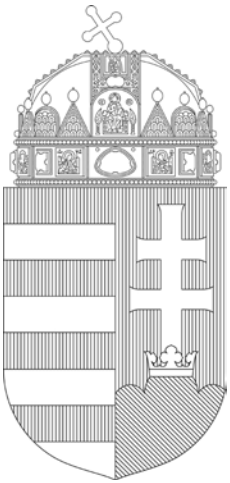
Annual report of the

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

2016

National Authority for Data Protection and Freedom of Information
Budapest, 2017



PREFACE

Welcome to The Reader,

2016 is a milestone in the history of European and national data protection, as after several years of preparation, at the end of April, the EU data protection reform package including the General Data Protection Regulation and the Police and Criminal Justice Directive has been adopted. In this light a new era begins for EU data protection authorities, two-year preparations for those new procedural and substantive mechanisms which make data processing faster, more efficient and hopefully even more secure have started. This report should therefore pay particular attention to these innovations and changes, underlining that there can only be a theoretical presentation at the moment, as the elaboration of relevant practices are being worked out on different levels with great intensity right now.

Besides protecting privacy, freedom of information is also priority for us, to ensure that the operation and management of the state is transparent to the citizens. Among the investigation cases, we provided information on the current legislative changes at trainings and conferences, shared our practical experiences with public service employees, seeking out that with our practical recommendations they will be able to fulfil their responsibilities associated with requests for access to public information more easily.

Among the international engagements of National Authority for Data Protection and Freedom of Information (NAIH), the Spring Conference of European Data Protection Supervisors held in Budapest is prominent, which was hosted for the first time in 2006 by the Hungarian data protection ombudsman and later in 2016 by the data protection authority (DPA). The two main topics of the Spring Conference were to strengthen international cooperation and also the control of national security services within constitutional framework. The importance of the latter subject is proven by the tragic terrorist attacks happened in Europe, as in the USA after 9/11 and also after 2016 in Europe, a serious dilemma has emerged in the issue of *security versus freedom*. Our answer is that bodies responsible for the safety of people should be left to work, but this work cannot remain without constitutional control. We believe that for this, there are constitutional frameworks, methods and practices which can prevent giving up European constitutional values, also including the right to privacy.

Since the Honourable Reader receives this report in 2017, I hereby would like to commemorate two important anniversaries.

The constitutional amendment of 1989-1990 raised the level of protection of Hungarian informational rights on fundamental level. Then, for the first time in the post-socialist Eastern European region in 1992, **25 years ago**, our first data protection and freedom of information law was born, three years ahead of the EU Data Protection Directive and also ahead of legislative processes in several Western European countries in this matter. From the outset, the Hungarian legislation follows the two fundamental informational rights combined-model, within an interacting regulatory framework, which apparently seems to be gaining ground in most parts of Europe.

The Hungarian Data Protection and Freedom of Information Parliamentary Commissioner's office began its operation with the election of the first data protection ombudsman in 1995. It has won the confidence of citizens very quickly, as well as it gained great importance in public life, as the voice – as the second Data Protection Ombudsman if you allow me so to speak: our voice – was heard in many important matter.

From 2011, however, the constitutional reform has brought the transformation of the ombudsman system and whereas EU law requires a completely independent organization, since 2012, **exactly five years ago**, in accordance with the new Privacy Act, the Authority responsible for data protection and informational rights has been established and continued its work.

Following the establishment of the new Authority great changes are coming again. The application of the new EU privacy rules gives tasks for all participants, not only for data controllers but for data protection authorities as well. The primary mission of the Authority for the coming period is to ensure a smooth application of the General Data Protection Regulation and to make certain that data subjects' rights are fully enforced in everyday life.

Budapest, 6th March, 2017

Dr. Attila Péterfalvi
Honorary University Professor

President of the
National Authority for Data Protection and Freedom of Information

I. Statistical figures and remarkable activities of the Authority

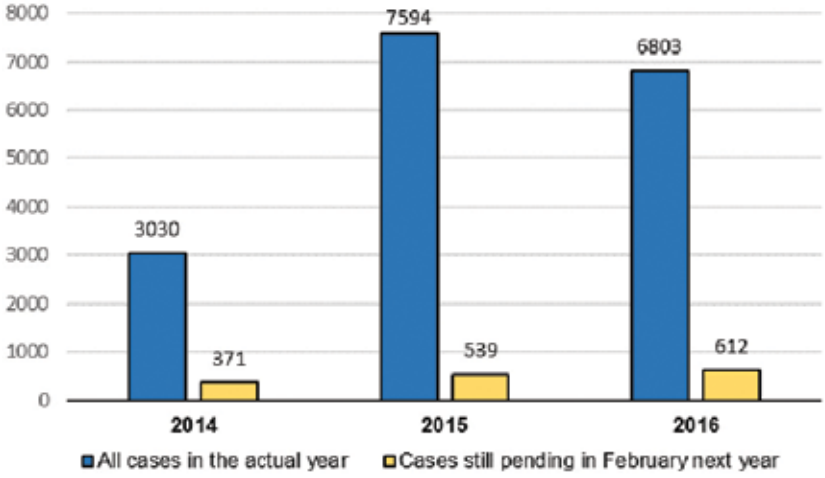
I.1. Statistical summary of our cases

Since the foundation of the NAIH on 1 January 2012, 2016 was the fifth year of its operation. In 2016, the electronic registry book contained a total of 6803 cases, 800 cases less than in the previous year, but the data protection registry contained 17091 new registrations which means 7000 more registrations than in the previous year (9965 registrations in 2016). One factor of the lower number is that while in 2015 350 management cases have been filed, in 2016 their number was reduced to 135 (-215), plus the number of filed cases involving data protection registry decreased from 3680 to 3251 (-429 cases), having regard to the fact that the Authority restored the call centre and consulting opportunities related to the data protection registry. The above figures show that there has been no significant changes in case numbers involving other meaningful tasks.

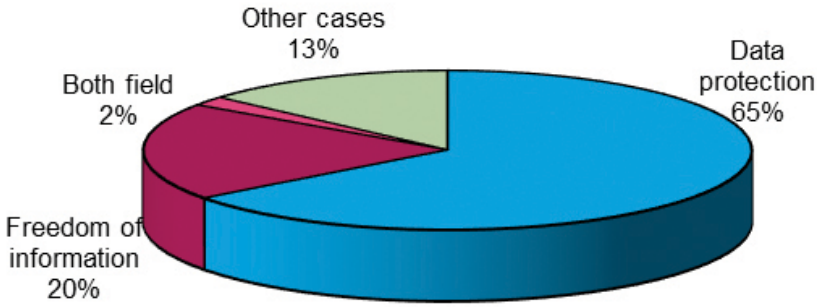
Out of the filed cases, data protection administrative procedure started in 113 cases. Out of 6803 cases, 2759 were treated as a matter of investigation. The number of investigations increased from 2655 to 2759, 104 cases more in 2016, and compared to data two years earlier (2026 cases), the significant increase has not stopped.

Other files were related to the tasks set out in the **Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (Privacy Act)**, to data protection registry-related matters, consultations and requests for information, activities related to legislation, regulations, opinions, international affairs, data protection officer's conference, data protection audits and BCR affairs, and the Authority's internal affairs, operations, information technology and administrative documents. Details of these data protection administrative procedures are further particularised in the administrative procedures part in the chapter on classified information and administrative cases.

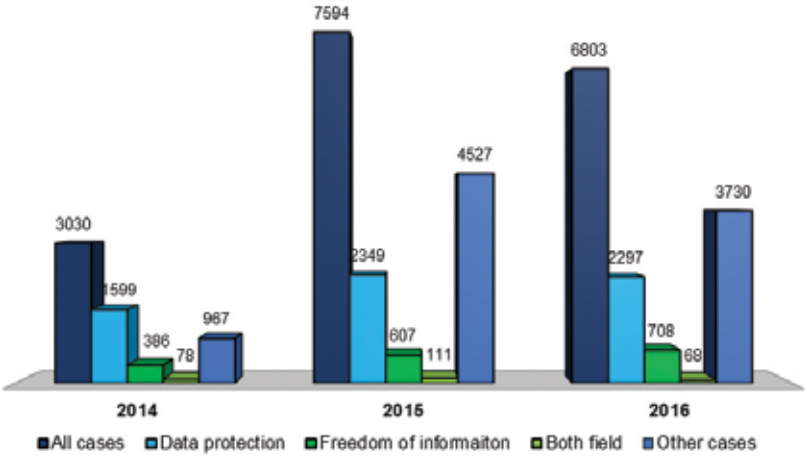
Registered and pending cases of NAIH 2014-2016



Distribution of cases by informational rights in 2016
(Without the cases related to data protection registry)



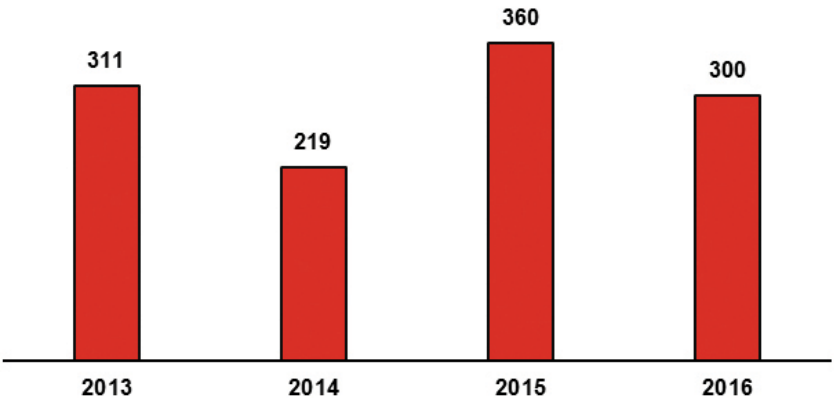
Distribution of incoming files 2014-2016
(Other cases also includes cases related to data protection registry)



In 2016 we reviewed 300 draft bills, which shows a 7% decrease compared to the previous year's particularly high number (360).

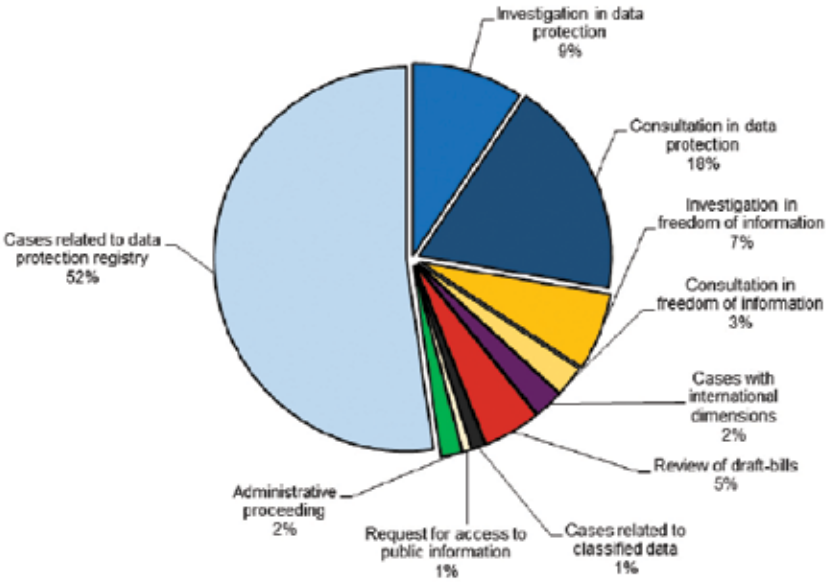
The Authority operates a legislative monitoring system, monitors activities concerning the codification of informational rights and, if necessary, reviews the draft bills and amendments that has made to the parliamentary stage.

Reviewed draft bills 2013-2016



In our ongoing cases in 2016, we initiated a total of 40 legislation amendments, 32 of them were data protection-related and 8 were related to access to public information. 14 files received were sent to other organs. Out of the cases in which the Authority initiated investigation procedure, 215 were data protection related and 69 related to access to public information. The number of rejected cases declined overall compared to the previous year.

Substantive cases in 2016



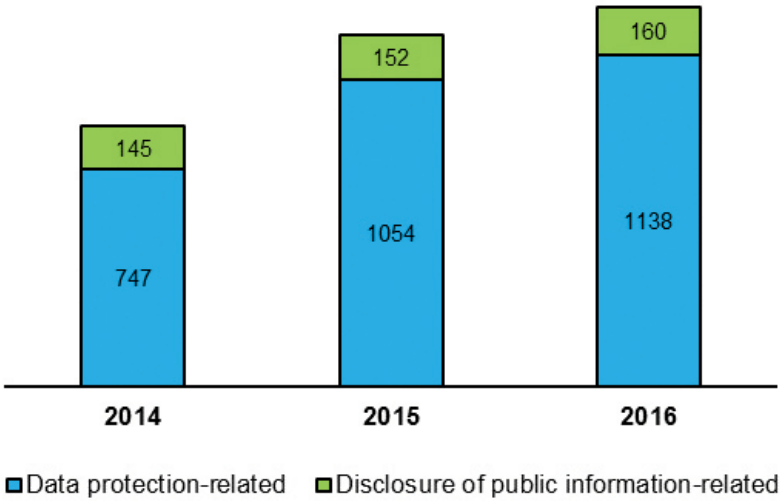
The number of actual investigation cases in 2016 was 990, 80 cases more than in 2015. Out of this, 582 (59%) were data protection-related, and 408 (41%) were freedom of information-related. Although the number of overall investigations increased, investigations concerning freedom of information is steadily rising year after year. At the time of writing this report, 482 unlawful practices have been determined out of the 990 investigation cases. The number of unlawful practices decreased, as 513 infringements were identified back in 2015.

Out of the unlawful practices, 249 were related to procession of personal data, 233 were related to public disclosure of data. Important information, that the identified data protection-related infringements have been decreased (-39),

while freedom of information-related infringements have grown from 225 to 233 (+8). So 52 % of infringements were informational self-determination-related and 48 % freedom of information-related in 2016.

There were 1298 consultation-related legal resolution cases which showed an increasing number compared to 2015 (+92 cases) which means 406 more cases than in 2014.

Consultation cases related to informational rights 2014-2016



In 2016 we had 117 cases with international dimensions, 34 investigation cases were international-related and also data protection administrative procedures had international dimensions as well (for example when the data controller or data processors is established in another Member State or in a third country).

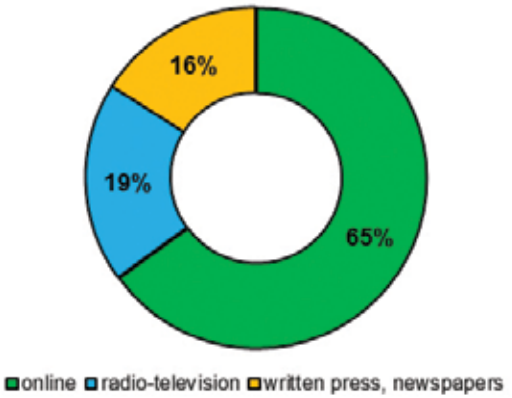
Cases related to control of secrets had a number of 70, so a growth can be seen in this area of law as well. Cases with national dimensions and control of secrets are presented as a separate chapter in the Report.

The number of data claims did not change compared to the previous year: 13 cases related to data protection audit, 54 cases related to the approval of Binding Corporate Rules. In 2016, NAIH received 47 requests on disclosure of public information, all of them have been answered.

I.2. The presence of NAIH in the media

Between 1st January 2016 and 31st December 2016, NAIH appeared in a total of 6435 times in the news, this is 1600 more appearances than in 2015. The number of online appearances was 4183 (65%), printed news 1007 (16%), in the electronic media 1244 (19%).

The ratio of NAIH's presence in the media



Source: Observer Budapest Médiafigyelő Kft.

II. The European General Data Protection Regulation (GDPR)

II.1. Introduction

The experiences of Directive 95/46/EC made it clear that a new data protection regulation is needed, because the Directive did not prevent the fragmentation of data protection rules in Europe. Natural persons became subject to the significant risks of online environment and data protection transposed on different levels into national law can stand in the way of the free flow of data. These differences are barriers to economic activities that might distort competition and hinder public authorities' duties.

On 27 April 2016, after four years of preparation, the European Parliament and the Council adopted the new data protection package:

- Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/EC (General Data Protection Regulation; GDPR)
- Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing council framework decision 2008/977/JHA.

The Regulation shall be binding in its entirety, it is directly applicable and does not require transposition by Member States. The Regulation is applicable from the date of 24 May 2016 the date of force however starts at 25 May 2018. Based on Recital (171) the data procession started before 25 May 2018 should be brought into line with the Regulation, which requires great preparation both from the controller and the authorities.

The Regulation does not apply to:

- Documents or sets of documents that are non-systematic;
- Activities outside of the scope of EU law (e.g. national security);

- Processing personal data by a natural person in the course of a purely personal or household activity (such as written correspondence, keeping an address book, contacting other persons online or on social networks);
- Personal data relating to deceased persons (however, Member States may provide for rules regarding the processing of personal data of deceased people).

II.2. Basic concepts of the GDPR

The GDPR[1] did not substantially modify the basic concepts and definitions found in Section 3 of the Privacy Act (e.g. the concept of personal data or of the data subject were not changed[2]) According to the Regulation the data subject is considered to be identifiable both directly and indirectly and should be viewed in the context of any information brought to his/her personal data. It is important to point out that "*natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them*"[3].

The processing of special categories of personal data has expanded with two categories compared to the Privacy Act: genetic data and biometrical data[4]. In the Hungarian data protection law, genetic data has always been considered as special data as it was processed as medical data by the authorized person.

Definition of data processing was made up in both the Privacy Act and the GDPR very similar.[5] The EU legislator defines 'processing' as any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means. The „*use*" of data is also defined as processing, which was not noted in the Hungarian Privacy Act.

1 Article 4 GDPR
2 Article 4 GDPR
3 Recital (3) GDPR
4 Article 4 13-14., Article 9 (1) GDPR
5 Article 4 point 2 GDPR

The definition of data controller[6] is very similar to the definition found in the Privacy Act, however the definition of data processor[7] became much more simplified in the GDPR, as it says that every organisation can be considered as processor, which ”*processes personal data on behalf of the controller*”.

Although the definition of consent[8] of the data subject slightly differs from the one found in the Privacy Act, there is no substantive difference between the two interpretative provisions. Consent has to be given freely and based on appropriate information. Regarding legal basis of data processing upon consent, the GDPR sets new requirements as well, which will be discussed later.

There are also many new definitions in the GDPR. ’Profiling’ as one type of automated data processing is specifically mentioned[9]. Profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is usually used for effective marketing.

’Pseudonymisation’[10] is a new definition, under the meaning of processing personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person.[11] Although the application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations.[12] The pseudonymisation can be used by the controller as a data security measure to mitigate the consequences of a data breach, for example,

6 Article 4 point 7 GDPR
7 Article 4 point 8 GDPR
8 Article 4 point 11 GDPR
9 Article 4 point 4 GDPR
10 Article 4 point 5 GDPR
11 Recital (26) GDPR
12 Recital (28) GDPR

the data unlawfully disclosed but pseudonymised won't reveal the identity of the affected.

'Cross-border processing' is also a new definition compared to the Privacy Act. It can mean either processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State, as well as processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.[13]

The definition[14] of 'main establishment' is also specified. A data controller with establishments in more than one Member State, the main establishment is the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment; or as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation.

II.3. Principles of the GDPR

Principles of the Privacy Act can all be found in the GDPR[15] as well. Nevertheless, certain data controller obligations found in Privacy Act have been raised to the level of principles in the Regulation.

Fair and lawful data processing gains additional meaning in the new GDPR. Data processing has to be transparent. This becomes very important as the data controller has to provide information to the data subject „*in a concise, transpar-*

13 Article 4 point 23 GDPR
14 Article 4 point 16 GDPR
15 Article 5 GDPR

ent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed."[16]

Meaning of the purpose limitation concurs with the one found in the Privacy Act, however the processing of personal data for purposes other than those for which the personal data were initially collected as a prohibition became a principle as well. There are two exceptions, one is that further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations. The other one is the complex criteria[17], where data controllers shall take some measures into account in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected.

Data minimisation as another principle of the GDPR also concurs with the one found in the Privacy Act, as it says, that personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

GDPR separates the purpose limitation and the obligation of data controllers, that personal data may be processed for longer periods insofar as the personal data will be processed solely for archiving purposes. This is called 'storage limitation'. This says that personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject.

Such measure can be pseudonymisation which we have already mentioned. In the case of a scientific research, this can be suitable for concealing the identity of the researcher, as the data suitable for identification is stored separately.

The principle of accurate and up to date data processing found in both legislations as well. Furthermore the GDPR integrated 'accuracy' into this principle,

16 Article 12 point 1 GDPR
17 Article 6 (4) GDPR

saying that every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.[18]

Integrity and confidentiality became a principle in the GDPR, which was stated as a security measure in the Privacy Act. By raising this provision on a basic conceptual level, the EU legislature wished to make data controllers to fill their operations with data security, as in recent years, more and more illegal acts (hacker attacks etc.) happened when hundreds of thousands of personal data have been compromised.

II.3.1. Accountability

It was an important experience under the application of the data protection regime established by the Data Protection Directive that the data protection principles and obligations do not sufficiently appear in the controllers' practices. During the creation of the General Data Protection Regulation it has therefore become a key priority to provide practical tools for controllers to help facilitate compliance with data protection provisions in their organization. Therefore it became necessary to introduce a general rule, which requires the data controller to demonstrate compliance.

This is the reason why accountability became a main principle in the GDPR. Controllers have to show compliance regarding their data processing activities from May 2018. From the planning of the data processing until the deletion of the data the controller has to be able to demonstrate how data protection requirements have been met.

Accountability is not a new phenomenon, it has been present in the corporate culture and in the field of data protection already. Section 22 of the Privacy Act contains similar requirements, although it was only related to enforcement before the court.

According to Article 5 (2) of the GDPR, the controller shall be responsible for, and be able to demonstrate compliance with the principles relating to processing of personal data ('accountability'). Article 24 has detailed rules on accountability: taking into account the nature, scope, context and purposes of processing as

18 Article 5 point 1 (d) GDPR

well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the Regulation. Where proportionate in relation to processing activities, the above mentioned shall include the implementation of appropriate data protection policies by the controller.

The principal of accountability means that controllers have to establish their organizational culture and all their activities in view of data protection considerations. Data protection requirements always have to be taken into account.

An indicative list of the relevant Articles to promote the fulfilment of accountability: Data protection by design and by default (Article 25); Records of processing activities (Article 30); Data protection impact assessment (Article 35); Articles on data protection officer (Articles 37-39); Codes of conduct (Articles 40-41), Certification (Articles 42-43) and Binding corporate rules (Article 47). There are also other ways to fulfil accountability: several Privacy Enhancing Technologies (PET) are not mentioned in the Regulation but help controllers to comply with the principle.

II.4. The legal basis of data processing in the GDPR

The most frequent types of legal basis can be found in the GDPR as well[19], however some of the them used by the controllers and found in the Privacy Act[20] are not listed in the Regulation.

The consent of the data subject is the first and most important legal basis in the GDPR. The requirements of the consent are set in Article 7:

- Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.
- If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain

19 Article 6 GDPR
20 Section 6 (6)-(7) of Privacy Act

language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.
- The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.
- When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

GDPR sets other requirements as well which might be familiar to the Hungarian data controllers since the Authority has previously applied them in its resolutions:
- Silence, pre-ticked boxes or inactivity should not constitute consent.[21]
- The Regulation – in line with the opinion of the WP29 – sets out that consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.[22]
- When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.[23]
- Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case.[24]

The Authority recommends data controllers to review their data processing based on consent to meet the new requirements set out in the GDPR. If the data processing is in line with the requirements, no new consent is necessary for the data processing. However if the new requirements are not met, data processing must be brought into line with the new rules until 25 May 2018.[25]

Other legal basis is when „*processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request*

21 Recital (32) GDPR
22 Recital (42) GDPR
23 Article 7 (4) GDPR
24 Recital (43) GDPR
25 Recital (171) GDPR

of the data subject prior to entering into a contract;."[26] The Privacy Act[27] also has a similar legal basis, but the cases showed that the data controllers did not really use it. In the Authority's opinion this legal basis must be interpreted restrictively thus it can be the basis of data processing only if it is necessary for the fulfilment of the contract (e.g. when processing the contracting person's identification data such as name, date of birth etc.) . In all other cases the clear consent of the concerned data subject shall be provided.

The GDPR contains two legal basis which is for data processing under law, therefore data processing is allowed when:

- „*processing is necessary for compliance with a legal obligation to which the controller is subject;*"[28],
- „*processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;*"[29].

The above mentioned two legal bases for the processing shall be laid down by Union law or Member State law to which the controller is subject.[30] With this, the Regulation allows Member States to adapt more precisely specific requirements and rules for the processing and other measures to ensure lawful and fair processing.[31] The GDPR does not require the legislature to set out data processing conditions in law (or in regulation issued under the authority of local government), but it gives opportunity to regulate these conditions in other, lower-level legislations.

GDPR also sets out purposes of the legitimate interests.[32] This legal basis allows data processing without the consent of the affected if processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. The controller has to examine whether the data subject can reasonably expect data processing by the controller.

26 Article 6 (1) point b) GDPR
27 Section 6 (4) of Privacy Act
28 Article 6 (1) point c) GDPR
29 Article 6 (1) point e) GDPR
30 Article 6 (3) GDPR
31 Article 6 (2); Recital (45) GDPR
32 Article 6 (1) point f) GDPR

The interests and fundamental rights of the data subject could in particular override the interest of the data controller when personal data are processed in circumstances where data subjects do not reasonably expect further processing. Such legitimate interest could exist for example where there is a relevant relationship between the data subject and the controller (e.g. the data subject is a client or is employed by the controller.[33])

In case of children this legal basis might be used under exceptional circumstances with extraordinary caution.

Given that it is for the legislator to provide by law for the legal basis for public authorities to process personal data, that legal basis should not apply to the processing by public authorities in the performance of their tasks.[34]

There are also further examples[35] in the GDPR for data processing under legitimate interest:

- The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned.
- The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.
- Controllers that are part of a group of undertakings or institutions affiliated to a central body may have a legitimate interest in transmitting personal data within the group of undertakings for internal administrative purposes.
- Indicating possible criminal acts or threats to public security by the controller and transmitting the relevant personal data in individual cases or in several cases relating to the same criminal act or threats to public security to a competent authority should be regarded as being in the legitimate interest pursued by the controller.

The GDPR essentially prohibits processing of special data.[36] However there are 10 exceptions when special data can be processed mainly in connection with public interest and data processing under law.

Among the exceptions mentioned above, it is worth highlighting the data subject's explicit consent[37], where – similar to Privacy Act – the consent does not

33 Recital (47) GDPR
34 Article 6 (1) point f); Recital (47) GDPR
35 Recital (47)-(50) GDPR
36 Article 9 (1) GDPR
37 Article 9 (2) point a) GDPR

have to be provided in written form. However, all requirements previously mentioned regarding consent should be taken into account. The burden of proof of the controller also extends on the verification of the knowledge of the data subject on providing special data and that the data subject has expressly contributed to the processing of special data.

II.5. Rights of the data subject

The challenges of the information society require innovative solutions in the field of affected rights. Due to the technological development, data subjects are less and less able to influence the content shared online, especially the use and fate of personal data. The balance between controllers and data subjects has been upset with the consequence that informational self-determination has become limited.

The GDPR was born – among other reasons – because *„there are significant risks to the protection of natural persons, in particular with regard to online activity"*.[38] This is why new rights have been put into the GDPR regarding data subjects. As long as the old ones are operating as a judicial remedy, the new ones are to strengthen the data subject's right of informational self-determination in the online environment. These new rules refer to the right to be forgotten and right to data portability.

Parts of the right to be forgotten (right to erasure)[39] can be found in Directive 95/46/EC as well. It has three aspects: the right to erasure, the rules in online environment and the limits of this right.

It should be highlighted that when information society services are directly offered to a child, the data subject is entitled to require the deletion of all his/her personal data without any reasonable delay. This provision applies to cases whereas the child has given his/her consent to the data processing but was not aware of the risks of it and later he/she wishes to remove his/her personal data in particular from the Internet.

GDPR says that *„where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are*

38 Recital (9) GDPR
39 Article 8 (1) GDPR

processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.".[40] When providing information, the data controller must take into account what technological possibilities are there to make sure they receive the queries and requests of the data subjects.

There are exemptions where the right to erasure does not apply. We can set up three main groups for the exceptions: first one is for exercising the right of freedom of expression and information[41], the second is for the performance of a task carried out in the public interest[42], the third one is for the establishment, exercise or defence of legal claims.[43]

II.5.1. Right to data portability

One of the GDPR's fundamental innovation is the acknowledgment of the right to data portability to empower data subjects to access and to make use of their personal data already provided. (Article 20)

The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided.

The necessary conditions of practicing this right is that the processing needs to be based on consent or on contract. Different legal basis is not appropriate for the practice of this right. It is also important that the processing needs to be carried out by automated means.

The controllers are not obliged to develop formats enabling data portability, however according to the Regulation they need to be encouraged to do so, and they are not required to introduce or maintain more technically compliant data processing systems. Nevertheless, where technically feasible, the data subject should have the right to have the personal data transmitted directly from one controller to another.

40 Article 17 (2) GDPR
41 GDPR 17. (3) point a)
42 GDPR 17. (3) points b)-d)
43 GDPR 17. (3) point e)

Another limitation of this right is that where, in a certain set of personal data, more than one data subject is concerned, the right to receive the personal data should be without prejudice to the rights and freedoms of other data subjects in accordance with the Regulation.

II.5.2. Preliminary information

Instead of the illustrative list of information to be provided where personal data are collected from the data subject as set out in Section 20 of Privacy Act the GDPR provides additional requirements:

- the identity and contact details of the controller and, where applicable, of the controller's representative, contact details of the data protection officer;
- the legitimate interest pursued by the controller or third party;
- the recipients or categories of recipients of the personal data;
- whether the controller intends to transfer personal data to a third country or international organisation;
- the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available;
- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- the right to data portability;
- the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
- the existence of automated decision-making, including profiling, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

If the personal data was not collected from the affected (it came from publicly accessible sources), it has to contain the source as well. In this case, the data controller shall provide the information within a reasonable period after obtaining

the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed.

If the personal data was not provided by the affected, the controllers can refuse to provide information when:

- the data subject is already aware of the data processing;
- providing information requires much effort or it is impossible, but in this instance, everything must be done to protect the legitimate interest of those affected;
- EU or national legislation requires the collection or transmit of data.

If data processing is for another purpose, the data subject has to be informed. It is not necessary to provide preliminary information if the data subject already has the information.

II.6. Duties and tasks of controllers and processors

II.6.1. Data protection by design and by default

According to these duties, the data controller has to implement appropriate technical and organisational measures to implement data-protection principles, such as data minimisation and pseudonymisation in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR.

Privacy by design and *privacy by default* were designed to encourage inventors, designers and users of services and products associated with the processing of personal data that when developing and designing these services they should keep the right to protection of personal data in mind, and – by taking into account of the state of science and technology – to comply with privacy obligations.

II.6.2. Stricter obligations for controllers and processors

The GDPR[44] requires that in view of the principle of transparency, any information addressed to the public or to the data subject be concise, easily accessible

44 Recital (58) GDPR

and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used. Given that children merit specific protection, any information and communication where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand.

The GDPR also requires controllers to help data subjects to exercise their rights. The controller should be obliged to respond to requests from the data subject without undue delay and at the latest within one month and to give reasons where the controller does not intend to comply with any such requests. The deadline in the Privacy Act was 25 days.

In the GDPR, the obligation to provide information differs whether the personal data was collected from the affected or not (it came from publicly accessible sources).

The Privacy Act and Directive 95/46/EC had only indication on joint controllers, but in the GDPR there are specific rules where two or more controllers jointly determine the purposes and means of processing. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under the Regulation.

The GDPR sets out the elements of the written contract between the controller and the processor and also tightens responsibility of the processor when it is intended to use a sub-processor, and also when the processor sets out the aim of data processing by itself as a *quasi* data controller.

New obligation is that a controller or processor not established in the Union shall designate in writing a representative in the Union. The representative shall be established in one of the Member States where the data subjects, whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, are.[45]

The representative shall be mandated by the controller or processor to be addressed in addition to or instead of the controller or the processor by, in particular, supervisory authorities and data subjects, on all issues related to processing, for the purposes of ensuring compliance with this Regulation.

45 Article 27 (3) GDPR

It is important that the designation of a representative by the controller or processor shall be without prejudice to legal actions which could be initiated against the controller or the processor themselves.

The above mentioned rules do not apply on controllers from a third country if:

a) processing which is occasional, does not include, on a large scale, processing of special categories of data or processing of personal data relating to criminal convictions and offences and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing;
b) the controller is a public authority or body.

The GDPR's new administrative rule is that instead of the supervisory authorities, each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility from 25 May 2018. The content of the record is also set out in the Regulation.

III.6.3. Data Protection Officer (DPO)

Section 24 of Privacy Act contains rules on internal data protection officer which says that some data controllers and processors shall appoint or commission an internal DPO. These are: authorities of nation-wide jurisdiction and data controllers and processors engaged in processing data files of employment and criminal records; financial institutions; providers of electronic communications and public utility services.

According to Article 37 of the GDPR, the controller and the processor shall designate a DPO in any case where:

a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.

When we look at the new rules, it can be seen that more DPO will be needed from 25 May 2018. Officers can be appointed also in cases which are not specifically named in the Regulation.

According to Privacy Act, an internal data protection officer is a person who holds a law degree, a degree in economics or information technology or an equivalent degree in higher education. The GDPR says, the DPO shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39 of GDPR. The necessary level of expert knowledge should be determined in particular according to the data processing operations carried out and the protection required for the personal data processed by the controller or the processor.

To be able to contact the officer easily, the GDPR orders the controller or the processor to publish the contact details of the DPO and communicate them to the supervisory authority.

According to Article 37, the DPO may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract. The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks and shall directly report to the highest management level of the controller or the processor.

It is observed that with the GDPR, the data protection officer has become more independent and receives explicit guarantee arrangements.

II.6.4. Data Protection Impact Assessment (DPIA)

One of the GDPR's major innovation is introducing the concept of the data protection impact assessment (note that the terms Privacy Impact Assessment, Privacy Risk Assessment, Data Protection Risk Assessment is often used in other contexts to refer to the same concept; hereinafter all referred to as DPIA).

DPIA is an integral part of two data protection concepts, one is the principle of accountability, and the other is the risk-based approach. DPIA helps the controller to comply with the Regulation and also to identify the risks and mitigate them with appropriate measures. As Article 24 states taking into account the nature, scope,

context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the Regulation. Those measures have to be reviewed and updated where necessary.[46]

There is no specific definition for DPIA, only its elements are noted in the GDPR. If we would like to define it, DPIA is a systematic examination of the data processing to detect, assess and mitigate the risks in order to facilitate compliance with data protection provisions. The assessment shall contain the systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller; an assessment of the necessity and proportionality of the processing operations in relation to the purposes; an assessment of the risks to the rights and freedoms of data subject and the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.[47]

A single assessment may address a set of similar processing operations that present similar high risks.[48] There are circumstances under which it may be reasonable and economical for the subject of a data protection impact assessment to be broader than a single project, for example where public authorities or bodies intend to establish a common application or processing platform or where several controllers plan to introduce a common application or processing environment across an industry sector or segment or for a widely used horizontal activity.[49]

The Regulation defines when DPIA is mandatory. The general criteria where the type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons.[50] This means in particular a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which

46 Article 24 GDPR
47 Article 35 (7) GDPR
48 Article 35 (1) GDPR
49 Recital (92) GDPR
50 Article 35 (1) GDPR

decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person. Moreover DPIA is mandatory if the data controller processing on a large scale of special categories of data, or of personal data relating to criminal convictions and offences. DPIA is also mandatory if a systematic monitoring of a publicly accessible area on a large scale is carried out.

The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment. The supervisory authority shall communicate those lists to the European Data Protection Board.[51]

The requirement to make DPIA refers to data processing following the entry into force of the GDPR and it should be carried out after the applicability of the GDPR. DPIA should be carried out (again) where it becomes necessary in the light of the time that has elapsed since the initial processing[52] or where the context of the data processing significantly changed. In any case, it can be stated that it is considered a good practice if data processing is reviewed at least once every three years by carrying out a new privacy impact assessment where processing operations are likely to result in a high risk to the rights and freedoms of natural persons.

DPIA needs to be carried out prior to the data processing which help facilitate compliance with the principles of data protection by design and by default.[53]

Where necessary, the controller shall review if the data processing is performed in accordance with the DPIA in particular when there is a change in the risks represented by processing operations.[54]

DPIA needs to be carried out by the controller.[55] Of course on behalf of the controller a third party can also carry out DPIA, but according to the principle of accountability, the controller is responsible for carrying out and for the content of the assessment. Furthermore the controller shall seek the advice of the data protection officer, where designated.[56]

51 Article 35 (4) GDPR
52 Recital (89) GDPR
53 Article 35 (1) and (10); Article 25; Recitals (78); (90) and (93) GDPR
54 Article 35 (11) GDPR
55 Article 35 (1) (2) and (9) GDPR
56 Article 35 (2) GDPR

Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.[57]

The most important issue regarding DPIA is how to carry out the assessment. First of all, the assessment has to describe the data processing in details in particular the planned data processing operations, the scope of the personal data processed, the purpose and legal basis of the data processing, the method of data collection, the access to the processed personal data, the retention periods, the IT systems supporting data processing; the functional description of data processing, etc. It should also be stated how the planned processing will comply with the GDPR and how the rights of the data subject set out in Chapter III will apply. The most important part of the risk assessment defining when the processing operations are likely to result in a high risk to the rights and freedoms of natural persons. The controller must examine the source, the nature, the severity and the characteristics of the risks. The planned processing operations need to be assessed in respect of all risks that may occur as unwanted effects, what is the probability of the risks, what consequences it has on the private sphere of the data subject.

The risks to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of chil-

57 Article 35 (9) GDPR

dren, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.[58]

In the DPIA the controller should define the measures aimed at reducing or eliminating the aforementioned risks. The suggestions and opinions of the data protection officer should be described.

The controller shall consult the supervisory authority prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk. As part of that consultation process, the outcome of a DPIA carried out with regard to the processing at issue may be submitted to the supervisory authority, in particular the measures envisaged to mitigate the risk to the rights and freedoms of natural persons.[59]

II.7. Code of conduct and data protection certification mechanisms

II.7.1. Code of conduct

The Member States, the supervisory authorities, the European Data Protection Board and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of the Regulation, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises.

Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation, such as with regard to: (a) fair and transparent processing; (b) the legitimate interests pursued by controllers in specific contexts; (c) the collection of personal data; (d) the pseudonymisation of personal data; (e) the information provided to the public and to data subjects; (f) the exercise of the rights of data subjects; (g) the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained; (h) the

58 Recital (75) GDPR
59 Article 36 (1); Recitals (84) and (94) GDPR

measures and procedures referred to in Articles 24 and 25 and the measures to ensure security of processing referred to in Article 32; (i) the notification of personal data breaches to supervisory authorities and the communication of such personal data breaches to data subjects; (j) the transfer of personal data to third countries or international organisations; or (k) non-judicial proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, without prejudice to the rights of data subjects.

Codes of conduct approved and having general validity may also be adhered to by controllers or processors that are not subject to the Regulation in order to provide appropriate safeguards within the framework of personal data transfers to third countries or international organisations. Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards including with regard to the rights of data subjects.

II.7.2. Monitoring of approved codes of conduct

The monitoring may be carried out by a body which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for that purpose by the competent supervisory authority.

The body takes appropriate action in cases of infringement of the code by a controller or processor, including suspension or exclusion of the controller or processor concerned from the code. It shall inform the competent supervisory authority of such actions and the reasons for taking them.

It is important that these rules do not apply on processing carried out by public authorities and bodies.

Joining codes of conduct and comply with them means several advantages for controllers and processors:

a. it can be a proof of complying with the Regulation;
b. it can prove that the controller has evaluated the potential risks and the processing operations offer appropriate data security;
c. when transferring data to third country, the approved codes can provide the ambience for a legitimate transfer and the guarantees for legitimate processing by third-country controller or processor.

In each case, when deciding whether there is a need to impose administrative fines or when determining the amount of an administrative penalty, compliance with the codes should also be taken into account.

II.7.3. Data protection certification mechanisms

The Member States, the supervisory authorities, the European Data Protection Board (EDPB) and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account.

The certification shall be voluntary and available via a process that is transparent.

A certification shall be issued by the certification bodies or by the competent supervisory authority, on the basis of criteria approved by that competent supervisory authority or by the EDPB. Where the criteria are approved by the EDPB, this may result in a common certification, the European Data Protection Seal.

The controller or processor which submits its processing to the certification mechanism shall provide the certification body, or where applicable, the competent supervisory authority, with all information and access to its processing activities which are necessary to conduct the certification procedure.

Certification shall be issued to a controller or processor for a maximum period of three years and may be renewed, under the same conditions, provided that the relevant requirements continue to be met. Certification shall be withdrawn, as applicable, by the certification bodies or by the competent supervisory authority where the requirements for the certification are not or are no longer met.

It is essential that the certification does not reduce the responsibility of the data controller or the data processor to be in compliance with the Regulation and does not prejudice the functions and powers of the competent supervisory authorities. Without prejudice to the tasks and powers of the competent supervisory authority, certification bodies which have an appropriate level of expertise in relation to data protection shall, after informing the supervisory authority in order to allow it to exercise its powers where necessary, issue and renew certification. The

certification bodies are accredited by the supervisory authority or by the national accreditation body.

The requirements set out in connection with the accreditation bodies are defined by the GDPR (demonstration of independence and expertise in relation to the subject-matter of the certification to the satisfaction of the competent supervisory authority etc.). The accreditation can last for five years but can be renewed. For this, the certification bodies are responsible.

Certification mechanisms together with binding and enforceable commitments of the controller or processor in the third country is capable for applying the appropriate safeguards, including as regards data subjects' rights.

The EDPB shall collate all certification mechanisms and data protection seals and marks in a register and shall make them publicly available by any appropriate means.

In each case, when deciding whether there is a need to impose administrative fines or when determining the amount of an administrative penalty, compliance with the certification mechanisms should also be taken into account.

II.8. Personal data breaches

Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.[60]

According to the GDPR, data controllers and processors have personal data breach notification obligation. The personal data breach shall be notified by the processor to the controller, and the controller to the supervisory authority, and in some cases, to the affected data subjects as well. The controller shall maintain a record of the data breaches.

According to Article 32 (2) GDPR, in assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthor-

60 Article 4 (12) GDPR

ised disclosure of, or access to personal data transmitted, stored or otherwise processed.

The wording of the Regulation practically coincides with the concept of data incident found in the Privacy Act, that when determining the appropriate level of security, the risks arising from the handling of data which can cause data incident has to be taken into account.

According to Article 33 (1) GDPR, in case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where such notification cannot be achieved within 72 hours, the reasons for the delay should accompany the notification and information may be provided in phases without undue further delay.

Another novelty of the Regulation is that the controller should communicate to the data subject a personal data breach without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of the natural person in order to allow him or her to take the necessary precautions.

In the communication to the data subject the controller shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33 (3) GDPR.

The information must therefore contain a description of the nature of the data breach, as well as the relevant proposals to mitigate the possible adverse effects of the incident. Data subjects must be informed within the limits of rationality as soon as possible, in close cooperation with the supervisory authority and also in compliance with the instructions given by the relevant authorities, such as the law enforcement authorities.

If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in Article 34 (3) are met.

The Regulation sets out those cases in which the notification of the affected can be omitted.

According to Article 33 (5) GDPR, the controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

II.9. Transfer of personal data to a third country or an international organisation

The Data Protection Regulation lays great emphasis on the transfer of personal data outside the EU, and regulates this area much more detailed compared to the Data Protection Directive as well as the Privacy Act.

According to Recital (101) GDPR, flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international cooperation. The increase in such flows has raised new challenges and concerns with regard to the protection of personal data. However, when personal data are transferred from the Union to controllers, processors or other recipients in third countries or to international organisations, the level of protection of natural persons ensured in the Union by this Regulation should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to controllers, processors in the same or another third country or international organisation. In any event, transfers to third countries and international organisations may only be carried out in full compliance with this Regulation.

The Privacy Act does not fully follow the rules set out in Chapter IV GDPR, Section 8 of Privacy Act has a different structure and also misses some of the tools of the GDPR. The Regulation will therefore bring significant improvements for those controllers and processors established in Hungary that are willing to transfer data to third countries. It will create a uniform set of conditions mandatory for all Member States.

The essence of the conditionality is that it sets out a basic principle (*„General principle for transfers"*) and after this – in a hierarchical order – it lays down the legal basis and the tools by which data can be transmitted outside of the EU.

The conditionality of the data transmission also defines a hierarchical order, therefore the transmitting body must examine according to the hierarchical order as to which legal basis or mechanism applies in respect of that given transfer.

II.9.1. Transfers on the basis of an adequacy decision

According to Article 45 (1) GDPR, a transfer of personal data to a third country or to an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.

There are detailed rules on accepting adequacy decisions. Decisions adopted by the Commission (for example Privacy Shield) on the basis of Article 25 (6) of Directive 95/46/EC shall remain in force until amended, replaced or repealed by a Commission Decision. (Article 45 (9) GDPR)

II.9.2. Transfers subject to appropriate safeguards

In the absence of a decision by the Commission, the controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies are available for data subjects.

The following data transfers with appropriate safeguards do not need the supervisory authority's permission:

a) A legally binding and enforceable instrument between public authorities or bodies;
b) Binding Corporate Rules (BCRs);
c) Standard data protection clauses adopted by the Commission
d) Standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure
e) An approved code of conduct together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights;
f) an approved certification mechanism together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

Subject to the authorisation from the competent supervisory authority, the appropriate safeguards may also be provided for, in particular, by:

a contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation;
b provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

<table>
<tr><th>Without requiring any specific authorisation from a supervisory authority</th><th>Subject to the authorisation from the competent supervisory authority</th></tr>
<tr><td>Legally binding and enforceable instrument between public authorities or bodies</td><td rowspan="2">Contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation</td></tr>
<tr><td>BCR</td></tr>
<tr><td>Standard data protection clauses adopted by the Commission or adopted by a supervisory authority and approved by the Commission</td><td rowspan="3">Administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights</td></tr>
<tr><td>Approved code of conduct</td></tr>
<tr><td>Approved certification mechanism</td></tr>
</table>

During the authorisation process, the supervisory authority shall apply the consistency mechanism.

The Regulation has detailed rules on BCR's. This is an important step forward because this tool was developed by the Article 29 Working Party, and the consistency of this global unified tool was provided by a number of its adopted working documents. The Regulation, in view of these working documents, defines BCR and provides a detailed, precise definition of the elements to be included in the BCR.

The Regulation clearly establishes the possibility that the newly introduced tools – the code of conduct and the certification mechanism – can be applied in the event of transfer of data to third countries as well. Detailed rules can be found in Chapter IV of the GDPR, however it also can be used in case of commitments by organizations located in third countries in order to create the data transmission guarantees.

II.9.3. Derogations for specific situations

The Regulation, similar to the Directive sets out that in the absence of an adequacy decision on the destination country or if there are no appropriate safeguards provided by the controller or the processor, transfer or a set of transfers of personal data to a third country or an international organisation is possible in certain situations.

According to Article 49 of the Regulation, these legal basis can only be used exceptionally and should be interpreted narrowly, and in the case of wide scale or regular data transfer – in accordance with the WP12 opinion of the Article 29 Working Party – they can not be applied. Such exceptional legal basis can be the explicit consent of the data subject or when the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request.

According to Article 49 GDPR, where a transfer could not be based on adequacy decision or appropriate safeguards including the provisions on binding corporate rules, and none of the derogations for a specific situation is applicable, a data transfer to a third country or an international organisation may take place only if it is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller and the compelling legitimate interests are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data.

The controller shall inform the supervisory authority of the transfer and the data subject, so in this case, the balance of interest need to be used.

Article 13 (1) point f) GDPR shall taken into consideration as the data subjects have to be informed about the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or about the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

II.10. Sanctions for infringements of the GDPR

1. According to Recital (129) GDPR, in order to ensure consistent monitoring and enforcement of this Regulation throughout the Union, the supervisory authorities should have in each Member State the same tasks and effective powers, including powers of investigation, corrective powers and sanctions, and authorisation and advisory powers, in particular in cases of complaints from natural persons, and without prejudice to the powers of prosecutorial authorities under Member State law, to bring infringements of this Regulation to the attention of the judicial authorities and engage in legal proceedings.

2. The corrective powers include the ability to take appropriate measures, to issue reprimand or impose fine. Appropriate measures will be similar to the current ones, while imposing a fine will be differentiated with regard of the type of the processing and significantly higher fines may be imposed.

According to Article 58 (2) GDPR, each supervisory authority shall have all of the following corrective powers to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation; to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation; to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation; to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period; to order the controller to communicate a personal data breach to the data subject; to impose a temporary or definitive limitation including a ban on processing; to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17 (2) and Article 19; to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met; to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case; to order the suspension of data flows to a recipient in a third country or to an international organisation.

3. According to Section 83 (2) GDPR, administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead

of, measures referred to in points (a) to (h) and (j) of Article 58 (2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;
b) the intentional or negligent character of the infringement;
c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;
d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;
e) any relevant previous infringements by the controller or processor;
f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;
g) the categories of personal data affected by the infringement;
h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;
i) where measures referred to in Article 58 (2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;
j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42;
k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

The maximum administrative fine is 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year if the infringements affect for example processing of children's data regarding information society, principles of data protection by design and data protection by default, records of processing activities, personal data breach, data security or data protection impact assessment.

The maximum administrative fine is 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial

year if the infringements affect for example the basic principles for processing, conditions for consent, data subjects' rights, the transfers of personal data to a recipient in a third country or an international organisation, infringement of any obligations pursuant to Member State law adopted regarding provisions relating to specific processing situations, or non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority.

II.11. Right to lodge a complaint with a supervisory authority or an effective judicial remedy against a supervisory authority

Every data subject has the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes the Regulation.

By contrast to the investigation procedure found in Privacy Act, if the supervisory authority does not act on a complaint, rejects all or part of it, considers unfounded, or does not inform the data subject of the outcome of the procedure within three months, the data subject has judicial remedy against the supervisory authority.

It is also a novelty, that where a data subject considers that his or her rights under this Regulation are infringed, he or she should have the right to mandate a not-for-profit body, organisation or association which is constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest and is active in the field of the protection of personal data to lodge a complaint on his or her behalf with a supervisory authority, exercise the right to a judicial remedy on behalf of data subjects or, if provided for in Member State law, exercise the right to receive compensation on behalf of data subjects. A Member State may provide for such a body, organisation or association to have the right to lodge a complaint in that Member State, independently of a data subject's mandate, and the right to an effective judicial remedy where it has reasons to consider that the rights of a data subject have been infringed as a result of the processing of personal data which infringes the Regulation. That body, organisation or association may not be allowed to claim compensation on a data subject's behalf independently of the data subject's mandate.

II.12. Right to compensation and liability

The Regulation sets out the responsibility for damages not only for data controllers but also for data processors. According to Article 81 GDPR, any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

A controller or processor shall be exempt from liability if it proves that it is not in any way responsible for the event giving rise to the damage.

Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject.

Any controller or processor which has paid full compensation may subsequently institute recourse proceedings against other controllers or processors involved in the same processing.

The judicial procedure for the enforcement of the right to compensation must be brought before the courts of the place of activity of the controller or processor. The data subject may start the procedure in the Member State of his or her habitual residence as well, except if the data controller or data processor is a public authority in one of the Member State.

II.13. Institutional system

According to the Regulation, it can be seen that data protection authorities will be strengthened, they receive new responsibilities and powers. In order to protect the processing of personal data of natural persons and to ensure the free flow of personal data within the internal market, the supervisory authorities monitor

the application of the provisions of this Regulation and contribute to its uniform application throughout the EU. For this purpose the supervisory authorities shall cooperate with each other and with the Commission.

The lead authority should be competent to adopt binding decisions regarding measures applying the powers conferred on it in accordance with the GDPR. In its capacity as lead authority, the supervisory authority should closely involve and coordinate the supervisory authorities concerned in the decision-making process. Where the decision is to reject the complaint by the data subject in whole or in part, that decision should be adopted by the supervisory authority with which the complaint has been lodged.

The rules on the lead supervisory authority and the one-stop-shop mechanism should not apply where the processing is carried out by public authorities or private bodies in the public interest. In such cases the only supervisory authority competent to exercise the powers conferred to it in accordance with the Regulation should be the supervisory authority of the Member State where the public authority or private body is established.

In order to contribute to the consistent application of this Regulation throughout the Union, the supervisory authorities shall cooperate with each other and, where relevant, with the Commission, through the consistency mechanism as set out in Article 63 GDPR.

According to Article 58 GDPR, new powers will take effect as follow:

- carry out investigations;
- corrective powers;
- authorization and advisory powers.

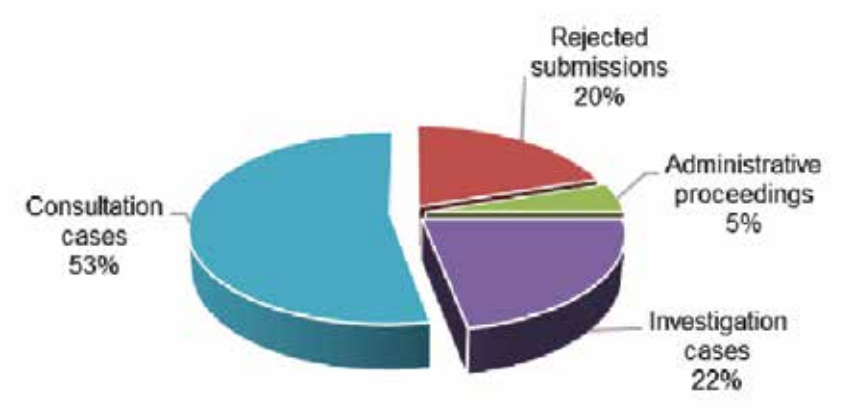
A new institutional stakeholder is the European Data Protection Board, which will not only have a coordinating and advisory role, but will make enforceable decisions. The EDPB replaces Article 29 Working Party. The dispute resolution mechanism will have a big role, whereby in case of disagreement between supervisory authorities, the EDPB shall decide with a binding decision.

III. Data protection

III.1. Statistical figures

In 2016 the work has been undertaken in the spirit of preparation for the GDPR.

Data protection cases in 2016



Half of the cases were consultations. In 20% of these cases the Authority did not start an investigation or proceeding. The actual procedural matters under examination make up a quarter of the total number of cases and the Authority found an infringement in half of these cases.

In 2016 – as in the previous years – we had more investigation cases than administrative proceedings which are usually more complex cases, more formalised and based on a detailed clarification of the facts with a longer duration period.

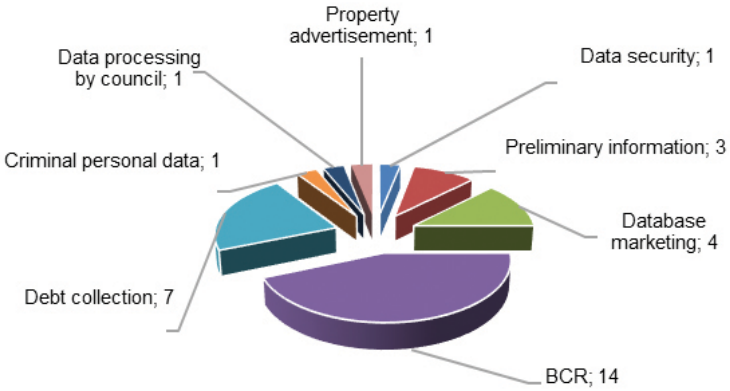
In 2016 we started 63 administrative proceedings, together with cases still pending from 2015 we had a total of 77 administrative cases.

Years	Number of proceedings	Decisions of NAIH			The amount of the fine imposed
		Ordering the termination of the proceeding	Decision on a fine	Decision without a fine	
pending cases from 2015, decision made in 2016	14	6	5	4	6.900.000 HUF
Cases started in 2016	63	4	5	12	13.300.000 HUF

In 2016 the Authority closed a total of 36 administrative proceedings, out of which we found 26 infringements and imposed fines in 10 cases.

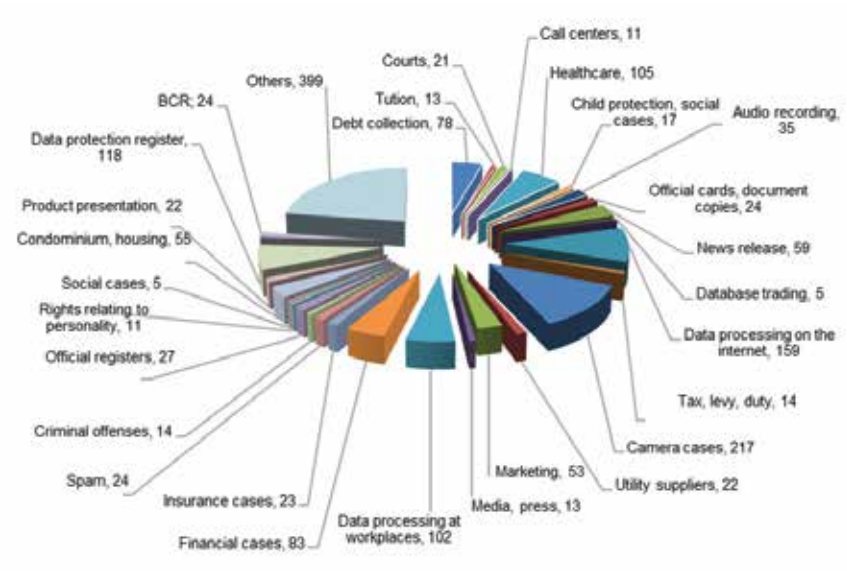
It can be seen that less fine was imposed in 2016. The reason for this is that in 2016, according to the final judgement of the Curia – derogating from the judgment of the Court of First Instance and from the Authority's position – NAIH had to comply with Act XXXIV of 2004 on promoting the economic development of small and medium-sized enterprises (hereinafter referred to as: Kkv.tv.). The Act says that in case of an infringement committed for the first time by small and medium-sized enterprises, a warning should be used instead of fines. This means that if the Authority finds that the data controller is a small or medium-sized enterprise, formerly no infringement was found and no exemptions set out in the Kkv. tv. are present, no fine can be imposed only a warning can be sent to the data controller.

Distribution of resolutions adopted in administrative proceedings for data protection

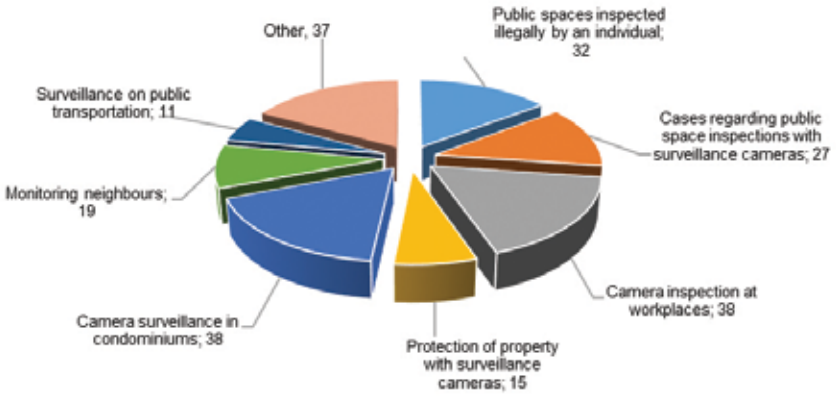


Lawsuits						
	2012	**2013**	**2014**	**2015**	**2016**	**Total**
Administrative proceeding	33	40	30	30	63	**196**
Judicial review	11	11	8	2	4	**36**
Pending lawsuit	0	0	2	1	4	**7**
Favourable result of the lawsuit	8	8	2	1	0	**19**
Partial favourable result of the lawsuit	0	2	1	0	0	**3**
Failure of lawsuit	3	1	3	0	0	**7**
All court decisions	**11**	**11**	**6**	**1**	**0**	**29**

Type of data protection cases in 2016



Surveillance cases in 2016



III.2. Experiences of the procedures

III.2.1. Investigation of complying with the requirement of providing preliminary information to the data subject

I. On the basis of experience of data protection procedures in previous years and in view of that every year the Authority receives a significant number of complaints for not providing adequate information for data subjects, we paid special attention to the requirement of providing preliminary information.

The legal basis of most data processing activities is the consent of the data subject. According to the Privacy Act, the consent is a freely and expressly given specific and informed indication of the will of the data subject by which he signifies his agreement to personal data relating to him being processed fully or to the extent of specific operations. If there is no appropriate information given to the data subject, the data processing should be considered unlawful. To successfully comply with these rules, the Authority issued a recommendation[61] in 2015.

61 http://naih.hu/files/tajekoztato-ajanlas-v-2015-10-09.pdf

The Authority found the following typical errors:

- insufficient information on the identity and contact of data controller;
- the aim of the data processing is usually superficial and not sufficiently specified, or the wording is not clear, the terms used have no clear, obvious meaning to everyone;
- typically it is unclear, what data is processed for exactly what purpose and as a result, it cannot be determined whether the controller fulfils the requirements the principle of purpose limitation;
- the range of data provided on mandatory and voluntary basis is not separated;
- when specifying the duration of data processing, there is no absolute time limit indicated, or the provide insufficient information, like, for example, the data processing will last until the end of the purpose of the data processing or until the end of the limitation period of the contractual relationship, specified in different legislations;
- lack of information on the data processor;
- no information available at the location of the data recording;
- focal clarity of the text remains a serious problem, when controllers are using only the terms of the legislations;
- not enough information on complex data processing;
- inaccurate reference to legislations.

Even though the quality of information and data processing improves gradually, there are still shortcomings when it comes to the criteria of transparent data processing.

III.2.2. Rights of the data subject

In 2016 the Authority has been continuously receiving complaints from data subjects about not getting appropriate information on the processing of their personal data.

According to the different processes, the most common errors can be summarized as follows:

1 The data subject's requests on data processing are considered service complaints, which are treated according to the data controller's complaint management rules. In the reply information is given only on sectoral regulations governing their activities.

2 Providing information shall not be made dependent on a condition e.g. demanding the applicant's personal appearance.
3 There are data controllers who attach forms to their privacy policy. Data subjects have to fill out these forms and provide detailed explanation on their problems.

The data subject may request information from the data controller on his/her personal data being processed. Since this is an essential element of the fundamental right of informational self-determination, there is no need to justify the inquiry.

4. Public administration bodies usually falsely consider the data subject as a customer and request the submission of missing documents by referring to the Act on the General Rules of Administrative Proceedings and Services.
5. Data controllers fail to answer the requests, even though a possible refusal of information would require a reason. They usually claim that it is an error of the customer service, but the Authority considers that this is not an excuse.
6. The data controllers often fulfil their obligation to provide inadequate information e.g. solely on the legal basis of the data processing without mentioning other important circumstances, such as the scope of the data, the data processor's name and address, purpose of the data processing etc.

NAIH's view is that using a data processor does not exempt data controllers from the notification obligation pursuant to the Privacy Act thus the data controller has to inform the data subject about the fact of using a data processor.

Generally speaking, the right to obtain information grants the transparency of data processing and helps to ensure the lawfulness and fairness of data processing. Also the data subject has the right to enforce every right in connection with the data processing, according to Sections 15-15 of Privacy Act.

Right to obtain information is a core prerequisite for the rights set out in Directive 95/46/EC that is, to ask for erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data, and to request information from third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with the above, unless this proves impossible or involves a disproportionate effort (Article 12 b), c). It is also essential for the enforcement of the data subject's right to object, set out in Section 14.

III.2.3. Data transfer to third countries

The actualities of the ruling of data transfer to third countries – as the creation of the EU-U.S. Privacy Shield and the amendment of the Hungarian Privacy Act on the Binding Corporate Rules – makes the Authority to concentrate on data transfers to other countries. The Authority investigated these cases according to Section 8 of Privacy Act.

In 2016 we had 24 cases regarding data transfer to other countries. Out of the 24 cases, 10 ended with decision and 4 ended with a termination order. 10 cases are still pending. Many times, using BCR as the legal basis of transferring data to other countries resulted an infringement, as it has not been approved by the Authority as to according to Sections 64/A, 64/B and 64/C of Privacy Act.

III.2.4. Data processing related to expert opinions

The Authority received submissions on the use of psychological and psychiatric expert opinions by other parties than to whom they were originally addressed, as well as on unreasonable and disproportional disclosure of personal data of documents generated at civil and criminal proceedings. In a specific case, the Authority found that the unlimited disclosure of personal data irrelevant to the official procedure does not correspond to rules set out in the Privacy Act.

This is especially true in the case when a medical/psychological certificate – including sensitive data – prepared by a judicial expert, psychiatrist on the party is fully accessible by the opposing party of a pending lawsuit. In our view that this kind of access to sensitive data is beyond the justifiable level of necessity and proportionality, therefore the Authority has presented a legislative proposal in connection with the new regulation on criminal procedure suggesting the consideration of the above anomaly.

In one criminal case of a light bodily injury, the applicant complained that the psychologist expert's opinion on his state was used in a trial by his ex-wife in the position of the opposing party without his consent. Respecting the principle of the independence of the judiciary the Authority does not have the power to verify the lawfulness of the use of evidence or exclude any evidence in a trial and argument or appeal in this matter is a subject of an action before the court. Since the dispute started between a separated couple as private persons, Section 2 (4) of

Privacy Act referring to the “household exemption” apply with the consequence that the Authority does not investigate such data processing.

III.2.5. Complaints on enquiry services

The Authority received lot of complaints in connection with an online site (hereinafter: website) providing enquiry services and processes personal data.

The complaints were aiming the fact that the website database is full of personal information (name, address, phone number etc.) which is being processed without the consent of the data subjects thus it was published and forwarded to another service provider unlawfully.

According to these complaints, the Authority has examined the legal context as follows:

According to Section 160 (2) of Act C of 2003 on Electronic Communications (hereinafter referred to as: Eht.), service providers shall prepare directories of subscribers of fixed network telephony services each year in printed format (phone book) or in electronic format, listing all subscribers of the service provider.

Section 146 (1)-(2) of Eht. rules that all service providers which assign telephone numbers to subscribers shall meet all reasonable requests to make available, for the purposes of the provision of publicly available directory enquiry services and directories, the relevant information in an agreed format on terms which are fair, objective, cost oriented and non-discriminatory. Service providers which assign telephone numbers to subscribers shall make available – subject to the subscribers prior consent – the names of subscribers, the part of their postal addresses conveyed to the service provider for publication, and their telephone numbers to the directory assistance service providers free of charge. The information so disclosed may only be used for universal directory assistance services.

In relation to the data transfer mentioned above, the Authority found that according to the judgement of the Court of Justice of the EU delivered in Case C-543/09 *“Deutsche Telekom AG v Bundesrepublik Deutschland”*, a service provider is entitled to transmit subscribers’ personal data without their consent to another company that is intending to publish a public phone book. Furthermore, national law can even require a mandatory transmission of the data.

Summarizing the above if the service provider informs the data subject sufficiently that according to the contract, personal data being processed by the service provider can be transmitted to another company (data processor), and the data subject gave his consent to the publishing of personal data in the data controller's phonebook, the transfer of these data in order to publish the same personal data in another phonebook can be realized without asking the repeated consent of the data subject.

If the data subject does not want to appear in the contact list, transmitting data to another service provider by the data controller creates unlawful data processing activity, because in this case, the service provider did not have proper legal basis for displaying/publishing the personal data in the contact list nor for transmitting personal data to another service provider.

The data subject has the right to withdraw his consent and if the service provider does not delete his data from the contact list, or the personal data is not deleted by the data processor, the data subject can turn to the Authority. The Authority will start an investigation and may order the data controller/data processor to delete the data in question. The Authority can also impose a fine. Moreover, the data subject shall be always entitled to have inaccurate data corrected and unlawfully processed data deleted.

III.2.6. Cases related to medical records

Submissions concerning the processing of medical data showed a mixed picture. A recurring incident is the problematic access to own health records generated by health care providers.

One submission, for example, contained the issue of a young mother, who wanted to get a copy of the data generated during prenatal care but the contract fee of the medical institution determined the cost of providing such copy unreasonably expensive, for more than 100.000 HUF.

In 2015 the Authority issued a recommendation concerning the practical application of accessing data/the right to ask for the copy of documentation, and proposed to determine fees for copying medical records in legislation. In 2016 this issue still has not been resolved, the appropriate legislative steps have not yet taken place.

Major infringement was spotted in a submission in connection with data processing of employees regarding sick pay. The employer has listed the diseases of employees who are on sick play which have been reviewed by the management on a daily basis. In his reply the data controller's (employer) referred to efficient organizational purposes as to ensure the optimal substitute for sick employees. However, the employer immediately ceased the problematic data processing, deleted all files and listings regarding this sensitive data and provided data protection trainings for the management.

Submissions regarding medical examination of jobseekers were also common. The question was whether the employer or the employment agency is informed on the detailed health status of the jobseeker.

According to Section 50 of Act XCIII of 1993 on Safety at Workplace, *„the worker can only be entrusted with a work that her/she is capable of, has the required knowledge, skills and proficiency on health and safety at work"*.

According to the law – in the context of obligation of cooperation – the employees are required to participate at regular medical examinations. The employer or employing authority processes data only on the result of the opinion whether the person is suitable for the job or not. Other health data or medical records shall not be transferred to the employer, the health care provider shall remain the data controller exclusively.

In its submission, a general medical practitioner stated that a firm specialized in hearing disabilities sends inviting forms to patients. The investigation found that the doctors did not give out information about patients of their district, however, while reviewing the company's privacy policy, a number of shortcomings were identified.

The National Ambulance Service contacted the Authority and asked, for who and what information can be supplied by the emergency services' dispatcher about patient care, and whether television crews can join the ambulance on a rescue mission. If yes, are they allowed to make video/audio recording of the emergency work?

The Authority's view is that in the absence of a statutory authorization but upon the written consent of the data subject, third parties could be informed about sensitive data. However, acknowledging the reasonable concern about their family members in urgent care cases it is not realistic that the ambulance unit

obtains the written consent of the patient justifying any data transfer. So if it can be predicted that the person inquiring information is a relative and so is able to identify the exact name and age of the patient, then information on the whereabouts of the patient can be provided according to Section 6 (2) of Privacy Act[62].

To provide additional information about the medical status of the patient falls within the exclusive responsibility of the health institution, therefore detailed explanation by the ambulance service cannot be provided on phone. If there is no likelihood that the person who requests information is a relative of the patient (being a journalist etc.) information cannot be provided at all.

In such cases, the recorded area, the board, the patient's clothing and his/her speech may act as special data because it can also provide a conclusion on racial origin, nationality, pathological passion of the patient, even if the patient's face is covered, as the patient's friends might still recognize him/her anyway.

Only with the written consent of the patient can television and other media join the ambulance on a rescue mission legally. However in urgent care cases is not realistic that the ambulance unit obtains the written consent of the patient on such data processing, therefore the Authority agreed with the position of the National Ambulance Service and stated that no video/audio recording is allowed in this way.

Recurring complaint is that insurance companies require health data for insurance claims. According to the relevant insurance legislation, a client's health data can only be processed with the written consent of the data subject. Confidential information on insurance related to the insurance contract, its creation, and its administration can only be processed by the insurance or reinsurance company. Aim of the data processing can only be the creation and modification of the insurance contract, fulfilment of claims or aims set out in the insurance legislation.

Generally it can be established that when the data request is not limited to information directly related to the scope of claims arising under the insurance con-

62 Section 6 (2) If the data subject is unable to give his consent on account of lacking legal capacity or for any other reason beyond his control, the processing of his personal data is allowed to the extent necessary and for the length of time such reasons persist, to protect the vital interests of the data subject or of another person, or in order to prevent or avert an imminent danger posing a threat to the lives, physical integrity or property of persons.

tract, data processing becomes too broad. It should be examined occasionally whether there are any law exemptions, or according to define the exclusions set out in the insurance contract require the inclusion of such special data.

III.2.7. Scientology

The Authority received complaints on data processing by the former Hungarian Church of Scientology and by the current Association of Scientologists (hereinafter: Association). According to these complaints, the data subjects' rights have been violated during the data procession. Therefore the Authority decided to launch an administrative proceeding for data protection. Within this framework site inspection was held at two locations (the body's central office in Budapest and at its Mission located in Nyíregyháza) and seized electronic and paper based data carriers. The aim of the administrative proceeding is to find out whether the data processing by the Association is in accordance with the Hungarian data protection provisions. The proceeding continues in 2017.

III. 3. Recommendations

According to Section 38 (4) point c) of Privacy Act, within its scope of responsibilities conferred under Subsection (2), the Authority shall make recommendations in general, or to specific data controllers. These provide guidance on privacy issues affecting many people and helps both data controllers and data subjects.

In the year 2016, the Authority published its recommendation on audio recordings and on the right to claim copy of the data processed, on the basic requirements of data processing on workplaces and on data processing by web shops.

III.3.1. Audio recordings

Regarding the huge number of incoming cases and reviewing the relevant legislation, it became clear that the practice of law in this area is not consistent, therefore the Authority has published a recommendation https://www.naih.hu/files/ajanlas_hangfelvetel_NAIH-2016-4718-V.pdf). on the issue and has called to unify the various sectoral legislations, to raise awareness and to promote law-abiding behaviour in this area.

I. The availability and the right to request copy of audio recordings

According to Section 14 a) of Privacy Act, the data subject may request from the data controller information on his personal data being processed. The data controllers' practice however differ from these rules when it comes to audio recordings.

Electronic communication service providers are required to make available the audio recording, while the sectoral laws for financial institutions determine other ways of receiving information (by retrieving the recording or letting validated protocol available).

Neither Act CLV of 1997 on Consumer Protection (hereinafter referred to as: Fgytv.) nor the Privacy Act define what type of information should be provided.

In order to ensure more complete realization of the informational fundamental rights the Authority intends to draw the data controllers' attention to the following aspects:

- Providing information to the data subject in connection with data processing of audio recording guarantees the highest standards of completeness and clarity when the data subject has the possibility to listen to the audio recording taking place at the controller's headquarters or premises, at the actual place of the audio recording, but may also happen by handing over a copy of the recording to the data subjects.
- Owning a copy of the audio recording may serve the legitimate interest of the data subject for example the copy can also be the used as proof when the protocol if the recording is being questioned. In some cases, the right of appeal is also ensured by owing a copy of the discussion at issue.
- The Authority believes that it is not the service provider who needs to judge whether the usage of audio recording by the data subject is justified or not.
- The release of copies of audio recordings shall not be subject to any other conditions but only those provided for by (the Privacy Act and other sectoral) legislations.

The audio recording companies unreasonably restrict the rights of data subjects when the release of audio recordings or copies depends on personal appearance of the client at the company's headquarters; unrealistically high amount of charge is assessed when requesting a copy of the data; or when they charge an attorney's fee for the procedure.

Furthermore, the GDPR also defines the right to request copy of the processed data. According to Article 15 (3) the controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

II. Audio recording by the data subject/customer

No legislation defines such activity as mandatory, but it is considered as a legitimate expectation that if the service providers and enterprises can record phone conversation, the possibility of doing so is afforded for the other party as well. The following aspects are to be considered:

- The activities concerned should not expand beyond the purpose, which is the same objective that the data controller wants to achieve by recording the conversation. Accordingly, the recorded conversation can also be used only during disputes with the controller, but the conversation cannot be disclosed. If it exceeds the rule set out in Section 2 (4) of Privacy Act, the data subject will become a data controller. During the conversation, the staff member represents the company and should inform the data subject about the audio recording.
- The contribution to the audio recording cannot be denied on the basis of business secret, as violation of business secret occurs already when the unauthorized person becomes aware of these secrets, regardless of whether or not the conversations is recorded. On the other hand, business secrets are data that actually undermine the financial, economic or market interests of the rightholder, which makes the data necessary to be treated as secret or confidential. The proprietor of the business secret has the responsibility of the fact that its employees do not disclose business secrets during a telephone conversation.

III. The result of the recommendation

The National Assembly – on proposal from the Minister of National Development – adopted Act CLXVIII of 2016 on the amendment of acts related to electronic communications and consumer protection. The rules set out in this Act comply with the recommendation.

III.3.2. Information on the basic requirements of data processing at workplaces

Because of the many submissions concerning data processing at workplaces, the Authority considered it appropriate to give out comprehensive guidelines on data protection requirements at workplaces addressed for both employers and employees. The guideline can be reached on the following link:
http://naih.hu/files/2016_11_15_Tajekoztato_munkahelyi_adatkezelesek.pdf

The guideline is made up of two main parts. The first part contains general rules and describes the basic privacy principles and rules applicable at workplaces. It emphasizes the importance of data processing based on the employer's legitimate interests as legal basis, since data processing realized by controlling activities of the workplaces can only be based on this legal basis.

The general information also covers guidance on how to provide preliminary information on data processing, how data transfer to abroad should work, on the notification requirement into the Data Protection Register, as well as issues relating to jurisdiction.

The second part concentrates on privacy requirements regarding application forms; aptitude tests; checking the integrity of the employee; rules on using GPS navigation systems; the applicability of biometric systems; whistleblowing.

A key chapter is about the control of the behaviour of workers in connection with their work, given the fact that most of the submissions received by the Authority affects this field. The main data processing issues when it comes to the inspection of workers are: workplace surveillance; monitoring the use of the employer's e-mail account, laptop, internet usage, the use of mobile phones provided by the company.

We truly hope that the guideline will help both the employers to introduce appropriate rules and also the employees to be more aware of their privacy rights at workplaces.

The GDPR has very similar requirements on this field so no great changes are to be expected after 25th May, 2018.

III.3.3. Information on data processing requirements regarding webshops

The legality of data processing of webshops are regularly questioned by the complaints sent to the Authority. Due to the great number of submissions the Authority considered it appropriate to issue guidelines on data protection requirements regarding webshops. To help both data controllers who operate webshops and data subjects who buy goods and services online.
https://www.naih.hu/files/2017-02-17-webaruhaz-tajekoztato-NAIH-2017-1060-V.pdf

The information gives assistance – through the procedural experiences of NAIH, as well as through real-life examples and best practices – for the target audience to identify the legal background of operating a web shop. It discusses the legal basis of data processing, the consent of the customers (preliminary information and consent), rights and obligations. It also provides an overview on cookie-s and newsletter service from a data protection view.

IV. Data Protection Audit and BCR's

IV.1. Data protection audit

2016 was the year of trend change. The majority of the data protection audits were "concept audits" meaning that the Authority reviewed the concepts of the data processing activities prior to the data processing.

The Authority welcomed the changed attitude of data controllers, as this way, a more successful and effective audit can be carried out assessing all the relevant data protection aspects prior to the processing. The controller can communicate more freely during the audit since a processing operation which has not yet been started can be changed more easily.

This approach is also welcomed because data controllers involved in such data protection audits were involved in a process very similar to the data protection impact assessment described in Article 35 of the General Data Protection Regulation, thus contributing to the transition of the new Regulation. NAIH audit is very similar to the above mentioned DPIA, as both documents contain a systematic description of the planned data processing operations; the purpose of the data processing, including the necessity and proportionality of the planned operations; assessment of risks to the rights and freedoms of the data subject; and all measures necessary for mitigating risks. Accordingly we may state that the Authority's data protection audit practices has been evolved into a quasi-privacy risk assessment.

IV.2. Binding Corporate Rules (BCR)

In 2016 NAIH received 26 applications for the approval of BCR. These had been already approved by other EU Member States data protection authorities (as leading authorities) after the completion of the cooperation procedure set out in the WP107 working document created by Article 29 Working Party.

The approved BCRs are published on the website of the Authority in order to promote awareness of the data subjects:

Date of approval	Name of the company	Data controllers using BCR in Hungary
15.12.2016	Novartis	Novartis Hungária Kft.
15.12.2016	Novartis	Alcon Hungária Kft.
15.12.2016	Novartis	Sandoz Hungária Kft.
15.12.2016	Intel	Intel Corporation Hungary Kft.
21.11.2016	Amgen	Amgen Gyógyszerkereskedelmi Kft.
21.11.2016	Johnson Controls	Johnson Controls Mór Bt.
21.11.2016	Johnson Controls	Johnson Controls Management Mór Kft.
21.11.2016	Johnson Controls	Johnson Controls International Kft.
21.11.2016	Johnson Controls	Johnson Controls Autóakkumulátor Kft.
21.11.2016	Johnson Controls	Adient Mezőlak Kft.
28.09.2016	Flextronics	Flextronics International Kft.
02.09.2016	American Express	Global Business Travel Magyarország Kft.
02.09.2016	American Express	American Express Services Europe Limited Fióktelep, Magyarország
26.08.2016	Novo Nordisk	Novo Nordisk Hungária Gyógyszer Kereskedelmi és Szolgáltató Kft.
23.08.2016	Citigroup	Citibank International Limited Magyarországi Fióktelepe
23.08.2016	Citigroup	Citibank Europe plc. Magyarországi Fióktelepe
11.08.2016	LeasePlan	LeasePlan Hungária Zrt.
29.07.2016	ING	ING Bank N.V. Magyarországi Fióktelepe
29.07.2016	Ernst & Young	Ernst & Young Könyvvizsgáló Kft.
29.07.2016	Ernst & Young	Ernst & Young Tanácsadó Kft.
29.07.2016	Ernst & Young	EY Training Center Kft.
29.07.2016	Ernst & Young	NCOA Kereskedelmi és Szolgáltató Kft.
29.07.2016	Ernst & Young	Vámosi-Nagy Ernst & Young Ügyvédi Iroda
28.07.2016	Philips	Philips Magyarország Kereskedelmi Kft.
28.07.2016	Philips	Philips Lighting Hungary Kft.
28.07.2016	Philips	PHILIPS INDUSTRIES Magyarország Elektronikai Mechanikai Gyártó és Kereskedelmi Kft.

08.07.2016	UCB	UCB Magyarország Kft.
08.07.2016	Cargill	Cargill Takarmány Zrt.
08.07.2016	Cargill	Cargill Magyarország Zrt.
08.07.2016	Shell	Shell Hungary Zrt.
20.06.2016	BP	BP Business Service Centre Kft.
2016.06.20	BP	BP Europa SE Magyarországi Fióktelepe
20.06.2016	BP	Castrol Hungária Kft.
24.05.2016	Capgemini	Capgemini Magyarország Kereskedelmi és Szolgáltató Kft.
24.05.2016	AstraZeneca	AstraZeneca Kereskedelmi és Szolgáltató Kft.
2016. 04.19	GE	GE Hungary Ipari és Kereskedelmi Kft.
19.04.2016	GE	General Electric International, Inc. Magyarországi Fióktelepe
19.04.2016	GE	GE Infrastructure Central & Eastern Europe Holding Kft.
19.04.2016	GE	GE Infrastructure Hungary Holding Kft.
19.04.2016	GE	GE Holdings Forint Hungary Kft.
19.04.2016	GE	GE Közép-Európai Ellátó és Szolgáltató Kft.
19.04.2016	GE	GE Water and Process Technologies Hungary Termelő és Szolgáltató Kft.
19.04.2016	GE	Zenon Systems Termelő és Szolgáltató Kft.
19.04.2016	GE	GE Energy Parts International, LLC Magyarországi Fióktelep Granite Services International Inc. Magyarországi Fióktelepe
19.04.2016	GE	Alstom Hungária Zrt.
07.03.2016	Corning	Corning Hungary Adatfeldolgozó Kft.
07.03.2016	GlaxoSmithKline plc	GlaxoSmithKline Kft.
07.03.2016	GlaxoSmithKline plc	GlaxoSmithKline Biologicals Kft.
07.03.2016	GlaxoSmithKline plc	GlaxoSmithKline-Consumer Kft.
11.02.2016	Continental Group	Continental Hungaria Kft.
11.02.2016	Continental Group	Contitech Magyarország Kft.
11.02.2016	Continental Group	Continental Automotive Hungary Kft.

11.02.2016	Continental Group	Contitech Rubber Industrial Kft.
11.02.2016	Continental Group	Continental Fluid Automotive Hungária Kft.
09.02.2016	HP Inc.	HP Inc Magyarország Kft.
09.02.2016	Hewlett Packard Enterprise	Hewlett-Packard Informatikai Kft.
09.02.2016	Hewlett Packard Enterprise	Hewlett-Packard Magyarország Kft.
09.02.2016	Hewlett Packard Enterprise	Hewlett-Packard Technológiai Licencek és Licencnyújtó Kft.

V. Freedom of Information (FOI)

NAIH's obligation arising from the Fundamental Law is not only the protection of personal data, but to guarantee the constitutional right of citizens to have free access to public information on the operation and management of the State. For the enforcement of transparency, state and local government bodies as well as companies of major state ownership had to be investigated in 2016. When the Authority's actions have not produced an effect, defaults had to be summarized in a report. Some parties still continued to dispute their status as body with public service functions, others wanted the disclosure of information underlying a decision to be interpreted broadly to limit publicity.

V.1. Bodies with public service functions

Since the Privacy Act contains no exact definition for public service function it can only be determined in relation to an individual case, taking into account all the circumstances. However, the concept should be broadly understood thus a wide range of activities is included.

The features determining a body with public service functions are wide. It may mean functions when the body or individual performs state or local government duties, as well as other public tasks defined by legislation. It also covers the management of national asset with the consequences that state or local government-owned companies cannot exclude themselves with reasoning that they are not bodies with public service functions as set out in legislations.

Decision 6/2016 (III. 11.) AB (Constitutional Court) concludes that in terms of freedom of information, all that matters is that the body processes public information, and therefore – in order to enforce the right of access to public information – has an obligation to comply with the data request. This is a general obligation and as such shall not be restricted with the limitation of the circle of the addressed bodies as it would limit the right of access to public information.

In one case, NAIH investigated the company called Erzsébet Üzemeltető Kft. (hereinafter: Company) which has refused to disclose information upon the argumentations that the Company is not processing data of public interest or data public on grounds of public interest and does not fall within the scope of the Privacy Act. According to the content of the Hungarian business register, the Authority

found that the Company is owned by HUNGUEST Vagyonkezelő Zrt., a private limited company, and more than 50% of voting rights belong to Magyar Nemzeti Üdülési Alapítvány (Hungarian National Recreational Foundation), which was set up to operate within the framework of a governmental program the property complex for providing holidays and recreational camps primarily for socially disadvantaged children. Therefore the Company is to be considered as a body with public service functions and has to provide information on contracts aimed to operate recreational camps with a contractual worth of more than 5 million HUF.

In another case, the definitions of *data controller* and *data processor* have been investigated in terms of FOI. The Cabinet Office of the Prime Minister refused to provide information on the accepted concept of the differentiated organization of human public services. The Cabinet Office referred to the relevant governmental decree, which entrusts the Minister of Human Capacities with the development of the concept and thus the Cabinet Office identified itself as no data controller of the concept in question. In view of Decision 6/2016. (III. 11.) AB (Constitutional Court), NAIH found that the above argumentation is false, denying to be a data controller is also not applicable therefore the Cabinet is obliged to provide information on the concept mentioned in the decree.

NAIH also investigated the Hungarian Court Bailiffs' Chamber as a body with public service functions. The Chamber refused to provide information on contracts worth at least 5 million HUF with the reasoning that the Chamber does not manage public funds, therefore the information in connection with the contracts do not qualify as public information. Moreover, disclosing the data would cause disproportionate difficulties for the Chamber. NAIH found that according to Act LIII of 1994 on Court Bailiff and in view of the Privacy Act the Chamber is a body with public service functions and therefore it must comply with Sections 26-30 of Privacy Act. Furthermore, the difficulty of providing public information is not a legitimate ground for refusal, but only a factor affecting the method and costs of disclosing public data.

In connection with the fully state-owned Nemzeti Eszközgazdálkodási Zrt. (hereinafter: Company) exercising ownership rights on state assets NAIH found that it is a body with public service functions and all the information in connection with its wealth management is considered to be public. Therefore information on the contract regarding the public procurement for due diligence of Adriatiq Island Group shall be made accessible to anyone with a claim access to these information. The data controller has violated the requesting party's right to access to data of public interest or data public on grounds of public interest when it refused to provide information on this contract.

NAIH reached the same conclusion regarding a company owned exclusively by a municipality. According to the provisions of the Fundamental Law, the Privacy Act, Act CVI of 2007 on State Property and Act CXCVI of 2011 on National Property the municipality owned company qualify as a body with public service functions and therefore is obliged to provide information to a request on data of public interest regarding the use of public money.

In 2016, NAIH received many submissions dealing with the sessions of the national student union, in particular with the publicity of the minutes of the union's meetings, of the Senates' meetings and also of the disclosure of the union's officials' personal data.

A specific case focused on the publicity of the minutes of the National Conference of the National Student Union (hereinafter: HÖOK). According to Act CCIV of 2011 on National Higher Education HÖOK represents the students on national level. HÖOK is considered to be a legal entity represented by its president. Its legal functioning is supervised by the public prosecution and its accountancy obligations are similar to other entities. The main function of this body is to represent the students on a national level within the democratic system of the higher education, which shall be inevitably considered as a public service function. This interpretation is supported by the fact that the member organizations of HÖOK are *sui generis* considered as bodies with public service functions, whereas their active participation in the functioning of the organization further strengthens its public body function. The final conclusion of NAIH was that the HÖOK carries out tasks associated with the democratic functioning of the higher education therefore HÖOK is a body with public service functions and as such is obliged to perform its duties deriving from the Privacy Act.

V.2. Personal data public on grounds of public interest

In 2016 NAIH received numerous submissions regarding the access to personal data of persons undertaking public duties. The most frequent questions were about wages, regular bonuses and asset declarations of these persons.

Request for disclosing information (including on the procedure, on the conditions and on the persons making the decisions) about wage bonuses received between 2010-2016 by the permanent secretaries of State and deputy secretaries of State working at the Cabinet Office of the Prime Minister was refused by the

Cabinet Office. NAIH found that this issue is linked with the use of public funds therefore the principles of transparency and verifiability shall be strictly respected. However the conflict between the right of informational self-determination and on freedom of information has to be balanced.

A balancing test shall examine whether the right to privacy shall not be disproportionally violated when disclosing personal data in connection with performing public duties. Typical categories of such data are personal allowances (both natural and pecuniary) given to higher ranked officials e.g. board-wages, premiums, replacement remuneration, wage allowances. These wages are considered as *personal data connected with the performance of public duties* and thus available for the public. However, the benefits assigned on a social or necessity basis e.g. housing, family or social supports belong typically to the private sphere of the beneficiary – who might happen to be a public servant supported by his employer (in this case a public organ). Therefore, in this latter fall the names should not be disclosed automatically but only with the consent of the data subject.

Section 26 (2) of the Privacy Act defines each personal data public which is linked to the official responsibilities of the individual performing state or local government responsibilities. This includes the amount of wages and bonuses of state secretaries, the name of the decision-making person and every factor orienting the decision on these benefits. Therefore the Cabinet Office has violated the requesting party's right to access to data of public interest when it refused to provide information on the above subject.

The same conclusion was reached regarding conditions of payment and reimbursement of travel expenses (including the financial support of local transport passes) granted for a notary of a local government. Concluding the investigation, NAIH found that the category of *"data on allowance"* need to be interpreted broadly, as it shall include all the emoluments and benefits regarding the civil service relationship. The publicity of these data can help – among other things – the realization of the principle of equal treatment when it comes to salary and other benefits.

Therefore any allowance received by the municipal notary are public data. When the major of the local government – as the employer of the notary – refused to provide information on the requested data, the requesting party's right to access to data of public interest or data public on grounds of public interest has been violated.

In relation to the publicity of asset declarations NAIH found the violation of the Privacy Act when the requester was allowed to submit his/her request for access to public information only in writing or when he/she was able to access the information only in person, that is to say by means of a personal appearance. It also violates FOI when the citizen is not able get a copy of the asset declaration of a municipal government council member. The asset declarations of the mayor and the representatives of local governments are data of public interest, which must be made available to anyone in accordance with the relevant legal provisions.

In another case, NAIH also emphasized that the rules on FOI set out in Privacy Act are applicable to the data contained in the asset declarations of national minority municipality representatives. However, Act CLXXIX of 2011 on the Rights of National Minorities declare these documents only as public, but does not require their disclosure. Consequently the disclosure of asset declarations of national minority municipality representatives may not be ordered by the local municipality on mandatory basis.

V.3. Information underlying a decision

FOI as a fundamental right is not absolute, in some cases exemptions or even exclusions from disclosure might be applied. The rules of the restriction can be found in Section 27 of Privacy Act, particularly important are the provisions in connection with the limitation of publicity of information underlying a decision.

The main aim of the protection of information underlying a decision in the decision-making process is the fulfilment of public duty free from unauthorized influence.

Information compiled or recorded by a body with public service functions as part of, and in support of, a decision-making process for which the body is vested with powers and competence, might not be made available to the public for ten years from the date it was compiled or recorded. Access to these information may be authorized by the head of the body that controls the information in question upon weighing the public interest in allowing or disallowing access to such information. According to Privacy Act, request for disclosure of information underlying a decision may be rejected, if the data really serve as substantial element of the decision making process, and the disclosure is likely to jeopardize the successful enforcement of the decision e.g. by providing unreasonable advantage for given companies.

After the decision was made, the protection can be maintained if the disclosure is likely to jeopardize the legal functioning of the body with public service functions or the discharging of its duties without any undue influence, or it may also influence future decisions.

If the information in question is part of a collection of data upon which a decision was made, but other parts of it will still be subject of a decision, these elements of the collection of data will not be public after a decision was made on a different part of data. It is not clear however, which data might be connected to a future decision. An information can be the basis of numerous further decisions. Additionally, access to information that has already been subject to a decision, but will likely be used in further decision-making processes, may be restricted. Identification of such data is nevertheless ambiguous, since any information may serve as the basis for numerous further decisions. Such a broad application of the restriction of freedom of information would however be unconstitutional.

After the decision, bodies with public service functions have to consider whether there is public interest in connection with the data inspection which underlies the restriction of publicity. If not, for example the decision has already been made, no further measures have to be taken and the data shall be disclosed. Similar consideration has to be taken in connection with information subject to further decisions: it has to be examined whether there is any decision, which might be unduly affected by with giving out information underlying a previous decision. In the absence of such reasons, FOI cannot be restricted.

In one case the National Election Office (hereinafter: NVI) refused to make accessible a guidance on inspection of signatures collected in connection with a petition for a referendum. NVI referred to as a ground for the refusal that the guidance contains data on information underlying a decision.

In the investigation – based on the data-principle and also on the practice of the Constitutional Court –, NAIH declared that the publicity of information underlying a decision can be restricted but not in a discretional mode. The restriction can be justified only on the basis of strict requirements laid down in the relevant decisions. NVI's decision was in line neither with the Fundamental Law, nor with Privacy Act and thus it has violated the requesting party's right to access to data of public interest or data public on grounds of public interest. For one part, NVI did not justify properly what is the ground of the restriction of publicity requested by the party. "*Inspection of signatures without any influence"* as reason cannot be considered as well-founded. On the other hand, NVI has failed to examine

the possible effects of publicity on the affected employees' work. NAIH's opinion was further supported by the fact that days after the refusal of the disclosure NVI made the requested document public as a response to "false statements" appeared in the press. Finally, instead of selecting the concrete data set, the whole document was considered as restricted within the meaning of Section 27 (5) of Privacy Act. Therefore NVI has violated the fundamental requirements set out in several decisions of the Constitutional Court.

In another case, after receiving a consultation submission, NAIH examined Section 9 (1) of the Governmental Decree 257/2016 on Municipality ASP[63] System, which says that *„information provided in the data registry contained by the governmental and local governmental decisions is underlying decisions".*

This interpretation, exceedingly qualifying the whole content of the registry as information underlying a decision, would violate both Privacy Act and Fundamental Law. On one hand, the kind of practice based on this interpretation undermines transparency of decisions made by state or governmental bodies regarding their data register. On the other hand, information underlying a decision cannot be qualified as restricted generally in view of the register. An information can also serve as foundation for any future decisions: an abstract relationship with an uncertain decision shall not justify restriction of FOI. This would entirely deprive the basic right to access data of public interest and data public on grounds of public interest.

In another case NAIH started an investigation because the Ministry of National Economy (hereinafter: NGM) refused to provide information on preparatory legislation impact assessments regarding the *Családi Otthonteremtési Kedvezmény* (family home purchase subsidy scheme, a non-refundable aid by the government for housing families). According to NGM, these documents contain information underlying a decision.

NAIH emphasised that according to relevant legislations, the summary of the preliminary impact assessment in accordance with the draft released for public negotiation should be made public. In case of data with obligation of disclosure, the reference to the quality of information as of underlying a decision is false since the online proactive publicity is ordered by law. This means that this part of the studies – or at least the internet links – should have been sent to the requesting party.

63 Application Service Provider: professional management and tax system for municipal governments

NAIH also found that access to documents shall be distinguished in accordance with the status of the relevant legal act based on the studies. By the creation of the legal acts, the interest of keeping the supporting analyses and studies as secret ceases. Only the disclosure of those parts of the documents might be considered acceptable, which are contrary to the legal acts or which parts of the studies have not been finally used. Summarizing the above, NAIH was on the opinion that the proceeding of NGM was contrary to the fundamental requirements on the restriction of publicity of information underlying a decision.

V.4. Rules of reimbursement of costs regarding data requests

In 2016 the 301/2016. (IX. 30.) Governmental Decree on the Costs of Disclosure of Information (hereinafter: Decree) was accepted and came into force on 15 October 2016. The amendment of the Privacy Act (coming into effect on 1 October 2015) provided the opportunity – in some cases – for bodies with public service functions processing the data in question to charge a fee and to communicate this amount to the requesting party in advance. However, the law did neither specify the cost elements nor the amount of the fee. The lack of proper legislation opened the possibility for abuses in resulting a constant challenge for the law enforcement practice. According to NAIH, the Decree would provide proper remedy for these problems.

It should be noted that with regard to the rules of Privacy Act, charging a fee is not obligatory, but left to the discretional competency of the body concerned.

In case of requests submitted prior to the entry into force of the Decree, the costs can be charged in accordance with the principles and rules developed by NAIH.

If the body decides not to exercise this right, it is not possible to determine it subsequently. Similarly, it is forbidden to demand from the requesting party the cost difference between the preliminary calculated/reimbursed costs and the actual costs.

It should be noted that according to Act CXXVII of 2007 on Value Added Tax VAT is irrelevant when it comes to the fulfilment of requests regarding data of public interest. Therefore, bodies with public service functions may not charge VAT in relation with the cost of disclosure.

Based on the Privacy Act, there are three cost elements in the Decree. According to Section 29 (5) point c) of Privacy Act, *in determining the fee chargeable the following cost items can be taken into account:*

a) the cost of the data storage device containing the requested information,

b) the delivery fee of the above data storage device to the requesting party,

c) if the fulfilment of the request for information requires disproportionate workforce needed for the ordinary operation of the body, the additional labour costs needed.

No other cost elements may be charged, as it would be contrary to Privacy Act.

Regarding the data storage devices, the cost of requesting copy is determined by the number of pages, not by document sheets. Since the minimum number of pages that may be taken into account is 10, therefore short documents containing data of public interest and data public on grounds of public interest cannot be subject to cost reimbursement. Delivery costs are not determined in the Decree, therefore postal service fees should be taken into account.

The amendment of the Privacy Act in 2015 provided the opportunity for bodies performing state or local government responsibilities to charge a fee for additional labour costs. In this regard, a lot of questions have been raised prior to the entry into force of the Decree, for example: what can be considered as additional labour costs, what types of costs can be determined, when can bodies charge a fee for reimbursement in relation to that cost element.

According to the Decree, cost of workforce may cover the time necessary for the identification, collection and arrangement of the requested data, the time for the duplication, and the time necessary for the anonymization of data that may not be accessible by the requesting party. If this period exceeds four working hours, this cost element should be calculated in the following way: the working hours of the correspondent must be multiplied by the actual labour costs per hour of work (according to the Decree, this amount may not exceed 4400 HUF). Other contributions, bonuses, rewards and other benefits, such as fringe benefits cannot be taken into account.

It is important that the extra labour expenses cannot be considered “remuneration” of fulfilling the request for data of public interest, which is not a service but a constitutional obligation of the concerned body. Moreover, providing copies cannot be considered as business activity but a possibility to ask for compensation in connection with raw material costs from the requesting party. Privacy Act

allows it only if it requires disproportionate heavy workload compared to basic duties of the given organ. In this meaning, outsourcing of work does not mean disproportionate workforce: cost reimbursement is only available in connection with the copy, not with additional labour costs.

Finally, NAIH emphasises that according to Privacy Act, bodies with public service functions have the obligation to provide information for parties requesting public data on the detailed amount of these costs, including all the reasons and cost elements. This does not mean that these obligations are restricted to provide information on the reimbursement rates of the cost elements. Providing proper information helps the requesting party to understand clearly, why and what kind of costs have to be paid in order to get the required data, and it also helps to decide on what legal remedies to choose.

V.5. NAIH's activities related to the prevention of corruption

NAIH has stated many times that FOI plays a key role in the prevention of and fight against corruption. The deterrent effect of publicity can also prevent these situations therefore special attention has always been payed to this topic.

In 2016, NAIH representatives have contributed to several anticorruption initiatives. In this context the educational and informative activities related to commitments within the initiative called Open Governmental Partnership shall be noted, which has given a real opportunity to create a close cooperation between the National Protective Service, the National University of Public Service and NAIH.

NAIH helped to create an e-learning curriculum for the fulfilment of these commitments in the spirit of 1460/2015. (VII. 8.) Governmental Decree. NAIH also became a member of the Integrity Development Committee of the National University of Public Service, which aims to help the development and renewal of education of integrity advisors within university frameworks.

In close cooperation with National Protective Service, NAIH participated in a workshop (22.10. – 12.12.2016) aimed to guarantee transparency in local municipality decision-making processes and also assisting publishing decisions with a help of a methodological guide.

VI. Legislative activity of NAIH

The table below shows the number of opinions on draft bills issued in recent years.

Opinions on draft bills according

Source of law	**2014**	**2015**	**2016**
Act	33	79	85
Government resolution	63	133	98
Ministerial decree	85	126	83
Government resolution	21	61	29
Other (parliamentary resolutions etc.)	7	27	20
Total	**209**	**426**	**315**

Number of remarks appeared in the opinions

Remarks related	**2015**	**2016**
Data protection-related	298	222
Freedom of information-related	53	101
Other	137	127
Total	**488**	**450**

The number of opinions on draft-bills dropped by about a quarter compared to 2015. However, a similar or greater case number fluctuations are common in recent years, therefore this single data is not enough to draw far-reaching conclusions.

Another important indicator is the number of substantive comments and proposals during the legislative preparatory discussions, suitable for comparisons between years. As we can see, the number of proposals slightly decreased compared to 2015, which indicates that despite the decline in the number of cases, the Authority pays similar attention to the informational rights as in previous years.

When making a distinguish between the reviewed draft legislations, one of the possible classification is that they are either developed on the basis of a long-term strategy and policy concept achievement, or answer unexpected regulatory

needs (which we believe that has grown in 2016). Looking for its reasons we see that the widespread and massive international migration in recent years that has reached Europe is a completely new and unprecedented phenomenon that could not be foreseen. In parallel, genocide terrorist attacks have been committed in European cities. We see that the stability in the world has decreased and such unfavourable changes occur, which will test the adaptability of countries and societies. These changes obviously generate a strong public response. The new challenges include the preservation of the country's stability and further legislation is needed for anti-terrorist actions as well. Obviously, these legislative changes will affect the legal regulatory conditions of informational self-determination and freedom of information, but it is not yet clear where the new balance of informational rights between the state and the citizen will be created. To what extent should informational rights be sacrificed in order to preserve our security? When speaking about regulatory related cases, we would like to present the dilemmas, the ways of finding answers to these questions.

VI.1. Combating terrorism: regulation on terrorist emergency

At the beginning of 2016 we learned from the press that the Ministry of Defence started negotiations involving parliamentary parties about the modification of special legal orders of the Fundamental Law, adding terror-related rules to it. This raised several constitutional concerns. The substantive question for the Authority was of course how informational rights could be affected by the proposed changes. In addition, we had to assess also that whether availability of data of public interest and the democratic values of the constitutional rule of law are in line with the fact that the political discussion about the amendment of the Fundamental Law organised by a ministry takes place behind closed doors. However, the first step was to make it clear whether the Authority may investigate the content of the amending draft.

The Authority took the view that the (amendment of the) Fundamental Law is the act of the constitutional power, which establishes the basic rules of the State, the system of the fundamental rights and goals. Therefore, the Fundamental Law constitutes untouchable public law reference system for state bodies born within its framework. The task of the state bodies is to give expression to the public will materialised in the Fundamental Law, in accordance with the regulations with their powers and duties. Consequently, the Authority respects the autonomy of the constitutional power. In this situation, the Authority's role is only to indicate

that an adopted amendment of the Fundamental Law would obviously create an internal conflict in conjunction with the informational rights set out in the Fundamental Law or in this respect it would be manifestly contrary to an international commitment of Hungary.

The formal analysis of the Authority's powers defined in the Privacy Act leads to the same conclusion. Indeed according to Section 38 (4) of Privacy Act, the Authority has powers to make recommendations for new legal regulations. According to Article T (2) of the Fundamental Law, legal regulations shall be Acts, government decrees, prime ministerial decrees, ministerial decrees, decrees of the Governor of the National Bank of Hungary, decrees of the heads of autonomous regulatory organs and local government decrees. In addition, decrees of the National Defence Council adopted during a state of national crisis and decrees of the President of the Republic adopted during a state of emergency shall also be legal regulations. Amendment of the Fundamental Law is not subject to legal sources listed above, so making recommendations on amendments of the Fundamental Law is not covered by the Authority's tasks defined in Privacy Act.

However, the Authority is competent expressing its opinion on drafts covering the amendment of the Fundamental Law and if appropriate, propose to adopt, amend or repeal such legislation.

Based on the analysis of the draft legislative package related to the amendment of the Fundamental Law, the Authority concluded that the examination of the statutory regulation on terrorist threat situation should not be conducted outside of its regulatory environment, because the common rules of the special legal order fit the legislation on terrorist emergency in a single regulatory structure. It already shows similarities to other legal institutions of special legal order, including certain rules and measures related to the introduction of the preventive defence. Therefore the Authority has examined, what constitutional limits can be defined on the different legal institutions of the special legal order considering fundamental informational rights. Answering these questions primarily falls under the competence of the Constitutional Court. However, the Constitutional Court will only take a position on an open question if the person entitled to initiate proceedings at the Constitutional Court turns to the body.

The review of the draft legislative package as well as the standards of the fundamental informational rights lead the Authority to make the following conclusions and comments:

– In Act CXIII of 2011 on National Defence and the Hungarian Armed Forces and the special measures deployable during special legal order (hereinafter referred to as: Hvt.) it is necessary to specify the substantive definition of terrorist threat and what are the thresholds of the introduction of emergency measures which are needed to avert actual emergencies. It is important to make the date of commencement of the terrorist threat situation clear, because this date is decisive regarding the incorporation of the restrictive measures. Also, the expiry or extension of the terror threat emergency period is adapted to this date accordingly.

– Having regard to Article 54 (4) of the Fundamental Law, clarification is needed in the Htv. to make sure which public body is entitled to apply the extraordinary measures introduced during the terrorist threat situation, what is the scope of their powers, what is the essence of the exceptional measures, for what purpose, against whom and how, under what conditions can these measures be applied.
– The Authority initiated to get to know the draft set out in Section 64 (7) of Hvt. so it can fulfil its task to make recommendations for new regulations set out in Section 38 (4) of Privacy Act.
– The Authority proposed considering the initiation of asking the interpretation of the Constitutional Court on the authorisation of limited rights beyond Article I (3) set out in Article 54 (1) of the Fundamental Law.
– The Authority invited the Chief of Staff of the Hungarian Armed Forces to take measures clearing the “NON-PUBLIC!” marking on the document containing the amendment of the Fundamental Law, as well as documents containing the amendment to the related drafts, because the amendment of the Fundamental Law in a democratic state is a public matter concerning every citizen. If the decision-making process has reached a stage where the political parties are consulting the amendments, the draft should be made public for discussion.

VI.2. Combating terrorism: the legislation package on home affairs

The anti-terrorist legislative package prepared by the Ministry of Interior reacting on the recent terrorist acts committed in Western European cities and also on the strong growth of the migration pressure, as well as the related negative phenomena in response to these difficulties envisaged amendments also restricting the right of informational self-determination in some cases. During the administrative discussion of the bill and also during the parliamentary debate the Authority has published its position. NAIH pointed out that the obligation of the State to pro-

tect fundamental rights laid down in the Fundamental Law means *inter alia*, that the legal restriction on informational rights resulting from the anti-terrorist action should not exceed what is necessary and proportionate and should not result too much informational power of the State over the citizens. Therefore it must contain the guarantee system of data protection and the protection of privacy in accordance with the relevant legislations.

The legislative package sets out such legal restrictions with preventive and protective nature which duration is not specified. It is not known whether they are temporary or long term restrictions. The proposed legal restrictions are constitutional and legitimate only as long as their cause, that is, the pressure caused by increased migration and the possibility of a terrorist threat exist. Therefore, the Authority has recommended that the legislature should periodically review the maintenance of these measures.

The measures set out in the anti-terrorist legislative package provide an opportunity for the National Security Services for automated data collection. Automated data collection eliminates the involvement of the data controller body and therefore increases the risk of unnecessary, unreasonable, mass data collection by National Security Services. Therefore, the Authority considers that automated data collection requires stronger privacy control regime within National Security Service departments and also within external independent evaluations. This need is supported by the fact that in the decision on destruction of the legal grounds of Safe Harbour system, the Court of Justice of the EU noted that the mass surveillance carried out by US Homeland Security is in accordance with the principles relating to the protection of European citizens' personal data. The European democratic states – including Hungary – have to meet the data protection and privacy-protection requirements and they can require other countries to respect these requirements as well.

The Authority also drew attention that entry into force of Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (hereinafter referred to as: Directive) requires the revision of the anti-terrorist measures. Chapter IV of the Directive sets out new kind of obligations, such as privacy by design and by default, data protection impact assessment and prior consultation with the supervisory authority. It sets out more detailed and comprehensive obligations on records of processing activi-

ties (Article 24) and logging (Article 25). Article 26 is a new legal instrument which regulates cooperation with the supervisory authority, it requires controller and the processor to cooperate, on request, with the supervisory authority in the performance of its tasks on request, while Article 30 requires the notification of a personal data breach to the supervisory authority. The Directive sets out new criteria for data transfer to a third country or to an international organisation.

VI.3. The anti-terrorist action: to oblige providers of information society services to cooperate with each other

The rapid development of information and communication technology did not stop with mobile phone technology. Within the new generation of electronic communications networks, the voice communication and electronic data transmission become more and more unified. Together with the appearance of a number of smart devices, applications and services related to communications appeared as well and the communication infrastructure is provided by these electronic communications services. This raises questions – and also attracted public attention in 2016 – regarding national security and law enforcement issues in the relation of protecting fundamental rights.

For example, with an application that is able to encrypt communication between endpoints at a time, the monitoring of the content of the communication can be prevented even if the public body conducting the monitoring is capable of understanding the signals transmitted over the network.

Therefore, the Ministry of Interior has prepared a legislation which required the electronic communications services within the scope of Act CVIII of 2001 on Electronic Communications (hereinafter referred to as Ekertv.) to provide access for entities authorized to gather secret information to data which is being transmitted via applications with encrypted communication systems. In addition, under the legislation, the e-commerce service providers are obliged to keep the data the subscriber or user and metadata of the communication.

This type of secret information gathering raises similar regulatory issues as that in the case of electronic communications services. There is no doubt that a greater proportion of communication is shifting from the traditional communica-

tions services to the application services. The new tools, services and applications started to play increasing role in individuals' privacy, therefore monitoring and gathering information from these communications by the State is suitable for gathering more detailed information than the surveillance of traditional electronic communications services (especially telephone calls) in the past, consequently, it enables a much deeper and more detailed understanding of the individual's privacy, communication and relationship system.

An additional risk to privacy is that the observation of data processing and communications observation can be more automated and wide scale by reducing or eliminating the intensive work, compared to the monitoring of traditional electronic communications services.

The secret information gathering from application services means stronger intervention and more risk associated with the individual's privacy and right to informational self-determination as the monitoring of electronic communications services, so the Authority considers that the regulations must contain additional warranties on data protection.

When speaking of data retention, the aspects related to the data retention of electronic communications services should be considered as basis for the e-commerce service providers as well. In 2014 the Court of Justice of the European Union invalidated the Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. According to the Courts judgement, the Authority did not consider the data retention on general basis, stockholding basis and for one year period admissible.

The Authority recommended defining the aim of the data retention in the regulation. While the overriding state interests – like the fight against terrorism or the response activities of the national security services – can have justifiable grounds within appropriate legal framework for the introduction of the obligation to retain data, in another case, for example the State control of home computers and people using torrent file sharing, the intervention would be disproportionate to the intended objective.

VI.4. The anti-terrorist action: protection of data on the safety of transport infrastructure

The amendments of legislations on the limitation of the publicity of data in connection with the safe operation of rail transport infrastructure and particularly important facilities to prevent terrorist attacks (Act CXLIV of 2016, Act XXXIV of 1995 on the Police and Act CXXVIII of 2016) came also in the scope of the Authority.

These rules do not protect personal data but the right of access to public information. The draft rules were not submitted to NAIH, however, Dr. Bertalan Tóth MP asked for a detailed resolution on the legislative amendments of the bills with an opportunity to explain, what are the criteria for reviewing these legislations, as well as similar restrictions on public information.

The Authority seeks to fully integrate the jurisprudence elaborated by the Constitutional Court, regarding the protection of fundamental rights and constitutional requirements. Our theoretical starting point is that the right to the dissemination of data of public interest and data public on grounds of public interest is being interpreted by the Constitutional Court as informational right, which was confirmed in its decision following the entry into force of the Fundamental Law as well. Freedom of information *"allows the control of the public representative bodies of the executive power, the legality and effectiveness of the administration, stimulates their democratic functioning"* (Constitutional Court Decision 32/1992. (V. 29) AB). On the other hand, freedom of information is a matter of justice and common starting point for the freedom of expression. This fundamental right plays a major role in shaping the democratic functioning of the State (Constitutional Court Decision 34/1994. (VI. 24.)

In addition to the decisions of the Constitutional Court, the framework of informational rights are defined by the Privacy Act, which is defined in Section 1. The Privacy Act defines the basic rules of protection of personal data and the enforcement of the right to access and disseminate data of public interest and data public on grounds of public interest. For example, that at least what subjects should be regulated in a sectoral legislation on mandatory processing. The Privacy Act also defines the aim of restriction of disclosing data of public interest in sectoral legislations. Tarnishing these rules is not possible in such a way that the law governing the processing of data derogates from the Privacy Act, and weakens the guarantees of informational fundamental rights in different areas coordinated by sectoral legislations.

In this specific case, the Authority made the following statements:

- The legislative amendments are in line with the Privacy Act. Preventing terrorist acts fall within the scope of law enforcement and national security interests. According to Section 27 (2) point b) and c) of Privacy Act, right of access to data of public interest or data public on grounds of public interest may be restricted by law – with the specific type of data indicated – where it is considered necessary to safeguard national defence and national security.
- The legislative changes include what data the restrictions apply on. Determining the scope of data is essential for determining the content of the subject of limitations. The Hungarian informational fundamental rights legislation enforces data principle according to the constitutional requirements extracted by the decisions of the Constitutional Court.
- In recent years some of the terrorist attacks against different big cities targeted public infrastructure or governmental operation and objects dealing with public supplies. The restrictions may apply only to those data which are sensitive in terms of the terrorist threat: just safety, security, technical, operational data may be involved. On the other, data relevant to the enforcement of freedom of information, such as limiting the information on budgetary needs and environmental impacts of the investments in facilities are not covered by the present draft amendments.
- Important guarantee of freedom of information is that the bills in question do not require *ex lege* publicity restrictions but balancing of the interests, that is, in connection with the data for which the request was submitted, the data controller must always consider whether the legal conditions of restriction of publicity exist or not. Disclosure of data would endanger the State's national security interests, or interests in crime prevention.
- The amendments set out a 30 years restriction on dissemination of classified information. The statutory definition of the deadline is important because if the rules would restrict the access to public information forever, this would affect the essential content of the right to access and disseminate data of public interest, since the essential content of fundamental rights cannot be limited.
- 30 years restriction on dissemination of classified information can be compared with the maximum validity period of the two highest classification ratings, the "Top Secret!" and "Secret", but broadly it is in line with the typical service life of the protected facilities, and therefore it can be acceptable.

VI.5. Reform of the external authorization system of secret information gathering

The review of the system of the external authorization of secret information gathering for national security purposes is mainly due because of the judgment of the European Court of Human Rights (ECHR) in Strasbourg delivered on 12 January 2016 (hereinafter to as: judgment). The judgment held, unanimously, that there had been a violation of Article 8 (right to respect for private and family life, the home and correspondence) of the European Convention on Human Rights, and no violation of Article 13 (right to an effective remedy) of the European Convention. The case concerned Hungarian legislation on secret anti-terrorist surveillance introduced in 2011. The Court accepted that it was a natural consequence of the forms taken by present-day terrorism that governments resort to cutting-edge technologies, including massive monitoring of communications, in pre-empting impending incidents.

However, the Court was not convinced that the legislation in question provided sufficient safeguards to avoid abuse. Notably, the scope of the measures could include virtually anyone in Hungary, with new technologies enabling the Government to intercept masses of data easily concerning even persons outside the original range of operation. Furthermore, the ordering of such measures was taking place entirely within the realm of the executive and without an assessment of whether interception of communications was strictly necessary and without any effective remedial measures, let alone judicial ones, being in place.

The judgment condemned Hungary because according to the rules set out in Act XXXIV of 1994 on the Police no independent external control is required when the Minister of Justice allows secret gathering of information subject to external authorization for the Counter-terrorist Centre. However, according to Act CXXV of 1995 on National Security Services, the external authorization of secret information gathering may also fall into the competence of the Minister of Justice.

The important issue of the lawsuit was the question of an independent external control safeguarding the lawfulness of secret gathering of information. NAIH was not involved in the case, so there was no way for the Authority to protect the Hungarian position by explaining its experience on independent external control of secret information gathering activities by national security services although the Privacy Act provides appropriate tools for the Authority to detect illegal secret information gathering and to take actions against the infringement.

The rules of the investigation procedure (Section 52-58 of Privacy Act) confer the power to access, to request a copy or information, to initiate an investigation in a same way as the ombudsman examinations. Section 71 of Privacy Act contains rules on the Authority's right to access information in cases related to the procedure of national security services.

The data obtained during the investigation – including national classified information – can be used by the Authority in the administrative proceedings for data protection, for example, to prohibit the unlawful processing of personal data, to order the deletion of the illegally processed data, to order the notification of the concerned data subjects in case the data controller refused to inform the affected person unlawfully, and also to impose a fine.

Based on its law enforcement practice the Authority assumes that secret surveillance deprives the data subject of using a legal remedy by its nature, this is why the independent external data protection control for the protection of informational privacy is a key element in this area. Accordingly, the Authority investigates every complaint or application regarding secret surveillance lodged by citizens, regardless whether the circumstances described in the submission show clear aspects of secret surveillance or not, and whether the person concerned can be informed of the outcome of the procedure or not.

Different models can be introduced by the modification of the prior external authorization system regarding secret information gathering. The complete independence of the external control – assigned to the court and not to the Minister of Justice – would serve the classical principle of the separation of powers, although the judgment allows also an interpretation which maintains the Minister's powers for external authorisation.

Experiences of a previous data protection investigation of NAIH indicates that the personal decision-making authority of the Minster of Justice may conflict with the requirements of grounded decision making. Director-generals of national security agencies make such a large number of submissions each year that one person – the Minister – is unable to make justified decisions. Therefore, if the power will remain within ministerial frameworks, it would be useful to set up a committee with a designated responsibility for the pre-review of the submissions on legal and necessity aspects. This commission would not be independent with members delegated by competent bodies and experts in secret information gathering, members of Ministry of Interior and homeland security) therefore would not constitute an external independent control, but could participate in preparing related decisions.

Finalising the above, it is essential that even when the jurisdiction of external authorization remains at the Minister, it still needs to be placed under an independent external control. From public legal point of view there are no obstacles to entrust the Authority – an independent data protection supervisory body as defined in the Fundamental Law with a duty of subsequently monitoring he legality of the secret information gathering – with this role..

VII. Cases concerning classified information

VII.1. Data Protection Audit of the Special Service for National Security

In 2015, the director general of Special Service for National Security (hereinafter referred to as: NBSZ) initiated that the Authority should carry out a data protection audit at the Service to review the activities and the associated data processing set out in Article 8 (1) point a) *("the NBSZ is delivering service – on written request – using secret information gathering within the framework of law, using secret data acquisition tools and methods for the activities of authorized bodies collecting confidential information.")* of Act CXXV of 1995 on National Security Services (hereinafter referred to as: Nbtv.)

The Authority has accepted the initiation but during the preparation for the tasks, it was realized that the subject of the audit is so different from other audits carried out by in our practice that if we stick to the previously well-established audit methodology, the control would have been stuck on an inadequate level without taking into account some relevant specificities of secret information gathering. In fact, it turned out that there is no formal method by which comprehensive data protection assessment could be carried out. To our knowledge, no data protection authority has ever conducted a comprehensive audit on methods of secret information gathering by national security services.

The Authority consulted with the designated experts of NBSZ on several occasions, as well as pre-analysed the internal norms of NBSZ related to secret information gathering. Finally, a new method was invented that is suitable for complex data protection inspection of secret information gathering activities in full compliance with the legal requirements.

The Authority's main conceptual starting point was that the secret information gathering from a privacy point of view is about the practical application of the significant part of essential equipment and methods, so the overall control method needs to be practice-oriented. The precedent-character of the data protection audit in question required precision and extensive work.

The established methodological requirements are the following:

Complexity: The data protection audit should cover the whole process of the secret information gathering service, from the point of the admission of a service order until the data is deleted.

Cooperation: The theoretical basis of the cooperation between the NBSZ and the Authority is laid down in the Fundamental Law with the obligation to respect and protect fundamental rights. The specialized knowledge requires joint work.

Transparency: For the effectiveness of the audit, NBSZ should allow access to their special, secret know-how therefore, activities carried out by the Authority during the audit has to be fully transparent for the NBSZ. All activities and experiences of the audit have to be carefully documented by both sides.

Data protection, protection of classified data:

- During the data protection audit, the Authority cannot use single data of the operating activities because this is not allowed according to the Privacy Act or the Nbtv.
- For the aim of inspection of tools and methods of secret information gathering personal data can only be used on prior authorization of the affected person.
- During the audit no access can be provided for the Authority to such data, which cannot be processed according to Section 71 of Privacy Act, or which is not necessary for the purpose of the audit.
- Specific security, privacy and information protection rules have to be clarified and documented in advance. The parties should ensure that staff are familiar with these rules.

The essence of the developed audit method is that an experimental situation is created by the Authority in which the NBSZ has to carry out its secret information gathering service in a very realistic manner.

The testing covered every tool and method of secret information gathering in connection with personal data as set out in Section 56 of Nbtv., regardless whether external authorization is required or not. The test was designed to create situations where the NBSZ has to make a decision with relevance to data protection.

We also created situations which although may occur only rarely in the real-world, but would be relevant for the control of the fulfilment of an essential privacy requirement. However, the aim was not to create completely far-fetched situations.

Certain elements of the standards of data protection (such as the principle of purpose limitation, of data minimisation, data quality etc.) were also investigated in different aspects (e.g. at various working phases, on possible automatic use of a given method, the scale of the use of a given tool, the relationship between data controller-data processor, clear legal positioning of the tools and methods within the portfolio of the Nbtv. etc.)

The preparation for the implementation of the tests required careful organization from both sides. The test plans could be learned only by designated contact points at the NBSZ in strict confidence. We took the chance to plan on a rolling basis, during the control of the given secret information gathering sector, the preparation of the tests aiming a different sector was already ongoing.

In general, the Authority provided tools, equipment, materials used in test situations. Our colleagues played the targeted persons, as well as other persons in connection with secret information gathering (including fictional Civil Intelligence Service officers).

NBSZ provided the special technical tools for secret information gathering, which were used by its staff during the tests. NBSZ staff involved in the tests were informed only that a data protection audit is in progress but no additional information was provided.

Preliminary briefing, confidentiality and privacy declarations and consents as well as the development of special technical environment adapted to the specific features of the given method being tested had to be achieved. For example, during the data protection audit of phone tapping we created an electronic communications test environment completely separated from the Authority's IT system in order to protect the privacy rights of other clients of the Authority.

The location of the tests were jointly selected by the NBSZ and the Authority. In some cases, test environments were designed in NBSZ objects, while in other cases, in the building of the Authority or in a hotel located in Budapest. The external test environments were chosen so as to ensure that third parties data won't be recorded.

The Authority examined the entire process as the secret information gathering realised by the NBSZ would happen in real life.

Each test started with the submission of a documentation to the NBSZ containing fictive facts. The documentation was sent in the name of a non-existent Civilian Intelligence Service through the Authority. The documentation contained the fictive authorization on secret information gathering subject to external authorization. During the preparation and implementation of tests, the NBSZ acted according to Article 8 (1) of Nbtv.

The implementation of the tests was recorded by the NBSZ in a protocol.

In the period between April 2016 and February 2017, 34 secret information gathering tests were implemented. The evaluation of the tests will happen in 2017, therefore we provide information – to the extent of relevant legislations and secrecy regulations – regarding this subject in the next year's report. However, it can already be stated that the practical approach of testing has been justified by the results.

VII.2. The experiences of administrative proceedings for the control of classified data

In 2016 the data protection audit of NBSZ has largely preoccupied the Authority's capacity. However, similar number of notifications regarding classified information was received as in the previous years, which were both data protection and freedom of information related. Most of the submissions have been dealt with by starting an investigation as the legal conditions of starting an administrative proceedings for the control of classified data were not met. (According to Section 62 (1) of Privacy Act, if the investigation of the Authority suggests that the classification of certain national security information is unlawful, the Authority may open administrative proceedings for the control of classified data.)

Based on the experiences of 2016 it can be assumed that approximately 6-7 administrative proceedings for the control of classified data will be initiated by the court in the future yearly, based on Section 31 (6a) of Privacy Act.

The case of the classification of the contract of entrusting a lawyer signed in connection with the repatriation of the so-called *Seuso Treasure*[64] was closed in

64 A treasure of great silver objects from the Roman Empire with an adventurous history, 7 items finally bought by Hungary in 2014.

2016. The Authority has contacted the classifier to provide the detailed reasons and copy of the documentations. The classifier has reviewed and abolished the classification of the documents, which have been disclosed since then, therefore the Authority has closed the administrative proceeding.

Other cases from 2016:

In another case, the classifier has decided on the classification of data after years of the creation of the data. In this regard, the Authority pointed out that if the requirements set out in the Act are met, the data classification has to be implemented right after the data procession without any delay, otherwise it may result in breaches of access to public information, and would also undermine the legal certainty as part of the democratic rule of law. This opinion is also in line with the provisions of Section 6 (1) of Act CLV of 2009 on Protection of Classified Information (hereinafter referred to as: Mavtv.)

It should also be noted that there are other negative consequences of the postponement of the classification regarding the access to the data before the actual start of the classification procedure. If the information was accessed by unauthorized person, then subsequently it is very hard to prove, what time did the person have access to the information: between the creation and the classification of the data, or after the classification, when the data was already classified and the strict access administrative rules for access already applied.

The abuse of classified information can be committed only after the initiation of the classification process, so in terms of legal certainty, the procedure which allows subsequently classified data to be processed together with non-classified data for a longer period of time is completely unacceptable.

In another case, the petitioner complained that the Constitution Protection Office denied to provide information on his own data – with no national security risk factors – which was collected during the national security inspection of the individual concerned. The authority started an investigation and reviewed the documentation and the internal control standards at the Constitution Protection Office. After the investigation, the Authority noted that the director-general of the Constitution Protection Office has restricted the affected person's right to information in accordance with Section 19 of Privacy Act and Section 48 of Nbtv. The reason of the restriction was that making the national security-related documentation available would help to reconstruct the procedure and content of the national security inspection. Keeping these procedures as secret is an essential

national security interest, as if these procedures would go public, it would harm the efficiency of national security inspection, therefore restricting the affected person's right to information is legal in cases even where the inspection did not find any national security risks at all.

In this case the Authority also investigated the legality of the data processing – performed by the National Security Office, as predecessor of the Constitution Protection Office – regarding the national security inspection.. The Authority noted that inspection's aim was to find out whether there is a national security risk or not in connection with the inspected person. The depth of the data collection was in accordance with the position filled by the affected person, which could be characterised as *"important and confidential"*. No unnecessary and unlawful data collection operation was identifiable. A summary report was made at the end with the conclusions of the inspection upon which a security expert opinion was issued. Between the security inspection and the Authority's investigation, part of the documentary material was scrapped, but it was carried out according to the internal rules of Constitution Protection Office.

VII.3. Opinions on bilateral confidentiality agreements

According to Mavtv., there is a difference between national classified information and foreign classified information. National classified information is data that was created by a body performing state or local government responsibilities. By contrast, foreign classified information is data created and classified by all institutions and bodies of the European Union, by Member States acting on behalf of the European Union, or by a foreign party or international organizations. The differentiation is important because national classified information limits the right to access to data of public interest, while strictly speaking, foreign classified information shall not be the subject of right to access to data of public interest. NAIH's powers cover only national classified information. Taking over foreign classified information by a Hungarian body does not constitute authority for NAIH, the information will remain in the authorization of the foreign classifier and the national body has the task to protect the information. This obligation arises from international conventions.

In light of the above, it is important that confidentiality agreements make a clear separation between national and foreign classified information and regulatory powers related to them.

It is problematic that from 2016, such bilateral international confidentiality agreements were prepared that provide common consensual regulatory powers for the parties regarding classified data created during their cooperation.

The Authority's view is that in the cooperation of the parties the bodies of both parties are involved. These bodies create classified information according to the rules of their own State. Indeed, bilateral cooperation between States will not wash away the boundaries of jurisdiction between States and does not create an independent institutional and legal order. The vast majority of bilateral international confidentiality agreements are based on the principle that State parties deal with the information they provide during the collaboration themselves. This is in line with the principle of state sovereignty and the general principles of international relations.

Speaking of data generated during the cooperation of the parties, the supervision and termination of the classification depending on the mutual agreement of the parties is disadvantageous for the disclosure of data of public interest. This is because the foreign party can prevent a supervision and termination of the classification at the time when it would be mandatory under Hungarian law. The substantive legal conditions of the termination of classification should also be determined, because preventing the possibility that one of the parties based on political considerations or other, non-legal reasons could prevent the declassification of information in the other party's State as well.

The rule at issue is not in line with the rules of Mavtv., as it does not allow the division of the power of classification between foreign State bodies and foreign institutions.

VII.4. Professional consultation with the National Security Authority

In Hungary, two bodies have power on classified data processing. According to the Privacy Act, the Authority conducts *ex officio* administrative proceedings for the control of classified data in order to fulfil its responsibilities, that is, to supervise and promote the enforcement of the rights to the protection of personal data and access to public information and information of public interest. The other organization is the National Security Authority (hereinafter referred to as: NBF), which is – according to Section 20 (1) of Mavtv. – responsible for the

official supervision of protecting classified information, the official authorization and supervision of processing classified information, as well as on-site industrial security official duties.

To make a clear distinguish between the two organizations, Section 62 (1b) of Privacy Act lays down that administrative proceedings for the control of secrets conducted by the Authority shall not concern the tasks conferred upon the NBF by the Act on the Protection of Classified Information. On the other hand, Section 20 (2) point r) of Mavtv. says that the NBF cooperates with NAIH in order to secure the fundamental right to access data of public interest and freedom of information. Under these rules, the powers and duties of both organizations are clearly distinguishable, however, the regulation creates the legal conditions for technical cooperation as well. For reasons of legal certainty, the experts of the two organizations hold discussions from time to time. During these meetings, the legal requirements for the qualification and the processing of classified information reconsidered.

An important topic of discussion was about the legal position of experts involved in the supervision of classification in 2016. According to Section 4 (3) of Mavtv. certain officials may assign their power of supervision of classification to experts involved in the supervision process according to the internal ruling. Both parties agreed that this assignment must comply with strict rules (written form is required and the scope and date must be precisely determined). However, the qualifier does not lose his power of supervision with the assignment and is entitled to terminate the assignment at any time.

Section 8 (1) also allows the involvement of an expert to help the work of any qualifier (not only those in certain positions as according to Section 4 (3)) but without empowering the expert of any decision making and no reference is required to the internal ruling.

Another important issue was about the extension of qualification which is possible within a repeated qualification process according to Section 5 (7) of Mavtv. The maximum term of extension shall be considered from the date of the decision on the extension of qualification.

VIII. NAIH's international cooperation

VIII.1. International engagements

According to Section 38 (4) point e) of Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information, NAIH shall collaborate with the bodies and persons defined in specific other legislation to represent Hungary in the joint data protection supervisory bodies of the European Union. The stakeholders of international relations and European data protection include national data protection authorities, the European Data Protection Supervisor and the Council of Europe cooperating with NAIH on a daily basis.

VIII.2. Budapest Spring Conference

The Budapest Spring Conference (http://www.naih.hu/budapest-springconf/) was already mentioned in the introduction, as an outstanding international event of 2016. Every year since 1991, European data protection authorities gather to discuss common professional issues. The members of the conference gain recruit by formal accreditation, the beginning of the event is open for the press, but after this the conference is private, only registered members and guest speakers, and the experts of the host organization can participate. After 2006, on 26-27 May 2016 NAIH hosted more than 100 registered participants in Budapest. The two main topics of the Budapest Spring Conference were strengthening international cooperation and also the control of national security services within the constitutional framework.

The new EU data protection provisions will fundamentally alter the rules of personal data protection. The GDPR is directly applicable in all Member States and national data protection authorities will carry out their activities with an inevitably closer cooperation. The authorities are preparing for this role, and in order to create the necessary resources, they are negotiating with the national bodies responsible for the budget.

The declaration adopted in data transfers to foreign countries reinforces the ambition of the European Union and the Council of Europe to provide the same level of data protection for European citizens even when their data is transmitted to

other continents. Transferring data to foreign countries cannot provide a loophole for pulling down a European standard of protection.

VIII.3. International projects

VIII.3.1. Arcades-project

In 2016, the ARCADES „introducing dAta pRoteCtion AnD privacy issuEs at schoolS in the European Union" project has been successfully completed. Teaching aids, data protection handbooks for school teachers can be freely downloaded on NAIH's website: http://naih.hu/arcades/dokumentumok.html. The recordings of the best data protection lessons are also accessible on: http://naih.hu/arcades/videok.html. The project's final motif and also the main prize of the privacy award was the participation at the closing ceremony in March 2016, the Barcelona Conference, where all participating countries presented their own results.

VIII.3.2. Macedonian project

Within the tender called „*Support to access to right on protection of personal data in Macedonia (EuropeAid/135668/IH/SER/MK)"* with NAIH as consortium partner and financed by EUROPAID, the first study visits in the Republic of Macedonia took place in 2016.

The three topics for the NAIH experts were:

- international cooperation in data protection,
- harmonisation of the two informational laws and
- data protection issues of the courts, prosecution and the ombudsman's data processing.

The project will also continue in 2017.

VIII.3.3.Participation in the Schengen evaluation of Malta

The implementation of data protection requirements during an inspection visit regarding Schengen acquis took place in September 2016, in which a NAIH

expert has also been involved. The 10-member delegation of different Member States and experts from the European Commission was responsible for the inspection, while a representative from the European Data Protection Supervisor was present as an observer. The inspection reviewed the practice of the relevant legislation and its application by local authorities. The experts made on-site visits to the Maltese Data Protection Authority, the Ministry of Foreign Affairs, the N.SIS Authority, the SIRENE Bureau and the Malta Information Technology Agency (responsible for the operation of the Maltese public administration IT systems). The report will be discussed in detail in the Council's Committee of Schengen and the final report will be adopted by the Justice and Home Affairs Council.

VIII.4. Citizens' requests relating to the Schengen Information System (SIS)

The Schengen Information System (SIS) is a highly efficient large-scale information system that supports external border control and law enforcement cooperation in the Schengen States. The SIS has strict requirements on data quality and data protection. The basic principle is that the state that entered the alert is responsible for its content. The national Data Protection Authorities supervise the application of the data protection rules in their own countries, while the European Data Protection Supervisor monitors the application of the data protection rules for the central system managed by eu-LISA. Both levels cooperate to ensure coordinated end-to-end supervision. If anyone would like to be informed whether his or her data is recorded in the SIS or requests the erasure or rectification of the recorded personal data, an application can be submitted by filling in the specified form to any government office, police station or to the Hungarian Consulate. The claims are being evaluated by SIRENE, an organizational unit of the International Criminal Co-operation Centre (NEBEK) which can also refuse to grant the requested information where appropriate, but must inform the applicant of this fact and the legal basis of the refusal. Against the SIRENE Bureau's decision, a claim can be submitted to NAIH which will review the decision.

In 2016 NAIH received 16 requests in this matter, of which four were Hungarian citizens, while the others were foreign citizens. In terms of the regional distribution we received submissions from the Middle- and Far East, from African and South American countries and from the Western Balkans and some regions of Ukraine. The Authority launched investigation in a total of 5 times, while in the

other cases it provided general information to the submitters on the right to turn to the National SIRENE Bureau.

In the two examination procedures, NAIH found that the applicant is recorded in the SIS because of crossing the Hungarian-Serbian border illegally, and the alert was placed and the data was processed in accordance with the legal requirements.

In two other cases Hungarian citizens purchasing vehicles in good faith were faced with the fact that their purchased vehicle was recorded in the SIS system as a wanted vehicle. The investigation revealed that in both cases the alerts should have been deleted from the system – this took place at a later date.

VIII.5. Participation in the EU data protection network

VIII.5.1. SIS II CSG (SIS II Coordinated Supervision Group)

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

In connection with the module containing SIS “alerts”, the working group has developed an audit framework based on different questionnaires, which help the national authorities to inspect the authorities responsible for operating SIS upon a uniform methodology.

The working group discussed a problem raised by a national legal practice. SIS data is being checked at several public administration procedures in Poland, also when licensing firearms. In this subject, the apparent legal basis is the national law governing the issuance of firearm licenses, which says, that that it should be checked that the claimant is not dangerous to the country’s national security. The law however does not explicitly mention SIS. The working group considers that the Polish legal practice is contrary to EU law, as according to the basis of the SIS II Regulation and Decision the system can be used only for law enforcement purposes. It has been checked whether any possible limitations of the national budget in Member States have any impact on data protection inspections in connection with the enforcement of Schengen acquis. Generally speaking, the national authorities

have not received additional resources related to the Schengen supervision – in this respect a joint statement is being drawn up addressed to national parliaments.

The European Commission's representative reported about the latest developments related to SIS II. The AFIS (Automated Fingerprint Identification System) implementation is going well, the eu-LISA agency responsible for operating the main system has started the preparation of technical conditions.

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

As a safeguard, the Europol Council Decision, which set up both Europol and JSB, contains a number of provisions relating to personal data protection. The main task of the JSB is to ensure that Europol complies with these data protection provisions. Important change of the near future is that from 1 May 2017, with the entry into force of the new Europol Regulation, the Europol Cooperation Board (ECB) will take over the tasks of the JSB Europol. The new body's administrative and secretarial duties will be carried out by the European Data Protection Supervisor (EDPS), which will have a permanent representative present at the meetings. It was suggested that within the ECB a standing committee should be created with a chairman, the EDPS representative and some candidates from Member States.

The JSB Europol discussed the findings of the privacy assessment of Europol, emphasizing that the quality of data processed by Europol – due to the volume of billions of data – in many cases did not hit the expected level, often poor quality data is being transmitted to the Member States. The volume has an effect on the efficient functioning of the system, since the data is stored for a long time. The JSB Europol recommended internal training to its staff in order to improve data quality.

Lastly, the "Europol data leak case" should be mentioned which happened in 2009 but was reported only in December 2016. A Europol employee copied Europol data to a USB-stick. The data was intended to be used for a presentation. Then, in the employee's home, the data was copied to a cloud-based hosting service. Since the service was not password-protected, everybody had access to the information over the Internet. The incident was spotted by a journalist as well. In connection with the case, the Europol declared that the concerned data had no operational risk because they are already quite old (data about the murder of film director Theo van Gogh in the Netherlands back in 2004 and about Dutch Islamists linked to the felony). The JSB emphasized that allegedly not only human negligence lead to the incident as at the given time Europol had no ad-

equate internal safety regulations, it was only created later in 2010. Moreover (in the context of a Dutch television documentary) JSB has just learned about this incident recently. A likely reason for this is that according to a Europol decision, Europol is not obliged to report data incident to JSB.

VIII.5.3. JSA Customs (Customs Information System Joint Supervisory Authority) and CIS CSG (The Customs Information System Coordinated Supervision Group)

CIS is an information system which centralizes all customs information, with the aim of a more efficient detecting and prosecuting of violations of customs and agricultural matters. With the CIS national customs administrations can exchange information and spread information about illegal trafficking and intervention requests. The Joint Supervisory Authority is competent to supervise operation of the CIS. From 1th May 2017 JSA Customs will be dissolved and CIS SCG (containing members of the EDPS and national data protection authorities) will take over its activities.

VIII.5.4. Eurodac CSG (Eurodac Coordinated Supervision Group)

Eurodac is a large database containing the fingerprints of applicants for asylum and of illegal immigrants found within the EU. Eurodac SCG is responsible for coordinating supervisory activities and common inspections, ensuring conformity with the data protection rules in the Eurodac Regulation and issuing recommendations for member states and the central unit.

The recent migration crisis conceived the need to establish a new system which can operate in crisis situations as well. In 2016 the European Commission put together a package of proposals to amend the Common European Asylum System and to reform the Eurodac system:

- Data relating to persons found illegally staying in a Member State would be stored as well. (Currently this data can only be compared with the data of asylum applicants stored in the system.)
- Beside of the fingerprints facial image as additional biometric identifier would be recorded and stored (long-term goal is the introduction of a facial recognition software), and the refusal of providing facial image or fingerprints would be sanctioned.

- Beside of the fingerprints personal data of the data subject such as the name(s), age, date of birth, nationality, other identity data and identity documents) would be stored in the system, and these data would be accessible in case of positive fingerprint or facial image result ("hit").
- The age for taking fingerprints would be lowered from 14 to 6 years of age in order to identify unaccompanied minors and finding the families of children as soon as possible.
- The data retention period of asylum applicants remains the same at 10 years, but fingerprint data for illegally staying third-country nationals who do not claim asylum would be retained for 5 years (similar to the data retention period of the Visa Information System and the proposed data retention period for storing data in the to-be-established Entry/Exit System). Data would no longer be deleted for subjects who were granted a residence document by a Member State (in this case their data will be marked, so it may than be possible to pass back the person concerned to the Member State that issued the residence document) or left the territory of the Member States.
- Marked data of subjects who were granted international protection would be accessible for law enforcement purposes for a period of three years (there is no change), but this time limit would not be applicable in case of illegally staying persons who were granted a residence document by a Member State. For return purposes, the proposal amends the rules on sharing data with third countries, but it does not grant direct access for these third countries.

The reform of the Common European Asylum System is in progress, developments are expected in 2017 in this regard. The Working Group has indicated that as the EU plans to set up practically an entirely new database, it would be important to conduct a preliminary privacy impact assessment. With regard to the supervision of Eurodac system by Member States, an investigation plan has been created, which national authorities can use as a guide for the national checks.

VIII.5.5. The Visa Information System Supervision Coordination Group (VIS SCG)

The Visa Information System (VIS) is the European Union's central information system for issuing short-term visas (also called Schengen visas) and for combating "visa shopping". VIS SCG is a forum for the collaboration of data

protection authorities responsible for supervision of the VIS consisting of one representative of each Member State's DPA and of the EDPS.

According to the European Commission representative's information, the shortcomings of Schengen Evaluations done by Member States revealed that in general, most data protection authorities do not use IT experts, and the absence of appropriate procedures in regard of complaints and right of access is also an issue.

The question on applicable law on Member States' missions located in non-EU countries arises when an embassy in the State outsources data processing jobs for a company located in a non-EU country. The common position will be discussed in early 2017.

VIII.5.6. Border, Travel and Law Enforcement (BTLE) Subgroup of Art. 29 WP

The subgroup concentrated on the possible effects of Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA in 2016.

The most important change is that the scope of the Directive will be wider (Article 2), as it covers non-state data processing by companies for but law enforcement purposes. This new approach (Article 4-7) brings new data protection principles, outlining the special obligations imposed on data controllers manifested in time limits for data storage and review, the distinction between different categories of data subjects and the distinction between monitoring the quality of personal data and the categories of personal data. Ensuring the legality of data management plays an important role as well (principle of purpose, automated decision making processes). More detailed rules were adopted in respect of data subjects' rights (Chapter III). Chapter IV of the Directive provides new kind of obligations similar to the Regulation (privacy by default, privacy by design, privacy impact assessments, preliminary consultation with data protection authorities.)

As an independent EU body, the Supervisory Board, which is responsible for implementing the Directive will have more power in connection with the various

national data processing aspects and is expected to carry out a more effective control than the existing coordinating bodies. With few exceptions, in most Member States data protection authorities have no direct control over the drafting and the implementation of the legislation, it is the task of the ministry competent in this matter.

In addition to the above, the subgroup also discussed the EU-USA "Privacy Shield" agreement, as legal basis for international data transfers. It still does not clearly define how the affected party can assert its rights, whether the complainant can turn directly to the EDPB or should contact first the national authority. It is also necessary to introduce a single complaint handling form by all Member States, and finally a secured communication channel is needed.

The subgroup also deals with the EU-USA "Umbrella Agreement" which is the only international treaty where the USA provides similar rights for non-American citizens as for Americans. The protection only applies to EU citizens, but it will represent an unprecedented level of cooperation among the Atlantic criminal cooperation. The American part of legislation is considered as complete. Joint audits will be required to check the compliance with the treaty.

VIII.5.7. International Data Transfers Subgroup (ITS) of Art. 29 WP

The supervision of transferring data to the USA was a priority issue in 2016.

At the ad-hoc Safe Harbour-working group meetings experts – representing the Hungarian, the Hessen, the Hamburg, the federal German, the Spanish and the French data protection authorities – have been discussing the on-going cases after the Court of Justice declared in the so-called Schrems judgement that the Commission's US Safe Harbour Decision as invalid where data controllers or data processors are still relying on the Safe Harbour plea.

In close cooperation with the BTLE subgroup the ITS reviewed from the perspective of conditionality and legal remedies the draft decision relating to the "Privacy Shield" convention in a "commercial" aspect, i.e. data transfer to US-based organisations from the EU. The WP29's opinion[65] on the Privacy Shield draft decision was disclosed on 13th April 2016, in which the Working Party welcomes

65 WP 238 in.: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendati/files/2016/wp238_en.pdf

the progress made in relation to the previous framework (Safe Harbor) but also proposes some amendments e.g. relating to principles or to judicial remedies.

The 2016/1250 implementing decision by the EU Commission on the adequacy of data protection provided by the EU-US Privacy Shield was adopted on 12th July 2016. The ITS hold consultations about the procedural order of the future legal remedy forum called "EU Informal Panel" consisted of the EU national data protection supervisory authorities.

For the more effective assistance the ITS has also developed a standard form in relation with the Privacy Shield-complaints handling by the national DPAs.

The subgroup experts also paid great attention to questions of BCR. Collaborative processes have been carried out in many cases according to the WP 107 Working Document and in the light of the GDPR the review of related Working Documents (WP 74, WP 107, WP 108, WP 153, WP 154, WP 155) has begun. The updated documents will be available in 2017.

VIII.5.8. The Technology Subgroup (TS) of Art. 29 WP

In relation to the GDPR, the subgroup was responsible for preparing several important new draft opinions (practical realization of the right of data portability, data protection impact assessment). It has also started working on opinions related to the incident report and data protection certification scheme. The subgroup has been selected for reviewing the ePrivacy Directive and for giving opinion on the new ePrivacy Draft Regulation.

The TS has also analysed the data protection risks of several new technologies e.g. connected cars or Smart Cities conception or user tracking devices based on Wi-Fi and Bluetooth communication channels (location tracking). Certain risks have been identified such as lack of transparency of data processing, high extent of identification of data subjects, vulnerability of privacy, problems related to profiling, to data request for criminal purposes or to defining the data controller. However, privacy-friendly technologies already exist e.g. in Norway a separate application shall be installed to the smart device which communicates the Bluetooth beacon using Bluetooth Low Energy (beacons aren't about sending location coordinates but about self-identifying.)

TS has reviewed the previous WP29 opinions of controlling employees and has also started preparing a draft opinion on the data protection risks of controlling employees with the help of modern technology. New challenges include the widespread use of cheap devices for employees monitoring, the “bring your own device” concept, new methods of telemetry (automated communications process by which measurements and other data are collected at remote or inaccessible points and transmitted to receiving equipment for monitoring) and of analytics.

The analysis of large IT companies (Google, Facebook, and Microsoft) practices and innovations has been on the agenda. The Belgian DPA’s procedure against Facebook ended with a court judgment stating that the ‘Datron’ cookie used by Facebook is against the law. The cookie follows data subjects who have not logged in to Facebook, but visit a website with a Facebook social plugin API for example via “like button” or a public Facebook page. The cookie gets on the user’s machine and will follow its browsing habits and positions. The data security objective cited by Facebook might be real but does not comply with the principle of proportionality or the requirement of providing adequate information, and the Belgian court did not accept such broad data processing purpose for remote safety aspects only.

VIII.5.9. The Cooperation Subgroup (CS) of Art. 29 WP

GDPR tightens the administrative cooperation between DPAs of Member States much closer and sets out the related procedures as well. The most important task of the subgroup in 2016 was to develop guidelines for national authorities to implement these new procedures. The four main topics are: the so-called ‘one-stop shop’ procedure for cross-border data transfers, the cooperation of DPAs within the framework of ‘mutual assistance’, several ‘joint operations’ by the authorities, as well as the common European system of the imposition of administrative fines. In the first three topics, the subgroup has already adopted working documents, which will be tested by the national authorities in 2017 and, if necessary, guidelines will be revised for the staff of these authorities. This is to ensure a same level of data protection and to create legal certainty for data controllers. In Hungary, the maximum financial penalty to be imposed is currently 20 million HUF (around €65,000) which will rise up to €20,000,000. The development of the uniform system will continue in 2017.

VIII.5.10. International Working Group on Data Protection in Telecommunications

The so-called “Berlin Group” has since 1983 adopted numerous recommendations aimed at improving the protection of privacy in telecommunications and Internet services. In 2016 the Working Paper on Biometrics in Online Authentication and the Working Paper to Update on Privacy and Security Issues in Internet Telephony and Related Communication Technologies were adopted.

It also discussed a new draft opinion about the personal data to be processed by e-learning platforms with such data protection risks as of collection of personal data not related to the studies or involving sensitive data (learning disability, political opinion etc.) as well.

More and more private companies offer free educational platforms for children for further use of personal data and for direct marketing purposes in return. The private operators with blurred accountability mostly use cloud-based IT services, in which the transmission and procession of personal data becomes non-transparent.

Privacy risks of topics related to smart televisions and to the conception of “connected cars” were also under discussion.

VIII.5.11. Police Cooperation Convention for Southeast Europe – PCC SEE

On 5 May 2006 the Convention was signed by seven countries: Albania, Bosnia and Herzegovina, Macedonia, Moldova, II, Romania, Serbia. Hungary joined the Convention on 11 December 2012 (according to Act XCII of 2012 on the Police Cooperation Convention for Southeast Europe). The aim is that the law enforcement authorities of the contracting parties render mutual assistance in the framework of their respective jurisdiction to take measures against threats to public order and/or security, to prevent, detect and investigate criminal offences, unless such a request or the execution of it, can only be dealt with by the judicial authorities under the law of the respective contracting party. The Committee of Ministers as the main decision-making body implementing the Convention created a data protection working group, which is responsible for drawing up the provisions of the data protection and the mutual evaluation process. Each contracting party appoints two members of this working group, an expert of the national DPA and a member of a law enforcement agency.

The last meeting noted that the implementation of Article 31 of the Convention guaranteeing the adoption of the necessary national provisions in order to achieve a level of protection of personal data was successfully completed by each party, so the Convention could be the legal basis for the exchange of personal data, however, given the fact that several non-EU Member States are involved as well, a more detailed, appropriate legal structure for data protection guarantees should be developed in the near future.

VIII.5.12. TFTP (Terrorist Finance Tracking Program)

The TFTP Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program was signed on 28 June, 2010. Its aim is to safeguard data protection rights relating to transparency, rights of access, rectification and erasure of inaccurate data. It guarantees non-discriminatory rights of administrative redress and ensures that any person whose data are processed under the Agreement will have the right to seek in the U.S. judicial redress for any adverse administrative action. The Agreement further acknowledges the principle of proportionality as a guiding principle for its application. Under the Agreement, Europol assesses whether the data requested in any given case are necessary for the fight against terrorism and its financing. Europol also verifies that each request is tailored as narrowly as possible to minimise the amount of data requested. If a request for data does not meet these conditions, no data can be transferred under the Agreement.

The report on the fourth review of the Agreement was conducted in March 2016 with the active participation of a NAIH expert. The report was adopted on 19 January 2017:
https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/crisis-and-terrorism/19012017_tftp_report_en.pdf

VIII.5.13. Passenger Name Record (PNR)

PNR data is information provided by passengers and collected by air carriers during reservation and check-in procedures. Non-carrier economic operators, such as travel agencies and tour operators, sell package tours making use of charter flights for which they also collect and process PNR data from their cus-

tomers. For flights from and to the EU, up to 60 individual pieces of data on passengers are collected and stored for five years. These include registration data,. travel itinerary, ticket information, contact details, seat and flight numbers, along with food preferences, baggage information, credit card details or IP addresses. EU-level measures such as the directive on Advance Passenger Information (API), the Schengen Information System (SIS) and the second-generation Schengen Information System (SIS II) do not enable law enforcement authorities to identify "unknown" suspects in the way that an analysis of PNR data does. Flights from third countries arriving or leaving a Member State, including transits, must submit PNR data to the PIU (Passenger Information Unit-PIU) which will analyse the data and, where relevant, inform the authority in the specific Member State.

Directive (EU) 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime came into force at the end of May 2016, and obliges airlines to hand national authorities passengers' data for all flights from third countries to the EU and vice versa. The Directive leaves no time for preparation for Member States. Currently, with three exceptions (United Kingdom, Romania and Hungary), most Member States still have not transposed the Directive into national law yet.

In Hungary, Act XXXV of 2015 created the Counter-terrorism Information and Criminal Analysis Centre (TIBEK) which carries out the tasks of the national PIU. In order to allow cross-border processing, the formats of the PNR and API data must be compatible and be supported by the systems of the national PIUs. In this context, Hungary was leading an EU project entitled "Pilot Programme for Data Exchange of the Passenger Information Units" (PNRDEP) in 2016 with Bulgaria, Lithuania, Portugal, Romania, Spain and the Europol involved.

VIII.6. Participation in the work of the Council of Europe

– The on-going reform of the Convention 108

The Convention opened for signature on 28 January 1981 was the first legally binding international instrument in the data protection field. Under Convention 108, the parties are required to take the necessary steps in their domestic legislation to apply the principles it lays down in order to ensure respect in their territory for the fundamental human rights of all individuals with regard to processing of personal data.

The Consultative Committee (T-PD) consists of representatives of Parties to the Convention complemented by observers from other States (members or non-members) and international organisations, and is responsible for interpreting the provisions and for improving the implementation of the Convention. In 2016 two delegations expressed significant reservations concerning modifications, so there was no chance approving the text in 2016. Discussions continues on expert level.

– The Committee of Experts on Terrorism (CODEXTER)

The Committee follows the implementation of the Council of Europe legal instruments against terrorism and coordinates the Council of Europe activities in combating terrorism.

During 2016, the Committee created the Special Investigation Techniques (SIT) subcommittee. The SIT's task is to review the recommendation of the Council of Europe, the Rec (2005) 10 on the use of special investigation techniques in the fight against terrorism and serious crime. Extending the scope of the Recommendation on financial investigative techniques is also under discussion.

VIII.7. Reviewing draft legislations with international dimensions

Upon the request of the legislature draft legislations with international dimensions have also been reviewed by NAIH.

According to the bill of the Treaty between Hungary and the Kingdom of Thailand on Extradition, the processing of personal data necessary for the application of the Convention is being realized under the law of the Contracting Parties who may impose additional conditions for the processing of data transferred. NAIH drew attention to the fact that a law enforcement agency shall not define data processing and data protection provisions with discretional power.

Regarding the bill on the publication of the Treaty on Extradition between Hungary and the Socialist Republic of Vietnam and the bill on the publication of the Treaty on the Transfer of Sentenced Persons between Hungary and The Socialist Republic of Vietnam, transfer of personal data is possible under the conditions of the Privacy Act and Directive 95/46/EC. The bill does not contain specific provisions for the protection of personal data, the Parties refer to the data protection provisions of the Convention on Mutual Legal Assistance be-

tween Hungary and the Vietnam Socialist Republic, which has not yet been announced. In NAIH's consideration legal aid can only be requested in the context of specific criminal proceedings and only in connection with person in connection with person subject to such proceedings therefore certain privacy guarantees should be incorporated in the Treaty itself. NAIH drew the attention of the legislature that according to Hungary's EU obligation, when transferring data to third countries, the level of protection afforded by Directive 95/46/EC has to be guaranteed

VIII.8. Matters related to Bitcoin technology

On the request, in two cases, NAIH has issued opinions about the Bitcoin system. Bitcoin is a digital currency that can be freely used by anyone, but which exists only virtually, as it is full of bits and bytes. Physical incarnation does not happen, actual coins or banknotes are not available. Unlike traditional financial institutions that protect customers' private information by withholding information about bank transfers, Bitcoin system ensure privacy in a way that information on the owners of the addresses are not known at all. When a user begins to use Bitcoin software for sending and receiving virtual coins, the software does not ask for any information regarding personal data and the user is not obliged to register on the network either.

In the first case a US attorney's office requested a review on the effect of new technology on the protection of privacy. We can say that specific legislative acts regarding this technology still do not exist in Hungary yet, but this shall not prevent any person or business to use the system freely for own purposes. However creating suitable legal framework regarding this technology would significantly contribute to prevent abuses in the future.

The second request came from a Hungarian district court for advisory opinions in connection with a pending criminal procedure on a suspected fraud committed with Bitcoin. The question raised at the criminal proceeding was whether the given amount of Bitcoins had market value and if the answer is yes, could it be accurately determined at a given time. NAIH's answer was a definite yes.

VIII.9. Drones

Pilotless aircrafts (Unmanned Aircraft System or Remotely Piloted Aircraft System), commonly referred to as drones raise more and more concerns about privacy.[66] Since the 1990s, European data protection authorities have been dealing with the impact of drones on private sector. These items – especially since they have become almost fashion items – violate our privacy even more severe than closed-circuit cameras. The observations made by them can be imperceptible, intrusive, also the device itself is available for almost everybody. NAIH issued a recommendation[67] on Drones in 2014, which explores the atypical processing of data with accessories fitted on vehicles, the data protection aspects of the civil use of these items.

Drones are increasingly being used for civil and commercial purposes in various sectors, but the regulatory framework remains uncoordinated. Basic national safety rules (already in effect or under preparation) apply to them but these vary all across the EU. A number of key precautions are not coherently regulated, therefore it is foreseen that in 2019 the national regulations (if any, in force in the Member State) will be replaced by a single EU Regulation. The draft is being prepared by the European Aviation Safety Agency (EASA). Based upon a risk assessment EASA created three categories of drones in 2015: open category (low-risk), specific category (medium risk), and certified category (high risk) with different licensing, inspection and registration rules. NAIH actively participates in the development of the privacy aspects of the draft regulation at various international workshops.

In 2016, the development of domestic legislation on drones has also begun. Pursuant to the relevant law, the concept of the drone has been established *saying "unmanned aircraft: a civil aircraft, designed and maintained in a way that its control is not carried out by a person on board"*[68]. The draft legislation prepared by the National Transport Authority is going to regulate drones over 0.25 kg weight and contains multiple data protection solutions recommended by NAIH. Commercial and private use is separated, and similar to the EU draft regulation, the national draft legislation sets up three different categories based on risk assessment and also deals with liability insurance. Currently, only oc-

66 International Working Group on Data Protection in Telecommunications 675.47.25., Data protection in case of aerial surveillance, Working document, seat 54, 2-3 September 2013

67 https://www.naih.hu/files/ajanlas_dronok_vegleges_www1.pdf

68 Act CXXXVI of 2016, Section 18 (2)

casional or limited use of airspace is allowed for drones, only as an officially approved activity, up to 150 meters of height and weight limit of 25 kilograms. The Aviation Authority provides the requested coordinates where other aircrafts cannot appear during that time.

NAIH's view is that the future legislation should strictly consider the principle of purpose limitation and the scope of data processing shall be limited on terms of time, geography and person as conducted by the aviation authority at an authorization procedure. Data processing with drones of private use cannot be extracted from the data protection guarantees, the recreational and hobby usage of drone cannot rely on the "Household exemption" of data processing but[69] the judgment of the Court of Justice of the European Union in the *Ryneš v Úřad* case should apply by analogy in order to protect individuals.[70]

In Germany, the amendment of the Aviation Act[71] is under judicial and social consultation review. The amendment aims to lay down rules for private usage of drones and it does not address the commercial operation of unmanned aircrafts. The new rules require valid liability insurance, in some cases, the German aviation authority approval process is also needed. The drone operators, private or commercial are alike to comply with the rules of the German Federal Data Protection Act.

According to the Act on the modernization of the Federal Aviation Administration of the United States of America[72], drone is *"an aircraft operated without the possibility of direct human intervention from within or on the aircraft".* The legislation created by the U.S. Department of Transportation aims to reduce the risk of damaging or hurting people, related assets and other aircrafts. Similarly to Hungarian rules drones cannot fly over anyone who is not directly participating in the operation and a continuous visual contact is also required with the unit. These rules are equally suitable for reducing the possibility of any injury and the protection of others privacy. As part of a privacy education campaign, the agency provides all drone users recommended privacy guidelines as part of the registration process.

69 Section 2 (4) of Privacy Act
70 C-212/13, EU:C:2014:2428
71 Luftverkehrs-Ordnung (LuftVO)
72 FAA Modernization and Reform Act of 2012, Pub. L-. No. 112-95. § 331(9)

Content

Nemzeti Adatvédelmi és
Információszabadság Hatóság

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

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

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

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

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