry and 340 other cases, of which 192 are complaints, 113 are consultative requests, 22 are international cases, 5 are requests for opinion on legislation, 8 are cases initiated ex officio and others.

Among the incomplete cases taken over there are some that were initiated not only in 2011 but also in 2010 and 2009. From 2010 we took over 1501 incomplete cases, of which 1419 are petitions to register in the data protection registry, and the remaining 82 cases are "currently under

investigation". From 2009, there remain 105 incomplete cases, of which 48 are petitions to register and 57 are incomplete for some other reason according to the database.

From 1 January 2012 until 26 March, we have entered 3824 cases into the database, of which 1006 are investigations and 2818 are petitions to register. As of the end of March, there were 376 cases taken over from the data protection commissioner that were still in process. From 1 January 2012 until approximately the end of May 2012, we pursued investigations in 1581 cases.

For more specifics on the National Authority for Data Protection and Freedom of Information, citizens may refer to our website, visit us and ask questions. Ultimately, a highly-regarded, best-practices model is the goal, and as such, the Authority looks forward to strengthening relationships with a balanced, wide range of stakeholders, including citizens, national and international bodies, NGO's, the academic community and more.

National Authority for Data Protection and
Freedom of Information
1125 Budapest, Szilágyi Erzsébet fasor 22/c
Postal address: 1530 Budapest, Pf.: 5

Telephone: +36 (1) 391-1400
Fax: +36 (1) 391-1410
Internet: http://www.naih.hu
e-mail: ugyfelszolgalat@naih.hu