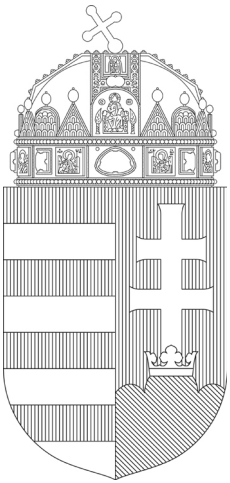
National Authority for Data Protection
and Freedom of Information

EXCERPTS FROM THE PAST 25 YEARS
OF THE SUPERVISION OF INFORMATION RIGHTS

Excerpts from the past 25 yearsof the supervision of information rights

Edited by Dr. Attila Péterfalvi



Introduction

As "***the peaceful transition from a single party system to a multi-party system, from the party-state to a constitutional state requires a substantial amendment to our current Constitution***",[1] Act XXXI of 1989 on the Amendment of the Constitution was promulgated on 23 October **1989**. This act, amending the text of the previous socialist constitution, was the first to declare that everyone in the Republic of Hungary has a right to the protection of personal data [Article 59(1)] and a right to access and distribute data in the public interest [Article 61(1)] as fundamental rights in its Chapter XII on Fundamental Rights and Obligations.

Three years later, on 27 October **1992**, Parliament adopted Act LXIII of 1992 on the Protection of Personal Data and the Accessibility of Data in the Public Interest (Data Act), when on 30 June **1995** it elected the first ombudsmen, including László Majtényi as data protection commissioner.

In this way, in September **1995**, the work which continues to date began in the Office of the Data Protection Commissioner.

In **2011,** the new Fundamental Law in its Article VI lays down the right to the protection of personal data and the freedom of information in the same locus together with the independent authority created by cardinal law to supervise the enforcement of these rights. By way of implementing these provisions, Act CXII of 2011 on the Right to Informational Self-Determination and the Freedom of Information was born in that same year to replace the Data Act and on 1 January 2012 the Nemzeti Adatvédelmi és Információszabadság Hatóság (Hungarian National Authority for Data Protection and the Freedom of Information – NAIH) began its operation.

The institutional framework changed, the legal environment was somewhat different, but the constitutional foundations were similar and in addition to the head of the supervisory authority, the persons of some senior staff members represented a kind of personal continuity indicating the unambiguous continuity of data protection supervisory activity.

1 Justification of Act XXXI of 1989 on the Amendment of the Constitution

The number of years passed, in particular the 25th anniversary, deserve honouring, but at the same time it requires a kind of accountability. The idea of this retrospective jubilee volume was born in the spirit of this intention endeavouring to draw the historical arch of the supervision of information rights from the beginning to the present.

As an opening upbeat of the volume, the first lawyer staff member of the Office of the Data Protection Commissioner recalls the initial "heroic age", the challenges of the era of the ombudsman protecting fundamental rights, citing concrete cases and complaints. The next block includes a bunch of the older writings of the second data protection commissioner and current NAIH president, exploring the essence of information rights in a kind of legal philosophical-theoretical train of thought taking the conditions of personality protection as its points of departure, and reaching the study of the human rights aspect through the amendments of the legal background. The author of the third part takes a new viewpoint: he presents the creation of GDPR and its impact on the Hungarian legal system. Finally, the volume closes with the writings of the most recent generation: the two winners of the student competition invited by NAIH (in the categories of tertiary and higher education) share their thoughts with the reader on the current challenges to data protection: "***Can a new perspective, the recognition of the right of natural persons to have pecuniary disposal over their personal data provide a solution to the data protection regulatory challenges of the digital age?***" and "***Issues of privacy in the area of data protection from the viewpoint of a high school student***".

We hope that while perusing the volume the interested reader will find thoughts and ideas that will urge him or her to think deeper or to reminiscence. We are convinced that the past of the subject matter is exceedingly rich and its future is virtually inexhaustible.

14 December 2020.

1. Dr. Júlia Sziklay: Recalling the beginnings – the ombudsman protecting fundamental rights

Júlia Sziklay PhD: lawyer and politologist, first legal staff member of the Office of the Data Protection Commissioner, currently head of the Freedom of Information Department of NAIH

In Hungary, the institution monitoring and supervising the enforcement of information rights as constitutional fundamental rights ex officio has been operating uniquely in a global comparison within the framework of a joint legal regulation, right from the very beginning. This task was handled by the data protection ombudsman between 1993 and 2011 (in terms of its practical operation from 1995) and by the Hungarian National Authority for Data Protection and Freedom of Information from 2011 to the present (whose first and second president has been Attila Péterfalvi, the second data protection commissioner). Undeniably, there is personnel and operational continuity, but the background and principles of operation of the two organisations are rather different, so apropos of the anniversary, it is interesting and worthwhile to recall the beginning of the operation of the data protection commissioner.

The institution of the ombudsman

"*If it is to be an ombudsman, then let it be a proper ombudsman by public law*"

Péter Tölgyessy[2]

The term "mediating person" reaching out from the family of the guilty towards the family of the victim with values promoting redemption of sin was used already in the Middle Ages by the German tribes. The term ***ombudsman*** was present in Swedish, Norwegian and Danish medieval legal terminology meaning "legal agent" or "representative". Official legal history underlines the name of Charles XII, king of Sweden, , who having lost the battle of Poltava in 1709 became acquainted with a judicial dignitary investigating administrative complaints at the court

2 In: A rendszerváltás forgatókönyve – Kerekasztal-tárgyalások 1989-ben. Bp. 1999. p. 451. Editor-in-chief: András Bozóki

of the Turkish sultan.[3] At the turn of the 18th century, Swedish public administration was about to disintegrate because of the long absence of the king, so in 1713, the king established the office of the ***Kungens Högste Ombudsman – Highest Royal Commissioner –*** later referred to as the office of the judicial chancellor to ensure that laws and other regulations were complied with everywhere and that officers and judges unfaithful to their office were punished. From 1766, the judicial chancellor was appointed by the Parliament, but the king regained the right of appointment in the era of the absolute monarchy.[4] For the first time ever in the world in 1809, the Estates represented in the Riksdag created their own office of the parliamentary ombudsman and incorporated the institution in their newly codified constitution. The Justitie ombudsman was granted the same rights and obligations as the judicial chancellor and his task was the parliamentary supervision of the king, the royal offices and the courts. These continue to be its main characteristics to this day with the note that most European ombudsmen cannot supervise the judiciary.

Three major waves of introducing the institution across Europe can be distinguished:
– establishment in the Scandinavian countries (18th-19th centuries)

– introduction in Western Europe (second half of the 20th century)
– institutions called to life to assist the process of democratisation in formerly dictatorial states (Greece, Spain and the former socialist countries) (end of the 20th century).

The development, and the international spreading can be described as intensive even today, thus by the 21st century the constitutional idea that highly respected persons are entrusted with the independent, informal and soft control of public administration has become reality virtually all over the world[5]. The 'ombudsman concept has become inseparably intertwined with the principles of democracy and constitutional statehood in the interest of their efficiency.[6] In the interest of the protection of

3 András Zs. Varga: Ombudsmanok Magyarországon, Rejtjel Kiadó, Budapest, 2004
4 André, Roles for the Ombudsmen – View from Sweden, in Rautio (ed), Parliamentary Ombudsman, Finland 80 Years, 2006, 36
5 Today, the International Ombudsman Institute of the University of Alberta (Edmonton, Canada) represents the ombudsmen of 125 different national legal systems; in 1976 this figure was 38.
6 See Mauerer, Die parliamentarischen Ombudsmann-Einrichtungen in den Mitgliedstaaten des Eu-

human rights and the responsibility for "good governance", the increasing importance of the activities of the ombudsman is recognised all over the world[7] and the institution can be found in every European constitutional state in one form or another.[8]

The International Bar Association defined the **concept of ombudsman** in 1974 as follows; the definition is still governing because of the international development:

"*An office provided for by the constitution or by Parliament and headed by an independent high-level public official, who is responsible to the legislature or Parliament, who receives complaints from aggrieved persons against government agencies, officials, employers or other independent bodies who acts on his own motion and has the power to investigate and recommend corrective action, and issue reports.*"[9]

This definition is still accurate as it summarises the essence well because the most important characteristic of the procedure of the ombudsman is independence[10], which as proven during the past years is best served by election by Parliament[11]. The importance of the institution of the European ombudsman and its proliferation in various legal forms is largely due to its unique constitutional position: it is almost perfectly independent of the branches of state power, which it can control. The powers and responsibilities are limited to the extent that he should not disturb the sensitive equilibrium of state powers. The key to his efficiency is ensuring his independence and his informal procedure fuelled by personal authority and commitment to public life. Taking these fundamental elements as the point of departure, the ombudsman can autonomously and individually develop his own procedures so that his activities make up for the deficiencies of the relevant legal system in protecting the rights of

roparates, In: Matscer, Ombudsmann in Europa. Institutioneller Vergleich, 1994, 123

7 See Reif, Governance, 55, 81: Robertson, National Government and the Ombudsman, In: Reif, Ombudsman Concept, 105

8 Gabriele Kucsko-Stadlmayer: Europaische Ombudsman-Institutionen, 2008 Springer-Verlag Wien

9 Quotation from Calden, In: International Handbook of the Ombudsman. Evolution and Present Function, 1983, 44

10 See IOI by-law, www.law.ualberta.ca/centres/ioi/docs/IOI_Bylaws.pdf (Art. 6b).

11 See Recommendation of the Parliamentary Assembly of the Council of Europe 1615 (2003) 1, No. 8 1.1.1.1.

citizens[12]. Over the past years, the institution proved its ability to develop particularly in the field of the protection of human rights, primarily in the countries where after the fall of totalitarian regimes help was needed in building up constitutional and democratic regimes. The development is not over anywhere because the international tenets of "good governance" and "good public administration" have targeted many ways of developing citizen-friendly public administration, in which an active role is intended for the ombudsmen. Moreover, the offices of ombudsmen have aimed for or have already gained the status of UN National Human Rights Institution (NHRI) in many countries. NHRI is an independent entity protecting rights with general powers, which is capable of efficiently performing the continuous control and protection of human rights in the country concerned and it has demonstrated in the course of a strict accreditation procedure that it meets international criteria. In this way, it becomes party to the international network operating on all continents under the direction of the UN. Full or partial compliance with the criteria results in status A or B, the absence of independence and/or efficiency in status "C".[13] The Office of the Commissioner of Fundamental Rights has had status "A" since 2014; unfortunately, however, there are news about its degradation.[14]

Classification based on competences results in three **ideal typical models[15]:**

– the classical model (the ombudsman does not have his own powers of coercive force to do away with maladministration, he can achieve his goals with a kind of "soft" pressure through the fact of his investigation, his own authority and the "weapon" of transparency),

– the constitutional state model (in addition to the "soft" instruments, the ombudsman is armed with several special powers and competences, for instance to initiate review by the Constitutional Court or the right to participate in court procedures), and

12 See Kelsen: Wesen und Entwicklung der Staatgerichsbarkeit, WdStRL5, 1929,30

13 Dr. Júlia Sziklay: Az ombudsman nemzeti emberi jogintézményi (NHRI) státusza In: Nemzet és Biztonság, December 2011, http://www.nemzetesbiztonság.hu/cikkek/sziklay_julia-az_ombudsman_nemzeti_emberi_jogi_intézményi_nhri_statusa.pdf

14 https://nepszava.hu/3081976.lefokozhatja-a-magyar-ombudsmant-az-ensz

15 Based on the theory of Linda Reif and Gabriele Kucsko-Stadlmayer

–the human rights model (special powers to remedy human rights infringements, for instance by constitutional complaint or the possibility to take legal action).

The models do not exist anywhere in their "pure" form; but based on practical experience, the national political role undertaken by ombudsmen has greatly exceeded the classical idea of controlling public administration by today.

In addition, we can distinguish ombudsmen with

– national competence and general powers,

– regional competence, but general powers,

– national competence entrusted with special tasks (the Hungarian data protection commissioner was in this category).

In the wake of the fall of the Soviet-type regimes, demand for the introduction of the institution of ombudsman as a new element of the public law system was also expressed in **Eastern Europe**; in Hungary, however – in accordance with the state of affairs at all times – there was a permanent inability to make decisions and confusion around the establishment of the institution and the selection of candidates.

The data protection ombudsman

In the case of ombudsmen, the selection of the person is of particular significance because owing to the "amorphous" nature of these right protecting offices – the office itself is strongly developed and formed, particularly in the first case, by the person filling that position in accordance with his personality, qualifications and activity (courage): "***Behind the lean legal activity of the ombudsman, there must be set of personal values necessarily expressing what the ombudsman thinks of the world and of the society, whose problems he confronts.***"[16]

16 Katalin Gönczöl - Judit Kóthy _ Ombudsman 1995-2001, Helikon Kiadó, 2002, p. 69-70.

The election of the ombudsman was required not only by the Data Protection Act of 1992, but also by EU law.[17] The fact that the Hungarian data protection commissioner put on the "coat" of an ombudsman had the consequence that in his statements he was able to enforce certain extrajudicial criteria (equitableness, justness, fairness). Among the institutions protecting rights, he was able to efficiently supervise the enforcement of information rights. When regulating his powers[18], the legislator supported the procedure of a separate commissioner in a welcome, but not self-evident manner with expressly strong rights as his powers extended to all the abuses related to fundamental information rights (except if there was a court procedure in progress in the case) and he was authorised to investigate all data processing in Hungary, irrespective of whether it took place in the private or the public sector. In discharging his duties, he could ask for information from the controller at any time, he could have access to any document, and he could enter any premises, if he deemed it important for the investigation.

The data protection commissioner – incorrectly his brief title only includes one of the rights supervised by him – became the "guardian" of two informational rights and he monitored the development and application of these rights ex officio or as a result of complaints. He gave preliminary opinion on the relevant legal regulations and he could put forward recommendations to the legislator to amend legal regulations at any time. Acting within his powers regarding the supervision of secrecy, he could call for the termination of classifications and in the event of disagreement, the classifier had to turn to the courts. (Later on the situation was rather similar when the data protection commissioner called upon the controller to cease unlawful data processing and the controller had to attack the commissioner's decision in front of the court.) The protection of informational rights met the highest-level criteria in an international comparison based on powers, which was due not least to the influence of the Constitutional Court.

17 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The directive required that Member States establish an independent data protection supervisory body.

18 His powers and responsibilities are primarily regulated by Act LXIII of 1992 on the Protection of Personal Data and Accessibility of Data in the Public Interest, but a number of other laws also contain authorising provisions, these include, for instance, the Act on the Protection of Classified Data, the Act on National Security, etc.

Figure 13: The data protection commissioners of the Republic of Hungary 1995-2011

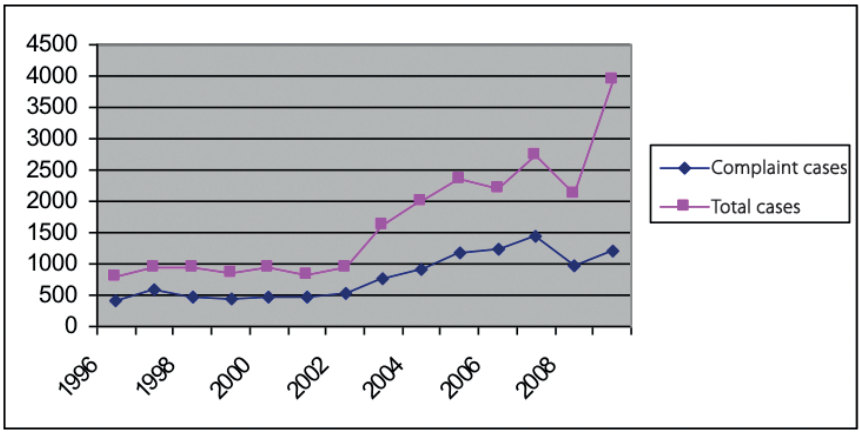


Figure 14: Case statistics of the Office of the Data Protection Commissioner, 1995-2009 (Source: ABI)

30 June 1995 – 30 June 2001: Dr. László Majtényi, the first data protection commissioner

1 July 2001 – 10 December 2001: The Period of the first "interregnum"

11 December 2001 – 10 December 2007: Dr Attila Péterfalvi, second data protection commissioner

11 December 2007 – 28 September 2008: the period of the second "interregnum"

29 September 2008 – 31 December 2011: Dr. András Jóri, third data protection commissioner, who was in office only for half of his mandate

Regime changing data protection

"I owe you gratitude for the benevolent and helpful administration of my request... Selfishly I must say it is a shame that your institution began its operation late from my point of view. If you were not there, who could (a poorer person) turn to, who representing his case as a good attorney also have authority, power and influence for its reassuring settlement."

The office could be defined as a regime-changing institution both according to its self-definition and its external profile. Right from the beginning of its operation it was seen that sensitivity in Hungarian society towards information rights was much more advanced than what could have been expected even relative to the niveau of general legal culture.
"Ornamental element or supporting pillar?" asked István Szikinger about the constitutional position of the ombudsmen in 1996; in his view, it depends on the approach of the parliamentary commissioners towards their role whether they become ornamental elements or supporting pillars of a constitutional state. Undisputedly, the "first generation" ombudsmen played a pioneering role in Hungary because they built up their offices from nothing, relying on their earlier experience, their expertise, their personalities and the understanding of their role. Dr. László Majtényi (formerly legal counsel to MAHART, then chief counsellor at the Constitutional Court in addition to being a university professor and author) defined his role as an ombudsman focusing on complaints and keeping a distance from power and politicians. (There is also an approach according to which the ombudsman should not avoid political storms, proclaiming instead the almightiness of constitutional rights, he should throw himself into all kinds of fights.) Majtényi discarded the concept of an "activist data protection commissioner" in his day-to-day work and "***averted the temptation of populist activism displayed in an ill-sense also in that he conducted ex officio investigations only in exceptional cases if particularly warranted when the individual whose constitutional rights were infringed***" was unable to do so (e.g. investigation into the anomalies of adopting "Internet" children cared for by the state or those surrounding the manufacturing of tax IDs.
Who turned to the data protection commissioner initially?
Citizens, politicians, celebrities and human rights NGOs "tested" the new human rights institution with a view to dealing with their complaints. Members of Parliament regularly mediate in their constituency's complaint case. Inventors contacted the office wishing to implement their IT id as through the office and a great many people who were pa ties to litigation asked for assistance with their lawsuits. These requests had to be rejected by the operation of the law.
Controller organisations asked for professional opinion to protect themselves or their customers typically when some practical problem

occurred - for instance the head of the Land Registry initiated consultation about the deficiencies and contradictions of the rules of property records. Right from the first moment, the developing good working relations and cooperation with the major state controllers is a highly important and positive step in the operation of an ombudsman's office.

The vast majority of the submissions were related to the change in regimes from some aspect through the political, legal or even economic consequences of the transition. It struck the eye how much emotion was expressed in the complaints received over the first months, turning to the data protection commissioner was the last desperate option for ordinary people without political or economic influence to hold on to the last straw. It was as general feature that these complainants had already exhausted the possibility of legal remedy through the courts – they were handed down rejecting verdicts or the litigation was still in progress.

A characteristic group of cases during the change in political regimes included the so-called 'surveillance' cases with the right to informational self-determination of those surveyed in the centre. In several cases, the complainants were active in public life, generally politicians, journalists, influential businessmen having extensive network of connections and influence. The recommendations of the data protection commissioner concerning the generation of the pre-regime change secret service documents held by various government agencies in 1995, the possibility of the citizens to exercise their right to informational self-determination and access to these documents by others and the enforcement of the freedom of information involved profound work of legal interpretation, which underlined the data subject's right to informational self-determination out of the web of various interests. The investigation was initiated by liberal politicians with the collaboration of the Nyilvánosság Klub, but other data subjects (former dissidents, etc.) also added their voice. Another type of the surveillance cases was expressed in a few shocking submissions, whose authors were "forced informers" stricken by conscience throwing light on the complicated and complex interpretation of the rights of the informers and those informed upon.

The statement concerning access to the video recording of the negotiations of the opposition round-table (EKA) documented by Black Box [Fekete Doboz] is also related to the change of political regimes. The data protection commissioner stated that in the light of the historical

events, EKA qualifies as a public law institution and as such the recordings of its meetings are public according to the general rule.
The issue of researching of archive materials generated in relation to the persecution of the Jews during the Nazi era also related to the topic of informational compensation. In this case, the statement by the data protection commissioner was initiated by a Hungarian historian entrusted by the Yad Vashem Archive of Jerusalem. The most important "result" of the 27-page statement was the conclusion of a bilateral international public law agreement enabling historical research, which grants the possibility of exercising the right to object for the data subjects and their relatives.
The change in the economic regime resulted in the entry of a new market building instrument: direct marketing; the new market agents were direct marketing companies, which tried to "obtain markets" ruthlessly for themselves and their customers until the enactment of the 1995 Act. The citizens' initial attention soon turned into aversion due to the not quite fair and not quite quality-minded shops and the overflowing mailboxes. Complaints against direct marketing firms, typically in the realm of privacy, arrived by the dozens. Citizens regarded the formally lawful solution as harassment and inacceptable from the viewpoint of data protection as the 1995 Act legalised the activity of these companies imposing legal limitations on them so that data subjects could exercise their right to self-determination only negatively by exercising the right of objection (opt-out).
Complaints against the new actors of the market economy, such as investment trust managers, are associated with economic restitution. These fund managers promised high yields to small investors, but they frequently went bankrupt before making good on their promises. Withholding data related to land auctions is also linked to restitution – according to the statement of the data protection commissioner, these are also public data in the public interest.
Certain procedures related to freedoms also had aspects related to data protection and freedom of information. An example of this is the enforcement of the right to a healthy environment through accessing information related to the establishment of a hazardous waste incinerator.

In consultation cases characteristically it was the controllers that needed the help of the data protection commissioner in disputed issues (e.g.

question by the lawyer of a telecom company whether the preliminary approval of the prosecutor is needed when the Police ask for data, etc.).
Data protection infringements and mistakes resulting in family conflicts classically belong to the sphere of privacy. The daughter of an alcoholic father initiated his treatment at the municipality, but the response arriving from the treatment facility revealed the "treachery" of his daughter to the father.The data protection commissioner established the infringement of confidentiality, but he was unable to set right the problem generated.
Interest groupings and class action participants evolving as a result of some kind of injury were important, such as the community of deceived small investors with an 'enthusiastic' leader, who took their common problems to all possible fora, or the action of the 'village spokesman' in the matter of the waste incinerator to be installed in their village.

An outstanding group of cases during the first (and similarly the second) period of the office was the entry of the new centralisation plans on the part of the government, which can be assessed as renewed attacks and the series of attempts to prevent the "new centralisation". In the 1970s, the emergence of information-related rights in Western Europe was linked to technical development, which enabled the appearance and operation of automated mega databases. In Germany, the government of Hessen promoted the "functionally integrated administrative system" through the use of computers in their publication called the "Great Hessen Plan" of 1970. The point was that society would transfer its tasks to the state and a gigantic IT system would come into being, storing roughly seventy items of information on every person. The data would be directly accessible within the system through searching for personal ID numbers, so for instance the statistical office, the police, the school or the doctor could communicate with one another within the system. As a result of the enormous public outcry, the plan failed in Germany.
In 1996 in Hungary a neo-centralist recording system was developed with a view to successfully collecting public debts based on the submission of the Ministry of Finance – which was owed apparently by the entire Horn cabinet. This system would not physically integrate all the records related to public debts, but would combine them from the viewpoint of accessibility (without contact codes). The plans affected data processing at the Tax Administration, the National Command of the Customs and

Finance Guard, the Pension Payments Directorate and the National Health Insurance Fund, the labour administration and the municipalities. According to the data protection commissioner, the implementation of the plan would mean that "*The state or rather the political group operating the state at any time would obtain a permanent and strong informational overpower over society and of course it would be pure illusion to imagine that this overpower would only threaten those violating the law as this would be the argument, they would try to get society to accept the plans. Just consider how a single erroneous data in the system would impact the life chances of a citizen*".

In 2005, the plan to develop a single recording system to improve the collection of public debt resurfaced within the framework of the "100-step programme" by Prime Minister Ferenc Gyurcsány first as a concept, then as a bill to amend the law. The plan to do away with parallel reporting, more efficiently enforce the rights of the insured and to control compliance in an up-to-date manner with the obligation to pay contributions aimed for interoperability among major public records (tax administration, health insurance fund, etc.), even though there are few examples in international practice for connecting major public databases set up and operated for different purposes in the way as recommended by the report. Because of this, the restriction of personality rights as revealed by the proposal was considered inacceptable by both data protection commissioners.

The social acceptance of the data protection commissioner

Based on the experiences of the first period, the social acceptance and publicity of the institution were good. Reactions according to which "the ombudsman sides with the criminals, representing the minority against the interests of the majority, etc" were rare. Such statements were generally based on lack of information or disinformation. A good example of this was the speech of the socialist MP Gyula Hegyi following the 1997 report of the data protection commissioner, when the MP aired his personal aversions in connection with the introduction of the residents' register of condominiums, even though the data protection commissioner never made a statement on this subject matter and there has never been an investigation into such a case.

The study entitled "The prominence and evaluation of parliamentary commissioners among the population" carried out by Szonda Ipsos

in December 1998 revealed interesting conclusions. There were few references made in particular at the data protection commissioner based on the answers of the representative sample consisting of a thousand adults. Being actively known increased along the dimensions of school qualifications and financial position just as in the case of the residents of settlements of higher status (the capital city and the county seats). The youngest and the eldest named the ombudsman as institutions providing assistance in the case of the violation of rights at a lower ratio than the middle aged. 10.8% of the respondents explained more or less accurately that the data protection commissioner deals with the protection of data and calls people accountable for compliance with the Data Protection Act, but more people used the term protection of personality rights, while two people formulated this from the viewpoint of the controller ("***We can say nothing to anyone except for those authorised***"). Only four respondents gave expressed praise.

The analysis of the total results showed that people mixed up the activities of the ombudsmen, but the vast majority of the answers reflected approval of the existence and work of the office. ("***It is good that there are ombudsmen, at least somebody can force the authorities to comply with the laws.***" "***The operation of the ombudsmen is useful because there is a need for more organisations to ensure the enforcement of the rights of the people in a democratic state.***" "***It is good that there are ombudsmen because an authority cannot disregard censure by such high-ranking people.***") Roughly half of the respondents fully agreed and about 20% tended to agree with these statements.

According to the analysis, the citizens greatly appreciated the fact that the ombudsman provides democratic control over the procedures of the authorities. Answers reflecting dissatisfaction remained in the minority (11%) ("***It is not worth a shit. Those who have money can buy the classified things.***" Or "***It is worth nothing, they issue data to anyone,***" or "***Protector of the rich and influential***", or "***It is bullshit***", or "***They do not do the work corresponding to their responsibilities***").

The analysis of agreement with negative statements by individual socio-demographic groups revealed that the same groups – graduates, prosperous, Budapest residents – rejected these statements the most vigorously, who identified the most with the positive opinions.

The statistics of the office show a somewhat different picture. The analysis

of the social position of the complainants demonstrated that data protection was not the "caprice" of the highly qualified elite, sensitivity to it could not be linked to any social stratum, level of education or economic status, it covers the entire Hungarian society from the unemployed homeless to the senior managers of multinational companies according the statistics of the office.

The situation is different in the case of those showing interest in data of public interest partly because the demand for access to data in the public interest is substantially behind data protection complaints in terms of its intensity – the hunger for information on the part of the representatives of the press as can be measured by the office is somewhat restrained – and the composition of the complainants is also different. A large number of controllers (mayors' offices, municipal executives, etc.) sought the office with issues of interpretation of the law, NGOs concerned initiated investigations at a rate of about 10%, while representatives of the press sought the office at a hardly higher rate. Citizens rarely lodge individual complaints, and if so, largely in relation to whether municipal documents are in the public interest (presumably, because they are personally affects). It is a new phenomenon that members of Parliament bombard ministries with requests for data in the public interest "as if it was a campaign" at around official (longer) public holidays, which of course does not exempt the controller from meeting his legal obligations.

Complaints have always made up more than three-quarters of the work of the Data Protection Office; in the remaining part providing opinion on legal regulations and the supervision of secrecy represent a much lower ratio than "other" cases (e.g. consultations or investigations launched ex officio.

It was an indisputable merit of the first data protection commissioner that he created his office from "nothing" and began his work facilitating the enforcement of information-related rights expressly within the framework of an ombudsman's work. With citizens' complaints in the foreground, he formulated his statement with a pure approach to protecting the law and the constitution, while taking care of the balance of information-related rights relative to one another. It was during that time that the principles were laid down, from which the consistent development of the data protection commissioner's case law began. That was a significant achievement, particularly in the light of the fact that at that time concrete

legal regulations applicable to individual life conditions were often missing.

The transition between the ombudsman and the authority

"Times were changing. The era of regime changing data protection came to an end. The task of Attila Péterfalvi, the second data protection commissioner, was totally different from that of his predecessor: he had to fine-tune the dogmatics of data protection law every day, he had to apply the text of a legal regulation reflecting imperfect codification work objectionable at several points from a professional point of view, day after day, from case to case. This was a less spectacular but very difficult task. In this new era, the demands formulated against the commissioner's office were also new: following the principles laid down as a result of the search for the path forward by regime changing intellectuals, if we wanted to resolve the problems of data processing by an international bank group, what counted was practical usefulness, legal precision, compliance with procedural due dates instead of recommendations of literary value. The small enthusiastic team had to be replaced by a well-organised office. The ombudsman model was gradually replaced by the logic of work by an authority."

Although openly professing to continuity and frequently referring to the decisions of his predecessor in office in his statements, Dr. Attila Péterfalvi has a different style as ombudsman. Earlier, he was legal counsel, attorney-at-law, college professor and external expert on Majtényi's staff. "***He paid less attention than his predecessor to building up case law, interpreting instead the law spanning cases, the solution to the given case seemed to be more important to him.***" The (abstract of) an answer he gave to a private person when dealing with a concrete complaint can be taken as his ars poetica: "***Albeit you expressly requested in your letter to give you an unambiguous 'yes' or 'no' answer, unfortunately the evaluation of this issue is more complicated than this. Believe me, my title as data protection commissioner does not predestine me to tire the already overburdened public with evasive, incomprehensible statements, quite to the contrary, the essence of the institution of data protection commissioner is to investigate and adjudge events clearly using only the twofold yardsticks of what is lawful/unlawful within the rather complex framework of the rule of law.***"

He was particularly frequently in the limelight; in 2003, he gave more than 300 interviews to reporters, so the issues of the office and of data protection and freedom of information became increasingly well-known in a wide range. (For instance, between 1 March and 7 April 2005, 37,569 visits were paid to the website of the data protection commissioner.)

In addition to domestic fame, the foreign relations of the office were greatly strengthened. The Hungarian data protection commissioner was an equal partner of his Western colleagues at every forum and in a sense he achieved a leading role among the representatives of the former socialist countries – this could be clearly seen at international meetings and in the course of international cooperation.

The amendment of the data protection act in force from 1 January 2004 was an important step in defining the legal status of the data protection commissioner: the commissioner was granted the powers of an authority by being authorised to order the blockage, erasure or deletion of data that were processed without authorisation and to prohibit the unauthorised processing of data and to suspend the forwarding of data abroad. The controller may turn to the courts against measures taken by the data protection commissioner. (To date, this happened in two cases: once because of the commissioner's decision objecting to the possessing the data of minors related to a programme by a commercial television channel reflecting dubious taste; in the other case, the secretary of state for public funds turned to the courts against the commissioner's decision objecting to the processing of hunter logs involving prominent persons, but later he withdrew his petition.) These authority-like powers clearly moved the data protection commissioner away from the classical role of the ombudsman, whose main feature is its position outside (but not above) public administration and its weak instrumentarium (the main weapon being publicity and not taking measures).

The shift towards being a data protection authority was also reflected by the cases. Naturally, the classical and constantly recurring complaints, such as copying the ID cards or criticism of direct marketing companies continue to flood the office en masse.

In addition to the classical ***privacy*** and freedom of information cases, the second data protection commissioner also had to react to new challenges, in which he was more of an active agent than an external supervisor. The series of decisions, measures and initiatives taken in the course of

building up the information society in Hungary, the presentation of the Hungarian Information Society Strategy at the end of December 2003 and the intensive commencement of its implementation with the ongoing collaboration of the data protection commissioner and his staff should be highlighted. The problems related to the application of EU law became a new challenge for Hungary upon its accession to the European Union. In relation to this, it should be noted that for a number of public controllers – for instance, in cases involving social insurance – the standard answer on the part of the controller was a reference – frequently ungrounded – to "new EU expectations". With regard to ensuring an adequate level of data protection from that point of view, Hungary could be regarded as an EU Member State already from June 2000; so we were well prepared in this field even relative to the European standards. This is substantiated by the "Peer Review report on Hungary's data protection" in June 2002, which assessed Hungary's administrative infrastructure from the viewpoint of adopting the EU's data protection corpus: "***We were highly impressed by the depth of knowledge on the part of the commissioner and his staff and their understanding of the issues of data protection. We also paid tribute to how seriously they take their work and what gigantic results they already achieved in spite of the limited instruments available to them.***"

Of the cases investigated by the second data protection commissioner, the statement objecting to data processing by the Church of Scientology and data processing related to the riots in the autumn of 2006 (including the answer to the question "Can a prime minister lie?" also deploying moral argumentation) commanded outstanding attention. From the viewpoint of interpreting the law, the opinion related to research involving healthcare data was very important as it answered the question whether the definition of medical research on humans clearly included research on identifiable data in addition to research on identifiable human substance/tissue. As the data protection commissioner's answer was a clear yes, research on healthcare data cannot be carried out without the permission of the ethics committee. Among the cases related to freedom of information, the statement concerning access to meteorological data (also raising the issue of the cost of the freedom of information), and the recommendation covering the experiences of six years and nine cases related to the accessibility of the supervisory activities of the Government Supervisory Office should be highlighted.

– One of the value assessment indicators of the activities of the data protection commissioner was the public opinion poll carried out by Szonda Ipsos between 15-21 February 2008 concerning the assessment of the ombudsmen, involving 1,000 adults with permanent residence in Hungary, using a questionnaire and personal interviews. Comparison with the 1998 data was particularly interesting – in the case of the data protection commissioner his active recognition increased 4.7 times in percentage terms.

Figure 15: Szonda Ipsos survey 1988, 2008: To which institutions can a citizen turn to in case of the infringement of his rights? (Source: Szonda-Ipsos)

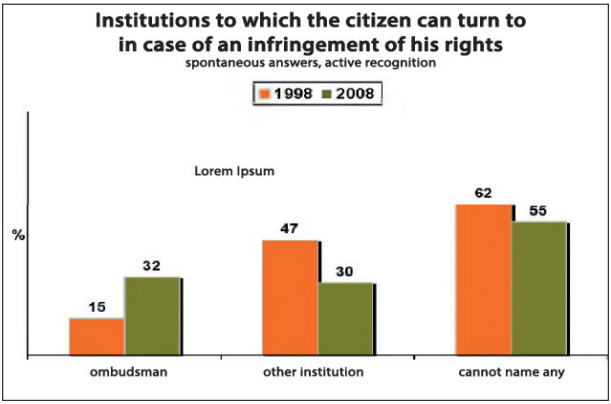
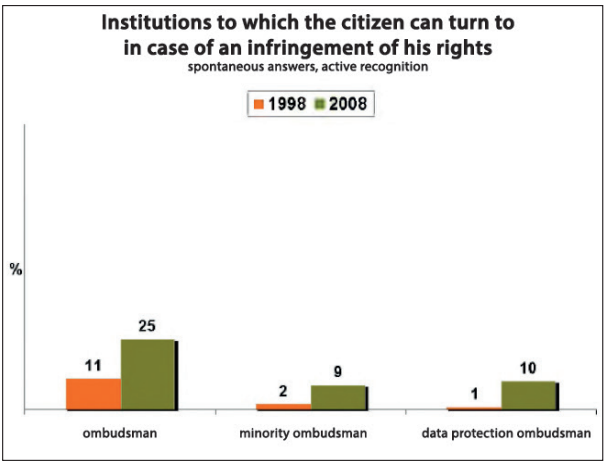


Figure 16: Szonda Ipsos survey 1998, 2008: To which ombudsman can a citizen turn to in the event of the infringement of his rights? (Source: Szonda-Ipsos)



The second data protection commissioner still worked within the framework set for the ombudsman, but with responsibilities and powers pointing towards a data protection authority. It should be added that this was not a personal decision but a fact of legal regulation. He was always willing to take on mediational tasks of the ombudsman which he executed efficiently, and he was an accepted and "presentable" partner both in the national and international scene. This can be regarded as a particularly important achievement in an area, where the large state and non-state data processing systems (chip card, waiting list, etc.) "kept pushing ahead" almost as unstoppable tanks. The recognition and acceptance of the institution by society (we could talk about its popularity too) came to its height as a result of his public appearances during his period in office.

The mandate of the third data protection ombudsman, Dr. András Jóri (earlier he had been a clerk on Majtényi's staff, then an attorney-at-law for a few years) ended at half-term and he produced annual reports only in the first two years of his period in office, so it is rather difficult to give a comprehensive evaluation of his professional performance. In both 2009 and 2010, he specified the creation of a new balance between data protection and freedom of information as his priority task and the issues raised then have been the most interesting points of the connections between the two information-related rights ever since.
The notion of data accessible on public interest grounds was introduced by the so-called Glass pocket Act[19] together with the rules of the Civil Code of the time pertaining to business secrets in June 2003; it was incorporated in the data protection act on 1 January 2004. It was further clarified by the amendment to the data protection act, which entered into force on 1 June 2005 and this definition was adopted also by the Privacy Act. According to this, ***data accessible on public interest grounds means any data other than data of public interest, the disclosure, availability or accessibility of which is prescribed by an act for the benefit of the general public.*** Accordingly, by definition, data accessible on public interest grounds can be neither data of public interest, nor protected personal data. At the same time, ever since 2005, the act declared that the personal data of persons acting within the powers and authority of any entity, carrying out public tasks related to their responsibilities, qualify as data accessible on public

19 Currently Privacy Act Section 26(2)

interest grounds[20]. With this, the crisis of interpreting the constitution appears to have been resolved, the basis of which was that law required wide accessibility to data in the public interest but failed to provide an answer to cases when information related to the operation of the public sector could be linked also natural persons, hence their personal data were subject to privacy protection. This line was reinforced by the fact that as of 2009 it has been mandatory to disclose the remuneration of managers of publicly held business organisations and managers of public limited companies. The data protection commissioner strengthened the pro-accessibility interpretation with his statements made in several major cases which received a great deal of publicity[21].

Making use of his powers as an authority, András Jóri brought decisions in two major cases. In one of the decisions he ordered that the Central Office for Administrative and Electronic Public Services, acting as the controller of "Social Consultation 2011" initiated by the government, erase the personal data included in the questionnaires returned by the citizens and at the same time he prohibited the creation of a National Consultation Registry.[22] The other decision called for the erasure of the "list of shame" published by the Hódmezővásárhely Mayor's Office. The list disclosed the names, dates of birth and accurate addresses of some 300 citizens "who abused aid and refused public work". János Lázár, mayor of Hódmezővásárhely, attacked the decision of the data protection commissioner in front of the court, requesting its review. In 2011, the Budapest Municipal Court finally approved the decision and ordered the Mayor's Office to erase the personal data. At half-term of the mandate of the third data protection commissioner, the institutional structure of the data protection ombudsman was replaced by the Hungarian National Data Protection Authority as of 1 January 2012, operating in the classical form and with powers in accordance with Act CXII of 2011 on the Right to Informational Self-Determination and the Freedom of Information, which corresponded to the provisions of the New Fundamental Law. This had consequences on both personnel and organisation.

20 Currently Privacy Act Section 26(2)

21 For instance, recommendation 2250/H/2209 on the disclosure of the salaries of heads of institutions of higher education, or the statement on the disclosure of the remunerations of managers of business organisations in public ownership.

22 Decision ABI-1642/9/2011/H, https://naih.hu/files/A-szocialis-konzultacio-adatkezelesevel-kapcsolatos-adatvedelmi-biztosi-hatarozatot-modosito-hatosagi-hatarozat.pdf

The European Commission brought an infringement procedure against Hungary because of the "removal" of the data protection commissioner from his office before his term had expired and in its judgment brought in case C-288/12[23], the European Court established the infringement of EU law with the justification that "***the independence of the authorities responsible for the protection of personal data requires that Member States honour the full term of these authorities***". On 8 July 2014, László Trócsányi, then minister of justice, apologised for the removal in a communiqué and the amount of compensation at HUF 69 million was disclosed at the same time. Since then, András Jóri has not appeared in public.
In actual fact, the "initial era of heroes", the era of the ombudsmen ended with this unfortunate and sad episode in Hungary.

The institution was created by the change in regimes and it began its work with that momentum largely in the spirit of the protection of fundamental rights and information-related compensation following the earlier dictatorship. An enthusiastic and committed team took part in setting up and operating the office, for whom assisting those in need and the efficient and flexible handling of the complainants' complaints was their "labour of love".
Along the forced trajectory of its organisational self-evolution, the institution took leave of this "heroic era" in a few years' time, and set out along the path of permanent growth, expansion of powers and the concomitant inevitable bureaucratisation, the endpoint of which was transformation into an authority within the EU that is uniform and standardised upon the application of GDPR. Let us not forget, however, that the Hungarian National Authority for Data Protection and the Freedom of Information – just like the data protection commissioner – is the supervisory agency of two constitutional information-related rights. In the field of the freedom of information, the authority is to decide and take action still like an ombudsman in less formalised investigative procedures, frequently taking into account the extra-legal criteria of equity, reasonable expectations and ethics in the interest of the transparent operation of public life.

23 https://curia.europa.eu/jcms/upload/docx/application/pdf/2014-14/cp140053hu.pdf

2. Dr. Attila Péterfalvi: Historical overview of the development of data protection in Hungary until the entry into force of GDPR

Dr. Attila Péterfalvi: President of the Hungarian National Authority for Data Protection and Freedom of Information, University of Public Service of Hungary– associate professor, Ukrainian National Academy of Sciences

Kiev Law School – doctor honoris causa

The essence of data protection[24]

The right to the protection of personal data was "called into being" by technological development at the end of the 19th century. In 1890, Lewis Brandeis and Samuel Warren, American jurists, specified "the right to be unmolested" in the law journal of Harvard University, which they identified with the protection of privacy and which was jeopardised by the proliferation of cameras and "other machines". The parent right for data protection is human dignity, which is inviolable and unrestrictable as explained in the justifications of many decisions of the Hungarian Constitutional Court.

Data protection legislation

Legislation was late to follow the specification of the right. The enactment of the first national data protection laws in Europe was triggered by the IT development taking place in the 1970s and the major registration systems then introduced in Western Europe. From the 1980s, however, legislation focused no longer on the technology, but increasingly on the protection of data subjects.

The beginnings of data protection in Hungary

To learn about the beginnings of data protection in Hungary, I find it important to present my historical review entitled "The principles and the system of the civil law regulation of personality protection" published in Magyar Közigazgatás in 1991, in which I presented the ideological basis

24 Dr. Attila Péterfalvi: A Magyar adatvédelmi jogi szabályozás változásai, In: Állam és Jog – Kodifikációs kihívások napjainkban, Magyar Jog- és Államtudományi Társaság – Gondolat, Szeged-Budapest, 2013

of the "socialist" protection of personality rights and the legal institutions built upon that.[25]

"The basis of regulation was the theoretical approach that personality is a complicated, complex and controversial human reality. It is inseparable from the community, it can only prevail through and by the community, yet it is relatively separated from the community and this separation constitutes the peculiar individual nature of personality."[26]

So, personality is a natural, a social and legal reality at the same time. In law, the term personality means that the human quality figures directly as the subject matter of legal protection.

However, there must be a distinction between the person and the personality in law. The person is the subject of the law, who may have rights and may be subject to obligations, while personality expresses the specific social role of "human individuals", who have values recognised by society and as such is the subject of legal protection.

Personality protection appears in a complex form in law and in accordance with the legislative hierarchy, the most important personality rights – such as the protection of life and limb and the various freedoms – are included in the Constitution which is at the apex of the hierarchy.

Certain personality rights are determined by international treaties raised to the force of law by the Presidential Council. For instance, the international convention promulgated by Law Decree No. 8 of 1976 states that "it shall be particularly prohibited to subject anyone to medical or scientific experimentation without his or her free consent."

The rights specified in the Constitution and international conventions were regulated in detail by the different branches of law according to the regulatory criteria characteristic of the given branch of the law.

25 Dr. Attila Péterfalvi: A személyiségvédelem polgári jogi szabályozásának alapelvei és rendszere, In: Magyar Közigazgatás, Budapest 1991
26 Dr. Károly Törő: Személyiségvédelem a polgári jogban, Közgazdasági és Jogi Könyvkiadó, Budapest, 1979, p. 15.

Personality right protection is implemented together by several branches of the law. Beside civil law, criminal law ensures the enforcement of the constitutional principles in the widest range in the field of personality protection. Doubtless, these are the most efficient instruments of legal protection.

Criminal law protection is distinct from civil law protection in the sense that it is applied in the case of specific infringements, yet it is not an instrument for satisfying individual needs, it is always applied to protect society even if it is used as a sanction for a specific personality right infringement.

Civil law personality protection is characterised by the criteria of civil law regulation. Civil law is designed to satisfy needs in an individually specified manner, the legal relationship comes into being always between separate, independent legal subjects of equal rank and equal rights. The sanction has a value equalising, reparative nature and as such is designed to satisfy individual needs. What characterises civil law personality protection? Civil law personality protection is generally a legal relationship of absolute structure. It means that there are unspecified obligors vis-à-vis the rightholder. Both natural persons and legal entities are eligible for personality protection.

Obviously, a legal entity is not eligible for rights, which can only be linked to man, for instance, the right to life.

Among the personality legal relationships, we can distinguish between general and special personality legal relationships.[27] General personality legal relationships are enforced in full, their only precondition is the genesis of the person (the birth of a man, or the coming into being of a legal entity), i.e. the existence of the person.

Special personality legal relationships are more complicated. In principle, the range of the subjects of the law is open in this case as well, but there are conditions to the coming into being of a concrete legal relationship.

27 Dr. Károly Törő: Személyiségvédelem a polgári jogban, Közgazdasági és Jogi Könyvkiadó, Budapest, 1979, p. 42.

(E.g. a deaf and dumb person may not claim protection for his voice; legal protection for intellectual work is conditional upon the work being done.)

In addition to the legal relationships of an absolute structure outlined above, there are also legal relationships of a relative structure. These legal relationships always exist between specific persons, they are individual legal relationships. In these legal relationships, mutuality is the direct determinant of the content of the legal relationship. The content of the legal relationship requires positive action (e.g. the connection between the physician and his patient). In the case of personality rights, personality rights are also enforced through a legal relationship with a relative structure.

If we attempt to define the notion of personality law, we can establish that personality law is the branch of civil law, which regulates the non-pecuniary personal relationships of persons.

There are two groups of personality law legal relationships. One group includes the personality legal relationships, which are related to the protection of the person as such (both natural persons and legal entities). Under such legal a relationship, the person as such receives protection irrespective of exerting any kind of activity. Such as, for instance, the right to life and limb. These legal relationships are referred to as personal legal relationship in a narrower sense.

In general, the rules pertaining to the protection of person-related rights are applicable to legal entities too, except if the protection by its nature can only be granted to natural persons. The biological basis of personality is absent in the case of a legal entity. Though, by their nature, the provisions regulating the protection of life, health and limb cannot apply to legal entities. The protection of the rights linked to person do not extend to the state as the personality of the state and guaranteeing it are of a public law or international law nature.

The second group of personality legal relationships include those, which are related to the intellectual works of individual persons (only natural persons) (works of authors, inventions, etc.). In these legal relationships

the basis of the legal protection is not the man in himself, so this kind of protection is not due to every person, but to those only, who have created an intellectual product. The legal relationships in this second group are referred to as the legal relationships of intellectual creation. Man is capable of intellectual creation; creative activity can only be human work. Hence, legal entities do not have personality rights related to intellectual creation.

However, legal entities can also acquire the right to the use of intellectual creations, they may obtain the right of disposal over the result of intellectual creation, the work itself. Nevertheless, the personality right in relation to the work is due only to the creator, that is, a man.

II.

As a result of what historical development did the person-related rights and the civil law instruments of the protection of these rights evolve and in what do the so-called "socialist" principles differ from earlier civil law regulation?

Historically, the legal regulation of person-to-person relations evolved in the course of "capitalist" development. The "capitalist" development of law established legal equality, as it no longer speaks about slaveholders and slaves, feudal lords and serfs, but only about man, about persons in general. Capitalist law is the law of the abstract person, in which the civil law protection of personality evolved. This protection is, in actual fact, the declaration of the equality of man, of the principle of equality in front of the law. "Capitalist" law developed and raised to a high standard the legal instrumentarium of the protection of intellectual creation. What kind of a change was brought about by the "socialist" model? In a "socialist" society, the situation of personality changes fundamentally. This has an impact on the legal regulation of personality protection. According to the ruling ideology, with the cessation of the commodity nature of labour, socialist equality in front of the law, the legal equality of people working according to their abilities and sharing the goods based on their work replaces the capitalist form of equality in front of the law. "This opens the way for the far-reaching build-up of legal protection for the person of the citizens, of

making the rudimentary capitalist protection complete on the one hand, and the improvement of the laws governing intellectual creation on the other hand... Accordingly, personality rights undergo a fundamental transformation in socialist law, and the protection of the personality rights of citizens becomes complete in all directions."[28]

Looking at it factually and free of any ideology, what did the fundamental transformation of personality law mean? "Act IV of 1947 meant a radical change in the legislation of the people's democracy creating a new world, which annihilated the remnants of the old feudal system: the ranks of nobility (aristocracy), the rank of *"örökös főispán" (eternal lord lieutenant), the ranks indicating title, the honorary officials, the title of vitéz, the use of toponymics by nobility, coat of arms, symbols of nobility, the use of any title indicating social distinction, none of which are conformable with the equality of all humans in front of the law professed by democracy."*[29]

According to the ideology, the "capitalist" instruments of legal protection are primarily of a pecuniary nature even in the fields where the infringement concerned non-pecuniary interest, socialist law in contrast gives preference primarily to the non-pecuniary instruments in the field of the protection of personality rights.

This was the theoretical foundation of Act IV of 1959, the first Civil Code of the People's Republic of Hungary, which declares that the rights linked to the person are subject to the protection of the law.

The rules pertaining to rights linked to persons are of a peremptory nature, any contract or unilateral statement restricting rights linked to a person are null and void.[30] Civil law grants protection to rights linked to persons and legitimate interests in general, it provides protection against all forms of the infringement of personality rights irrespective of whether a given infringement conflicts with a separate legal provision or not. The system of rights linked to persons was as follows in Act IV of 1959: right to a name[31],

28 Miklós Világhy: Dologi és személyi jog. JK 52-10. 266/SzT
29 Dr. Gyula Dezső: Népi demokratikus magyar magánjog alapelemei (Vezérfonal az 1. évfolyami magánjogi előadások hallgatásához) Manuscript. Szeged, 1950.
30 Civil Code Section 81(2)
31 Civil Code Section 82(1)

right to good reputation[32], right to the secrecy of correspondence[33], right to a private home and premises for the purposes of the legal entity[34], rights to one's image and sound recording[35].

Based on the act, the sanctions for the infringement of personality rights can be divided into two groups. One group of sanctions is objective, i.e. they are linked to the act causing injury, irrespective of whether the infringement was culpable or not.

The other set of sanctions for the infringement of rights linked to persons is subjective, i.e. they are applicable only to culpable infringements.

Whoever suffers an infringement of his rights linked to person may demand the establishment of the fact of the infringement, irrespective of the culpability of the infringer, to cease and desist the infringement and the prohibition of any further infringement, or demand that the infringer should give satisfaction by statement or in any other way and ensure appropriate publicity for this, if applicable, and demand the termination of the injurious situation, the reestablishment of the conditions prevailing prior to the infringement, the annihilation of the thing produced with the infringement or the divestiture of its infringing nature.[36]

The subjective sanction for the infringement of person-related rights, which depends on the culpability of the infringer, is compensation. There is a theoretical distinction between the "capitalist" and "socialist" protection of personality rights also concerning the issue of compensation. "Capitalist" law knows the notion of non-pecuniary or moral damage, or intangible loss and acknowledges the right of the party suffering the infringement to compensation for non-pecuniary damage to various extents.

There were itemised rules with respect to this in our earlier law and a judicial practice evolved in general, which acknowledged the possibility of claiming compensation for non-pecuniary damage in the case of

32 Civil Code Section 82(2)
33 Civil Code Section 83(1)
34 Civil Code Section 83(1)
35 Civil Code Section 83(2)
36 Civil Code Section 85(1)

every infringement of person-related rights with the condition that the compensation should be equitable according to the circumstances of the case.

Compensation for non-pecuniary damage was particularly well known in the case of acts committed to infringe "female honour"[37], such as seduction or rape. In such a case, compensation was imposed because of a reduction in the chances of getting married.

According to the ruling socialist ideology, this form of protecting non-pecuniary interests is based on the approach of capitalism, which turns moral values into merchandise. Hence, according to the approach of the socialist law prevailing at the time, a grievance, which cannot be expressed in monetary terms, cannot be compensated for with money. Because of this, the Civil Code of 1959 enabled the imposition of compensation for infringement of person-related rights only, if the infringement also caused pecuniary damage. The 1977 amendment of the Civil Code made changes to legal regulations that corresponded to this approach.

The 1977 amendment to the Civil Code, incorporated into Act IV of 1977, brought about substantial changes in the field of person-related rights and the instrumentarium of protecting these rights. In many cases this also meant a change in approach. Prior to the amendment, it seemed contrary to the absolute structure of the personality relationship that legal entities should also have personality rights corresponding to those of people among the subjects of the law. The legal capacity of legal entities was limited. According to the earlier regulation of the Civil Code, a legal entity had legal capacity only within the circle defined by its social purpose and the requirements of socialist cohabitation.

The new regulation did away with this distinction. As a general rule, the legal capacity of a legal entity extended to all the rights and obligations which by their nature could be associated not only with man. The status of being a person is the basis for exercising subjective rights that regulate the realisation, enforcement and protection of the personality. Hence, a legal entity has person-related rights by necessity.[38]

37 Polgári jog és Családi jog Volume I. Felsőoktatási és Jegyzetellátó Vállalat. Budapest, 1960.
38 Civil Code Section 75(2)

The obligation to respect the personality rights and interests of others cannot be limited exclusively to man, hence the legal entity is also an obligee of the personality relationship. In this way, according to the new approach to legal relationships of personalities, the legal entity is also subject to personality rights. The content of the personality rights is, however, less in terms of the rights exclusively linked to man already referred to.

Beyond the range of the subjects of the law, the amendment also affected person-related rights. The right to a name was extended to names, assumed in relation to scientific, literary, artistic or other activities involving public appearances.[39] To avoid similarities of names that could give rise to mixing up people pursuing scientific, literary and artistic activities, to protect the right of a person who used to pursue such activities earlier, which name has become well-known as a result of these activities, the amendment made it possible to force the person entering public life at a later date to modify his name in a way that is suitable for distinction upon request, even if his name was not an assumed name.[40]

However, this did not mean a full or partial name replacement, the change could involve the expansion or shortening of the name. In terms of bearing a name, the amendment included the right of already operational legal entities to have their name protected by forbidding newly established legal entities to bear a name, which could give rise to mixing up their name with the name of an already existing legal entity.[41] The amendment extended the protection of the secrecy of correspondence to the protection of private secrets, and plant and business secrets.[42] The obvious reason for this was the protection of the interests of business organisations.

At the time of the enactment of the Civil Code in 1959, the use of computers was not yet widespread because of the level of technological development. By the time of the 1977 amendment, the extensive use of computers warranted the extension of personality protection.[43] Protection

39 Civil Code Section 77(2)
40 Civil Code Section 77(4)
41 Civil Code Section 77(3)
42 Civil Code Section 81
43 Civil Code Section 83

is bi-directional: on the one hand, information cannot be provided to unauthorised persons about the data recorded and processed, on the other hand, rectification of untrue facts and data can be requested. Although the rules concerning computerised population records and data processing were highlighted in the course of regulation, this did not mean that protection was narrowed down to this circle. The instruments of the protection of rights could be applied also in the case of infringements related to registration and data processing carried out with miscellaneous methods.

Beyond the extension of the range of rights related to persons, the 1977 amendment to the Civil Code broadened the instrumentarium of protecting rights that could be made use of in the event of infringements.

The new provision enabled the court to sequestrate the instrument of infringement as an interim measure, if the infringement was probable.[44]

Prior to the 1977 amendment, the Civil Code did not enable compensation for non-pecuniary damage. Judicial practice, however, endeavoured to grant financial compensation under the heading of general compensation for damage for disadvantage that could not be expressed in monetary terms. The notion of costs necessary for the elimination of the non-pecuniary disadvantage sustained by the injured party was extended to the expenditure deemed to be necessary to mitigate non-pecuniary damage or render it more easily bearable. Life, therefore, forced out the possibility of compensation for non-pecuniary damage, which had earlier been known in our law.
The point of departure of the reasons for the amendment was that the act causing damage could infringe the interests of the injured party also by causing non-pecuniary damage in addition to the pecuniary damage, whose impact could even be more severe than that of the pecuniary damage. It would therefore be unequitable to prevent a person sustaining such severe disadvantage from receiving compensational satisfaction merely because the damage he sustained could not be measured in monetary terms. Monetary compensation could be suitable to mitigate non-pecuniary damage. This, however, did not mean that it was possible

44 Civil Code Section 85(4)

to receive compensation for non-pecuniary damage in an unlimited manner in every case.
Compensation for non-pecuniary damage was permitted only in cases of more severe infringement when the damage made the injured party's social life and private life – taken either together or separately – increasingly difficult in a lasting or permanent manner. In other words, the condition of compensation could be found in the consequences of the damage sustained by the injured party.

By their nature, the range of events and consequences described were associated primarily with damage to life and limb, but infringement of other rights linked to person could also result in the possibility of claiming compensation for non-pecuniary damage. In addition to natural persons, legal entities could also claim compensation for non-pecuniary damage, if it had a disadvantageous influence on the participation of the legal entity in economic turnover.[45]

A new institution introduced by the 1977 amendment was press correction as a specific objective and restorative type instrument to protect one's reputation.[46] "The press correction is a specific instrument of personality protection, which is limited to a specific range of personality infringement, whose application is subject to separate conditions."[47]
Pursuant to the legal regulation, press correction may take place only if the infringement was done through some disclosure (allegation) in a newspaper, journal (periodic newspaper), radio, television or newsreel.

The enforcement of a claim for press correction is subject to personal objective and formal conditions. Only those may take legal action for press correction, who have the right to claim it. Both a natural person and a legal entity may enforce such a claim because by its nature protection is not limited exclusively to the person of man. The subject matter of the procedure is to order the publication of a corrective statement requested by the person whose rights were infringed.

45 Civil Code Section 354
46 Civil Code Section 79
47 Dr. Károly Törő: Személyiségvédelem a polgári jogban, Közgazdasági és Jogi Könyvkiadó, Budapest, 1979. p. 385.

The procedure was made possible through the enactment of a new Chapter XXI of law decree 26 of 1972 amending Civil Procedures before the 1977 amendment of the Civil Code. This law decree introduced the enforcement of claims for press corrections as a new institution and regulated it as a civil procedure.

Section 79 of the Civil Code stipulated by Act IV of 1977 regulated press correction in accordance with this principle as a specific instrument of personality protection, which could be applied to remedy the publication of untrue facts, spreading allegations or presenting true facts in a false light, in other words harm to good reputation as set forth in Section 78 of the Civil Code. The preconditions of its application include that the infringement be caused by culpable behaviour and the amount that could be awarded as compensation would not be proportionate to the severity of the culpable behaviour.[48] This possibility had already been a proven solution in terms of copyright protection.

III.

As the regulation presented above was rooted in the "soil of socialism" and it did not evolve from the principles of market economy, it would be useful to re-regulate personality protection in accordance with the European norms in force. Another argument for regulation is that during the period since the 1977 comprehensive amendment to the law, new questions have arisen affecting personality rights to which legislation has not yet responded.

To my mind, one of the most important issues raised is the freedom of information and data protection. The reason for this is that during the last decades of the 20th century, a new industrial revolution took place in the advanced regions of the world. The role of computer science and information increased substantially. The possibility to automate the processing of information has already exerted a substantial impact on many areas of society's life. Potentially, this holds additional risks.

48 Civil Code Section 84(2). Separate legislation, Ministry of Finance Decree 14/1978 (VIII.8.) provides for its use.

Regulation of information in general, and data protection in particular, is an important factor of civil well-being, as even the most intimate sphere of private life may become "data" in a computerised state, thus "there is a danger that unauthorised persons may have access to the data or that they are used for purpose other than what they were meant originally."[49]

The regulation of information has to stand for openly opposing interests as the free flow of information is a sine qua non of the efficient operation of society, while there are countless political, economic, business and other interests in conflict with the disclosure of information; the right to information may be at loggerheads with the right to informational self-determination.

The statement of the Constitutional Court concerning the personal identification number also throws lights on the significance of these problems. Legal regulation has to resolve these conflicts. The codification work on the regulation of information is at an advanced stage. Taking into account West European legislation in force, the goal of the bill being drafted is to "clearly determine the freedom and limitations of obtaining, processing and the flow of information and to determine primacy in the conflict of a person's right to informational self-determination and the right to have access to information and not only to render the relevant principles of the state's information policy public and mandatory, but to guarantee data subjects to have an appropriate say in developing them."[50]

An act corresponding to the above principles which takes into account established international legal practices could be a substantial step in the comprehensive codification work meeting the demands of a market economy.[51]

49 Géza Kilényi: Informatika, közigazgatás-jogi szabályozás, Valóság, November 1986
50 László Sólyom: adatvédelem és személyiségi jog. Világosság, January 1988.
51 Dr. Attila Péterfalvi: Amendments to Act LXIII of 1992 on the Protection of Personal Data and the Accessibility of Data in the Public interest in Tízéves az Adatvédelmi Biztos Irodája, Adatvédelmi Biztos Irodája, 2006.

Amendments to Act LXIII of 1992 on the Protection of Personal Data and the Accessibility of Data in the Public Interest – 1995-2005

The right to the protection of personal data and the right to have access to data in the public interest were elevated to the rank of constitutional fundamental rights by the Constitution of 1989 following the change in regimes. Thereafter three years were needed to enact the Data Protection Act and six years to inaugurate the commissioners safeguarding the protection of the constitutional fundamental rights. Although the process of the preparation of the Data Protection Act began in the mid-1980s and the government required the minister of justice already in January 1989 to submit the bill by the end of December 1990, Act LXIII of 1992 on the Protection of Personal Data and the Accessibility of Data in the Public Interest (hereinafter: Privacy Act) was promulgated only on 17 November 1992. The due date for the election of the commissioners (1 October 1993) lapsed without result. Although the President of the Republic gave a hearing to the nominees, their election in Parliament was unsuccessful. Finally, Parliament put the parliamentary commissioners in office on 30 June 1995.

Concerning the regulatory concept of the Data Protection Act, we always emphasised that a single act covers both data protection and the freedom of information which is unique in Europe and a single specialised ombudsman oversees the protection of these rights. The primary example during the work of codification was the 1981 Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data. In his report of 1997, the data protection commissioner wrote with some critical edge that it was not quite comprehensible why the ratification of the Convention took so long and why its promulgation was delayed as no fundamental issues of law harmonisation were encountered. Another factor playing a role in the prolongation of accession was that the Hungarian legislator was waiting for the enactment/adoption of sectoral data protection acts. This gave rise to a peculiar situation in that the Republic of Hungary had the obligation to apply the Convention under international law, but the promulgation of Hungarian legislation mandatory for the Hungarian subjects of law did not take place. It was promulgated only in 1998.[52]

52 The Republic of Hungary promulgated the Convention with Act VI of 1988, which entered into

1995-1999

In 1995, a directive directly applicable in the Member States of the EU was adopted in Brussels.
The purpose of the adoption of the directive[53] was to ensure the free flow of personal data within the borders of the European Union and their identical level of protection. Accordingly, Member States had three years to meet their legislative obligation for implementing and applying the directive. The directive limits the transmission of data to third countries outside the EU, classifying it as lawful only if the third country provides an adequate level of protection. In his 1997 report, the data protection commissioner poses the question – what will be our ranking as a country? "***Although presumably Hungary may expect to have the status of a 'well-bred third country' based on the current protection of rights until her accession to the EU that would still only result in a fairly inconvenient situation, so it is only to be hoped that with the accession we shall be rid of the third country label as soon as possible... I see no reason why Hungary cannot take a bold step and anticipate the requirements of accession.***"

The 1995-1996 report already contained the observations concerning the amendment to the Privacy Act, which had to be implemented with a view to complying with the directive. One important point, which is also one of the main deficiencies of the Hungarian legal regulation, is that it fails to distinguish between controller and processor. The external processing of personal data without the consent of the data subjects is unlawful. The purpose of the distinction applied in the directive is to enable the controller to use an external collaborator for whose activities the controller is, of course, responsible. Pursuant to the directive, the processor may process the data exclusively in accordance with the instructions of the controller and in compliance with the controller's data security requirements. Should the processor deviate from these, its liability according to the Civil Code can be established. The directive also urges that rules of ethics be elaborated for various data processing sectors/branches and encourages controllers to present their rules to the data protection authority. The

force on 1 February 1998.
53 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Hungarian data protection regulation only contains the principle of fair and lawful processing. It is also necessary to supplement the regulation concerning the processing of special data as pursuant to the directive such data may be processed if it is necessary for the protection of the legitimate interests of the data subject or another natural person and the data subject cannot give his consent because of his lack of physical or legal capacity. The directive also contains the notion of prior checks, meaning that certain processing operations have to be reviewed even before they begin in order to protect the rights of the citizens. It can be seen from this that the fundamental (and desirable) points of rendering the Privacy Act EU conform have been known since the establishment of the institution of commissioner. Legislation reacted somewhat more slowly since the Privacy Act was amended not once in a comprehensive manner, but several times and this process took nearly ten years. In his 1998 report, the commissioner urged repeatedly the performance of the tasks of law harmonisation related to the preparation of the accession process, i.e. the adjustment of the Privacy Act to the EU directive.

The first major amendment to the Data Protection Act took place in 1995. That was the year when Act LXV of 1995 on State Secrets and Service Secrets (Secrecy Act) and Act LXVI of 1995 on Public Documents, Public Archives and the Protection of Documents in Private Archives (Archives Act) entered into force. The Secrecy Act supplemented the powers of the commissioner by allowing him to initiate either narrowing or expanding the types of data specified under state or service secrets and if the classification of data was unjustified, he could call upon the classifier to alter or terminate the classification. Legal remedy against the commissioner's action can be sought at the courts, the classifier may resort to the Budapest Municipal Court which acts out of turn in a private hearing. The Archives Act amended the definition of data in the public interest. "***On the one hand, the range of agencies subject to the scope of the act became wider, and on the other hand, by omitting the usual 'elastic rule' the '***save as otherwise provided by law ***[...]' formula, which relativises every rule, the provision became more concrete and more closed. Accordingly, in addition to those listed before, agencies and persons performing other public tasks specified in legal regulation were also authorised to order the processing of data. The supplement to Section 19(2) prevented the evolution of a number of later legal disputes, which***

would have been difficult to resolve. Accordingly, the names and positions of persons taking action within the powers of these agencies are public data accessible to anyone unless otherwise provided by law."[54] Two new paragraphs were added to this same section. The above provision was extended to all the personal data related to the public task of the person acting in an official capacity and it declares that data prepared for internal use and data in preparation of decisions shall not be public for thirty years following their generation.

The next amendment of the Data Protection Act was made in 1999. Act LXXII of 1999 on the Amendment of Certain Acts related to the Processing of the Personal Data of Citizens amended the data processing rules of seven acts. The Privacy Act was supplemented with the rule, according to which the controller may entrust others with the processing of the data, naturally provided that appropriate guarantees are given. With this amendment, by delineating the responsibilities of the controller and the processor and incorporating the notions of data processing and processor into the act, the legislator partially adjusted the Privacy Act to the rules of the directive. Later, this provision was criticised in legal literature: "*Simultaneously with the introduction of the notion of the subject (the processor) into the act, the legislator – deviating from the set of definitions in the directive – deemed it necessary to define also the activity carried out by the processor which – through the restrictive interpretation of the law by the data protection commissioner and its impact on the novelties of 2003 – led to the fact that as of today the range of activities of the processor is very narrowly delineated in Hungarian law... So, the directive does not know the category of 'data processing'. The set of terms used in the Directive accurately reflects the situation that we are dealing with an activity (data processing) the person carrying out this activity being entrusted to do so is the data processor and the person who determines the purpose and mode of processing is the data controller – so we are not necessarily dealing with the separation of two subjects, but much more with the separation of two functions.*"[55]

The data protection commissioner gave his opinion on the draft law

54 Report of the data protection commissioner 1995-1996, p. 13.
55 dr. András Jóri: Adatvédelmi kézikönyv. Osiris Kiadó, Budapest, 2005, pp. 154, 157.

several times; most of his observations were accepted. Nevertheless, several provisions were left in the law which unjustifiably extend the mandatory processing of personal data. "*Such an aimless provision is, for instance, when it is mandatory to notify the population register about the fact that the ID card was confiscated from the data subject when he was taken into custody. Simultaneously with the amendment of the Privacy Act, the facts of the case regulating unauthorised processing was also modified in Act IV of 1978 on the Criminal Code. Presumably, as a result of an error of codification, the perpetrator of unauthorised processing is not to be penalised – he only may be penalised according to the amended Section 177/A of the Criminal Code, contrary to the rules based on the facts of the case of other criminal acts,.*"[56]

1999 was a significant year also with regard to the fact that the Data Protection Working Party of the European Union stated its opinion on the Hungarian data protection provisions, the level of data protection guaranteed by the laws. "*In its working study on the forwarding of personal data to third countries, the Working Party presented the requirements of the directive, which have to be complied with and listed the specific elements, which must be implemented when assessing the existence of an appropriate level of protection. What follows from the comparison of the rules of the directive and the Hungarian law is that Hungarian law, which applies the provisions concerning automated and manual processing taking into account the principles of the Council of Europe document referred to above, operates according to principles with regard to the protection of personal data and its mechanisms, which guarantee the level of efficient application of the principles.*"[57] Based on all this, the Working Party recommended that the European Commission and the Council determine that Hungary ensures the level of adequate protection required by the directive.

With its decision of 26 July 2000, the European Commission adopted the assessment and recommendation of the Working Party and regarding Hungary in its assessment as being equal to the EU Member States from the viewpoint of data protection, it gave the green light to forwarding personal

56 Report of the data protection commissioner 1999, p. 157
57 Opinion 6/99 of 7 September 1999 on the level of the protection of personal data in Hungary

data to Hungary. The existence of adequate protection was determined by assessing the legal system and the data transfer operations, taking the general and sectoral rules into account. The Commission established that the Hungarian regulations in force extend to compliance with all the principles necessary for an adequate level of protecting the personal data of natural persons. The protection of personal data is guaranteed by the Constitution and the Data Protection Act and sectoral laws also contain data protection provisions. The implementation of the legal provisions is guaranteed by the possibility of enforcing rights and the data protection commissioner elected by Parliament. The fact that Hungary qualifies as a country guaranteeing adequate protection and is treated equally as the EU Member States is a substantial recognition of Hungary's legal system and institution for data protection.

2001-2002

The work of codification envisaging the next substantial amendment to the Data Protection Act began in 2001. Based on the government's law harmonisation programme, the review of the Privacy Act was included in the legislative programme of the second half of 2001 in order to render it fully compliant with the directive. The technical materials produced in the course of preparing the bill were sent to the first data protection commissioner then still in office by the ministry in charge of the preparations at the end of March 2001. In view of the fact that it was not an elaborated draft law, the commissioner did not make any observations. In the meantime, Dr. László Majtényi's mandate expired. At the end of July 2001, the Ministry of Justice sent the draft of the law "***on the protection of personal data and the accessibility of data and information in the public interest***" to the parliamentary commissioner of citizens' right acting as deputy for the data protection commissioner. The submission contained a fundamental change of concepts. They wished to incorporate the rules governing the protection of personal data and those of access to data in the public interest into two separate acts; new terms were introduced in relation to the processing of personal data; a number of new tasks were specified for the data protection commissioner (participation in the assessment of automated individual decisions, the mandatory decisions of the commissioner acting as an authority), (blockage, erasure and

annihilation of data processed without authorisation) enforcing their execution; participation in the judicial review of the decisions; ex-ante control; information on new legal regulations affecting accessibility of data in the public interest and on judicial and other decisions).
The enactment of two independent acts was recommended based on the following reasons: amendment of the Privacy Act was necessary because of EU law harmonisation obligations; data protection and the freedom of information are both fundamental rights, which differ in content and occasionally vie with one another. The Hungarian regulation stipulates as a fundamental principle that personal data do not qualify as being in the public interest. The recommendation to regulate the two fundamental rights in separate acts aims to implement this principle more consistently; the regulation of access to information in the public interest in an independent act facilitates greater emphasis being laid on this fundamental right than before; separation is also warranted by the fact that owing to the identical terms, a clear interpretation of the law related to information in the public interest has not evolved over the past ten years, particularly in comparison to the protection of secrets.

A staff of the office of the data protection commissioner produced their observations related to the draft, which was presented to the competent parliamentary commission by the general deputy to the parliamentary commissioner for citizens' rights. The slit of the Privacy Act in force is not warranted, regulation by an independent act has no significance from the viewpoint of the enforcement of any fundamental right. "***Having a uniform interpretation of the law depends not on regulation by a separate law, but on the precision of the text of the law elaborated on the basis of the analysis of the interpretative activities of the Constitutional Court, the data protection commissioner and the courts of justice. The legal practice of the data protection commissioner is uniform and consistent, and it is also in compliance with the relevant decisions of the Constitutional Court [...]***"[58].
The draft included elements which failed to comply with the constitutional

58 Quotation from the Observations drafted by the Office of the Data Protection Commissioner

principles of the restriction of fundamental rights, the provisions of the decisions of the Constitutional Court and with regard to the subject matter of regulation, the provisions should be incorporated into sectoral acts rather than into the Data Protection Act. The main tenets of the draft – expanding the procedural authorisation and powers of the data protection commissioner, but without financial and personnel conditions – did not seem to be acceptable and well-grounded in this form at the time. The commissioner stated in his 2001 report that "*under current conditions, the Privacy Act in force for almost ten years is time-proven and may be an exemplary piece of legislation also for the legislators of other countries; nevertheless, it is favourable from the viewpoint of the protection of personal data and the accessibility of data in the public interest that preparation for the re-regulation of the Privacy Act has begun based on the experience collected in applying the law and with regard to the requirements of EU accession*".[59]

In 2001, the data protection commissioner made recommendations for an important legal regulation to the legislator with a view to enforcing data protection and the freedom of information.

"*Summarising the experiences of about six years, the data protection commissioner stated that the right to the protection of personal data and the protection of the freedom of information under the criminal law are not enforced to the desired extent because of the deficiencies of regulation. The provisions of the Criminal Code related to these two fundamental rights draw the boundary of culpability too broadly on the one hand, in other words, acts are ordered to be punished action against which does not require the instruments of the Criminal Code and, on the other hand, terms are used which do not comply exactly with the theoretical scheme of the data protection law.*"[60] The commissioner recommended to the minister of justice that only those unlawful processing of data should be sanctioned by the Criminal Code, in the case of which this is absolutely warranted. The acts thus excluded from criminal liability should qualify as petty offence. In order to create a uniform judicial practice, the terminology of the Privacy Act and of the Criminal Code should be aligned; he also

59 Report of the data protection commissioner 2001, p. 150
60 Report of the data protection commissioner 2001, p. 153

recommended that criminal acts involving personal data and data in the public interest should not be dealt with within the same section of the law. After this, the legislator relaxed the excessive rigour of the facts of the case in the Criminal Code, but failed to establish the legal conditions for sanctioning acts of petty offence excluded from criminal liability. So, in 2003, the commissioner approached the minister of the interior again, initiating an amendment of the legal regulation in order to provide for the possibility of taking action according to petty offence law in the case of minor infringements of the protection of personal data. In the course of the investigation into data processing related to the Internet, the commissioner recommended to the legislator to amend the Privacy Act in terms of the regulation of forwarding data abroad, harmonising it with the provisions of Directive 95/46/EC. With a view to establishing the freedom of electronic information, it should be stipulated that a specific range of data in the public interest should mandatorily be published or made accessible also in an electronic form. A legal possibility of defence against hackers should be introduced, unsolicited business messages should be regulated and the framework for the lawful processing of turnover data should be established.

The review of the Privacy Act and its harmonisation with the directive was included again in the government's working programme for the second half of 2002[61]. Following a wide-ranging technical reconciliation, the first version was revised at several points, but the enforcement of the two fundamental rights was recommended to be regulated still in two separate acts instead of a single one as before. When providing an opinion on the draft law, the position of the data protection commissioner was that "*The terminological culture and certain rules of the draft law under preparation will certainly have a developing impact on the law, but the draft fails to give an answer of merit to the question of why it is necessary to incorporate the rules pertaining to personal data and the accessibility of data in the public interest in two separate acts, putting an end to the proven and internationally acknowledged mode of the Hungarian regulation, namely that it regulated data protection and the freedom of information in a single act, with regard to each another. We also objected to the fact that misunderstanding the relevant Community directive,*

61 Government Decree 2099/2002 (III. 29.)

the draft wished to break with the regulatory logic of the Privacy Act to date, which bore in mind the constitutional conditions of restricting fundamental rights, according to which the sectoral law determining the types of data and data subjects, or the consent of the data subject may create the legal basis for the processing of personal data.[62]"

The idea of enacting two separate laws was included in the various drafts on the amendment to the Privacy Act until 2003. Although the Data Protection Commissioner's Office and then, from 2002, the data protection commissioner did not regard this as warranted and legally grounded, the legislator was not convinced by arguments and the prepared technical documentation. A highly thorough and consequently highly time intensive work of codification would have been needed for the enactment of the two separate acts, which was rendered impossible by the plethora of tasks related to EU accession and the tight deadlines. It should, however, be mentioned that in essence this bill was the basis and point of departure for all that finally resulted in the substantial amendment of the Privacy Act in 2003.

2003-2005

As far as legislation was concerned, 2003 was the year of data protection and the freedom of information. Following lengthy preparatory work and multiple reconciliations and revisions, the amendment to the Data Protection Act was adopted together with the Secrecy Act as a result of several years of legislative process and the so-called Glass Pocket Act also entered into force.

The amended Data Protection Act[63] primarily expanded the chapters concerning the processing of personal data and the data protection commissioner, adding new notions and rules. Taking the provisions of the directive into account, it was justified to accurately specify the personal, objective and territorial scope of the Privacy Act. Thus, the scope of the act extends to all data processing carried out in Hungary, irrespective of the citizenship, place of residence or registered offices of the controller or

62 Report of the data protection commissioner 2002, p. 128

63 Act XLVIII of 2003 on the Amendment of Act LXIII of 1992 on the Protection of Personal Data and the Accessibility of Data in the Public Interest

the processor. The provisions of the act have to be applied to equally to processing carried out using IT devices or manually, but it does not extend to data processing by natural persons serving their own purposes.

The new provisions of the Privacy Act extended the range of special data – which had been categorised here based on the legal practice of the data protection commissioner to membership in a trade union as this could also refer to political opinions. In terms of the second group of special data (data concerning health, addiction, sexual life) the new act takes into account the position of the Data Protection Committee of the Council of Europe and instead of referring to special data concerning criminal records, it speaks about criminal personal data. These include the data related to the data generated by the agencies authorised to conduct criminal procedures and to investigate criminal acts, as well as by the penitentiary agencies concerning the data subject, as well as data concerning criminal records.
The act introduced a new term, data accessible on the grounds of public interest, which means data other than data in the public interest, processed by natural persons, legal entities or organisations not having a legal personality and access to which is ordered by an Act of Parliament on the grounds of public interest.

As a main rule, the Privacy Act links the processing of personal data to the consent of the data subject or a provision of the law, but it did not contain any guidance on the consent or making statements. In his case law, the data protection commissioner consistently enforced and applied the rule of the directive, according to which the consent of the data subject to the processing of his data must be voluntary, deliberate and based on informed consent. The amendment introduced this provision into the act. The data subject has the right to object to the processing of his data and may request the termination of processing or the erasure of his data.

The act specifies when in particular a data subject can be regarded as identifiable: he is directly or indirectly identifiable based on name, identifier, one or more factors characterising his physical, physiological, mental, economic, cultural or social identity. The amendment introduces an additional requirement for lawful processing, namely that in the case

of mandatory processing, the law or municipal decree has to define the range of the processed data, their accessibility, the purpose, the conditions and the period of processing, as well as the person of the controller. As of 1 January 2004, with a view to compliance with the directive, personal data, including special data, may be processed if it is necessary to protect the legitimate interests of the data subject or another person, or for the prevention of disaster or emergency and if the data subject is unable to give his consent because of his physical incapacity. The act also provides an opportunity for the data subject to set forth all the essential facts and circumstances concerning the processing of his data, its mode, period and purpose in the contract concluded with the controller. The contract must unambiguously contain the written consent of the data subject to the processing of his data.

Following the amendment of the Privacy Act, the contract of assignment between the controller and the processor concerning the processing of data must be incorporated in writing. As to the content of the contract, the general terms and conditions of contract specified by the Commission of the European Union must be taken into account, particularly in the case of assigning processing to a processor outside the EU. Another important rule is that the scope of the Privacy Act also extends to the cases when a controller outside the territory of the European Union assigns the task to a processor in Hungary. In such cases a representative must be designated in Hungary.

In accordance with the directive, the Privacy Act was supplemented with the general list containing the cases when personal data may be processed in compliance with the requirement of purpose limitation. Thus, in particular, it is possible to do so if it is necessary for the performance of a task in the public interest, or legal obligation for the performance of the official task of the controller, for the protection of the legitimate interests of the data subject, the performance of contract between the data subject and the controller or the lawful operation of social organisations.

To meet the requirements of the directive, the act stipulated that only state or municipal bodies may process criminal data for the purposes of prosecution and crime prevention, public administration and the

enforcement of the law, as well as files concerning petty offences, civil lawsuits and extrajudicial affairs.

The data subject is entitled to the right of self-determination with respect to his data, he himself may decide whether to provide them, he may request the rectification of his inaccurately recorded data and with some exceptions, the erasure of his data. Following the amendment of the Privacy Act, the data protection commissioner (and the court) may order the erasure of personal data. The data subject must be notified of the rectification and the erasure. The notification may be waived, if in view of the purpose of processing it does not violate the legitimate interests of the data subject. Only an Act of Parliament may restrict the rights of the data subject. Following Hungary's accession to the European Union, a law may provide for the restriction of the rights of data subjects with a view to the protection of the significant economic or financial interests of the European Union.

With a view to harmonisation with the directive, objection against the processing and forwarding of data was introduced into act as a new provision. This is possible, if the processing only serves the interests of the controller or the third-party recipient; the purpose of the use/forwarding of data is for direct marketing, public opinion polls or scientific research; the act enables the data subject to exercise the right to objection. The Privacy Act was supplemented with the rules of exercising the right to objection by specifying the periods open for procedural action and the obligations of the controller. If a data subject is unable to enforce his rights vis-a-vis the controller, he may turn to the courts.

Although there had been earlier examples of controllers requesting the opinion of the commissioner prior to the commencement of their activities, this became mandatory after 1 January 2004 in the cases specified in Section 31 of the Privacy Act. For certain major controllers (national registers of the authorities, labour registries and criminal registries affecting a wide range of citizens and the client data of financial organisations, public utilities and telecommunication service providers among the actors of the market sector), the act requires that the data protection commissioner must be notified of the processing of new

data sets or the use of a new processing technology 30 days in advance, who, if he so decides, may check the processing prior to its actual commencement. The commissioner may call upon the controller to alter the range of data to be processed, or the method of processing based on his audit. If after the commissioner's review the processing is qualified as unlawful and the controller does not terminate it, the commissioner may order the blockage, erasure or annihilation of the data, and he may prohibit unauthorised processing and suspend the transfer of the data abroad. The controller or processor concerned may go to the court against the decision of the commissioner, but the processing must be suspended and the data must be blocked until the decision of the court.
However, the act leaves a number of important questions unanswered. The procedural rules, on the basis of which the commissioner may exercise his powers as an authority, are not specified. There are no requirements either of content or form with respect to the mode and form of ordering, prohibition or suspension. This would, however, be indispensable in the case of a quasi-authority. It is also questionable what will happen, if the controller neither terminates the unlawful processing, nor turns to the court as the commissioner has no additional powers apart from ordering (he cannot impose a fine or call for enforcement). The act also fails to provide for the type of procedure under which the court should deal with the case. In 2004, the controller turned to the court in two cases. One controller subsequently waived his petition, while in the other case the procedure is still in progress. The litigation was started on the grounds of the infringement of rights related to person in accordance with the general rules of the Act on Civil Procedure; the controller was the petitioner and the data protection commissioner protecting the rights of the data subject was the respondent. The review and the amendment of this provision is indispensable so that the court procedure should be conducted in accordance with the rules of administrative litigation in these cases.

The agencies and companies listed in the Privacy Act must appoint an internal data protection officer, and draw up their privacy policy. State and municipal controllers subject to the obligation to register in the data protection register must prepare their privacy policy.

In April 2003, the Parliament adopted the package amending 19 acts, widely known as the glass pocket act[64]. The goal of the act is to ensure the accessibility, transparency and control of the use of public funds and public property. In the course of the multi-round professional debate, all the observations of merit of the data protection commissioner were incorporated in the draft. The act (and its implementation decree) constituted substantial progress in the field of the freedom of information as the legislator resolved the contradiction between the protection of business secrets and the accessibility of data in the public interest; by introducing the institution of data accessible on grounds of public interest, the freedom of information was extended to the organisations of the private sector having financial or business relationships with general government, the disclosure obligation in a website applies to a wide range of data in the public interest related to general government; all the organisations within general government must entrust a person or organisation having appropriate expertise to carry out the tasks related to the disclosure of data in the public interest.

Ministers and chapter owners must draw up action plans in order to provide credible and easy to understand information to citizens and to examine the possibilities available for disclosure; they have to put forward recommendations for the amendment of legal regulations, in which the disclosure obligation of specific data in the public interest is justified to be required and, finally, they have to negotiate with the minister of finance about supplementary funding necessary for the implementation of these tasks.[65]

As a result of several years of preparatory work, the amendment to the Act on State and Service Secrets entered into force in 2003.[66] In the context of accession to the European Union, it became necessary to transform

64 Act XXIV of 2003 on the amendment of certain Acts related to the use of public funds, the publicity, transparency and expansion of control of the use of public property

65 Following the entry into force of the Glass Pocket Act, the Government enacted Government Decree 95/2003 (VII. 15) on the amendment of Government Decree 217/1998 (XII. 30) on the order of operation of general government and Government Resolution 1096/2003 (IX. 11) on certain tasks stemming from the Glass Pocket Act on the use of public funds, the transparency of the use of public property and the extension of its control and those serving the modernisation of the IT and operational system of general government.

66 Act LXV of 1995 on Government Secrets and the Service Secrets, and in relation to it, Act LIII of 2003 on the Amendment of Other Acts.

the system of classifications to introduce the four-level, harm-based classification system, the elimination of automatisms in classification, and the adoption of the EU classification markings into the Hungarian legal system. The EU did not regard embracing a large quantity of highly classified data as justified, and because of this, all those legal regulations, which suggested such a classification automatism had to be repealed. The number of the types of secrets does not change with the introduction of the four-level, harm-based classification and marking system, but more levels of protection will be available, and state secrets will be assigned the "Top secret" marking. The classifier decides on classifying data as state or service secrets and on choosing the classification marking best warranted relative to the value of the data to be protected from the package of protective measures, providing for a more flexible instrument for the required protection proportionate to costs. According to the position of the data protection commissioner, certain amendments to the text of the bill, which were drafted virtually in the last minute, were objectionable from the viewpoint of the accessibility of data in the public interest and led to an internal contradiction in the regulation of secrets. "*The annulment of the provisions requiring automatic classification was a conceptional element of the correction of the regulation of secrets. This appropriate goal was, however, only partially achieved. Parts resulting in 'ex lege' classification remained in Act CXXV of 1995 on the National Security Services (National Securities Act). These include Section 30(4), Section 42(1) and the template of the questionnaire used for national security checks in the annex to the National Security Services Act.*

The Annex to the Secrets Act superfluously specifies criteria governing the use of the 'top secret' marking assigned to government secrets because this, and only this, marking has to be applied to all government secrets. It may lead to problems in the application of the law that the criteria governing the classification marking of government secrets are not in line with the legal definition of government secret. The confusion in the internal coherence of the regulation may prevent the classification of data as government secrets, in the case of which the constitutional conditions of restricting accessibility prevail.

It is dubious whether the service secret is suitable to fill in the role of 'weak government secret' intended according to the legislators' conception

because the difference between government secret and service secret is still not that of grade, but that of quality, in view of the different subject matter of direct protection."[67]

In 2005, one of the reasons for the amendment to the Data Protection Act was the anti-constitutional omission established in relation to the regulation of "***data generated for internal use and related to decision-support***" and its correction. In its decision 12/2004 (IV. 7.) AB, the Constitutional Court stated that the legislator failed to provide for the guarantees offered by the rule of law needed for the legislator to restrict the fundamental right of access to data in the public interest only to the extent that is constitutionally acceptable in relation to materials created for decision-support and for internal use. For the majority of the documents related to cases, the restriction of access to data in the public interest guaranteed by the Constitution in the interest of decision-support is no longer warranted once the decision is made. The notions and data sets of "***related to decision-support***" and "***generated for internal use***" as included in the Data Protection Act are inaccurate and unspecified, their application constitutes the unnecessary and disproportionate restriction of the freedom of information as a fundamental constitutional right. In this context, the Constitutional Court expounded that the legislator failed to distinguish the restriction of public access to data related to decision-support before and after decision-making as it suffices for the controller to state that the data are related to decision-support or they were generated for internal use. The fact in itself that the data were generated in the course of the everyday work of an agency discharging a public task, or in relation to the preparation of decisions by that agency does not adequately warrant the blocking of the data in the public interest from access. When evaluating documents/materials created for internal use, subjective criteria may also arise because the data are protected not on account of its content, but on account of the intention of its creator. "*The restriction is warranted, on the one hand, if it is permitted by Section 19(1)-(3) of the Privacy Act and, on the other hand, if the disclosure of the data in the public interest threatens the discharge of public tasks, or the discharge of a public task exempt from external influence. The criteria of convenience of agencies and persons discharging public tasks cannot have priority over a fundamental right. Section 19(5) of the Privacy Act meets the requirements of the Constitution only if the legislator clarifies the purpose*

67 Report of the data protection commissioner 2003, p. 165

of restricting the freedom of information, the data set blocked from public access is confined to a reasonable level and access to data in the public interest is restricted only to the necessary and proportionate extent."[68] It is an additional problem that according to Section 19(5) of the Privacy Act the restriction of public access may be upheld for an indeterminate period, because its duration is to be calculated from the processing of the data (the continuous storage of the data also qualifies as data processing). The Constitutional Court established in its decision that the legislator failed to provide for an actual, substantive review of the restriction of public access and thus the possibility for an effective legal remedy by the courts. Pursuant to the Privacy Act, a review by the courts extends only to a review of the formal criteria set forth in the legal provision. "***The absence of the compelling reasons for restricting public access and of the legal remedy aimed at its review allows for the unjustifiable restriction of access to data in the public interest, in other words, of the constitutional right to accessing data in the public interest at the controller's discretion .***"

The amendment of the Data Protection Act in 2005[69] was justified by the decision of the Constitutional Court referred to and the elimination of the anti-constitutionality manifested in the omission. At the same time, it provided an opportunity to clarify the notions related to processing/accessing data in the public interest and the inclusion of rules concerning the powers and procedural authorisations of the data protection commissioner.

The Act clarified the definition of data in the public interest. It made it clear that any knowledge, recorded information on any kind of the data carrier, irrespective of the mode of processing or the independent or collective nature of the data, qualifies as data in the public interest. The notion of the data accessible on grounds of public interest was changed: it includes all data not covered by the notion of data in the public interest, whose publication or accessibility is ordered by law.

The right to access data in the public interest can be restricted in view of the court procedure; following the amendment of the Privacy Act,

68 Constitutional Court Decision 12/2004 (IV. 7) AB

69 Act XIX of 2005 on the amendment to Act LXIII of 1992 on the protection of personal data and the accessibility of data in the public interest.

this restriction also extends to the procedure of public administrative authorities.

Following the amendment of the act, the Privacy Act qualified the personal data of persons discharging public tasks related to their responsibilities as data accessible on the grounds of public interest and rendered such data accessible to anyone, similarly to data in the public interest. At the same time, certain data continue to be inaccessible in the case of civil servants and public employees (such as, the civil service and public employment registers). The reason for this is that the "act" included in the definition of data accessible on the grounds of public interest does not refer the Privacy Act and neither the Civil Service Act, nor the Public Employees Act provide for the disclosure/accessibility of these data.

The Act provides a definition for the content of the range of data that are subject to automatic restriction of access, when it allows for the restriction of access to data generated prior to decision making and used as a basis for that decision for a period of ten years within the powers and authority of an agency or person discharging public tasks.. The phrase 'as a basis for that decision' refers to the purpose of the generation or recording of the data, thus its applicability does not depend on whether a decision has actually been made relying on the data used as a basis for it. According to the act, the head of the agency may reject the request for access after decision making only if he can demonstrate that access to the data would jeopardise the order of legal operation of the agency or discharging its tasks free of unauthorised external influence.

Pursuant to the act, anyone may submit a request to access data in the public interest in any form (orally, in writing or electronically). Access to data in the public interest published electronically may not be subject to registration, only the personal data, which are technically indispensable, may be processed. Based on the principle of purpose limitation, in the case of requests only those personal data may be processed which are required for the payment of the costs and meeting the request.

The act also clarified the powers of the data protection commissioner. Pursuant to the Privacy Act, he represents the Republic of Hungary in

the joint data protection supervisory body of the European Union. The amendment of the act clarified the hitherto unsettled procedural issue, namely that the data protection commissioner brings a decision following the inquiry related to personal data processed without authorisation and a court review of his decision can be initiated in accordance with the rules of the Act on Civil Procedure pertaining to administrative litigation.
By regulating the freedom of electronic information by law in 2005[70] (Freedom of Electronic Information Act), citizens were empowered to have access to data in the in public interest more simply and efficiently. The act specifies the obligation for the electronic disclosure of data in the public interest and data accessible on the grounds of public interest and its content, it renders legislation more open with the help of the Internet, it makes the digital version of legal regulations accessible and it establishes the possibility of accessing the anonymised decisions of the Supreme Court and of the courts of appeal.

The provisions of the Freedom of Electronic Information Act enter into force gradually in order to give sufficient time to all the agencies/organisations subject to the act for preparation. The agencies named in the act have the obligation to maintain an Internet website and to keep information in the public interest published there up-to-date. Electronic disclosure has to extend to all the data, which enable contacting the agencies that discharge public tasks, the use of their services and the transparency of their operation/financial management. Naturally, the disclosure obligation does not exempt the agencies discharging public tasks from rendering the requested data available to the applicant in the case of a request for the issue of individual data in the public interest.

To create transparency in legislation, the act requires the ministries preparing bills to publish the bills in their websites, indicating the status of reconciliation. There are certain objects of regulation and interests that are more important than the transparency of legislation where disclosure may be waived; these, however, are named by the act. Citizens using the Internet cannot be expected to be in the know about which ministry prepares which bill, hence the database of bills has to be published in the government's portal.

70 Act XC of 2005 on the Electronic Freedom of Information

The third area regulated by the Freedom of Electronic Information Act is ensuring the accessibility of legal regulations, which is implemented by making the authentic text of legal regulations accessible to anyone through the Internet. The act requires the publication of Magyar Közlöny and the journals of the various ministries via the Internet. In order to be able to learn about the practical application of the published legal regulations and the legal practices of the Supreme Court and the courts of appeal, the decisions of merit in cases, which they tried have to be made accessible electronically (the act exempt certain decisions from the obligation to publish). Access to the published decisions cannot be restricted, but with a view to protecting the right to informational self-determination and personality rights, the published decisions must be anonymised.

Data protection and freedom of information as reflected by human rights – 2007

In 2007, as a conclusion of my tenure as data protection commissioner, I addressed Parliament presenting the new approach to information rights[71] entitled ***Data protection and freedom of information as reflected in human rights*** on Human Rights Day (10 December):

"Naturally, it is an impossible undertaking to give a full review of the right to the protection of personal data and the right to access data in the public interest, ultimately of data protection and freedom of information as human rights in twenty minutes, so only the most important "evidence" can be presented to verify the statement. First and foremost, allow me to reflect back on the roots of the two human rights included in the title, because the formulation of honouring the individual and the community has preoccupied public thinking since ancient times.

The Laws of Moses, the Ten Commandments received from the Creator contain the fundamental but nevertheless unassailable rules of the man-to-man relationship. In the New Testament, Matthew in his Gospel puts forward the classical truth also referred to as the golden rule: "So in everything, do to others what you would have them do to you".

71 Dr. Attila Péterfalvi: Adatvédelem és Információszabadság az emberi jogok tükrében, In: az ombudsman intézménye és az emberi jogok védelme Magyarországon, pp. 29-38. Országgyűlési Biztos Hivatala, Budapest, 2008

Among the legal scholars of Rome, Ulpian and Justinian believed that the commands of the law was: to live honourably, not to harm any other person, and to render each his own.
Cicero was resolved in declaring that the moral order was regulated by natural law. "True law is right reason in agreement with Nature; it is of universal application, unchanging and everlasting; it summons to duty by its commands, and averts from wrong-doing by its prohibitions.. (...) It is a sin to try and alter this law, nor is it allowable to attempt to repeal a part of it, and it is impossible to abolish it entirely.."

The notion of moral natural law (lex naturalis) appeared as early as in ancient Greek philosophy. The sophists were the first to distinguish itemised human law from law regarded as rightful by nature. "Our most important goal, Chrysippus wrote, is to live in harmony with nature, both with our own and with that of the universe, doing none of the things which the common law of mankind is in the habit of forbidding, and common law being identical with *orthos logos* which pervades everything.

St Augustine traces the notion of natural law and natural law regulating moral order back to the eternal law, to God. According to his work on Free Will, the principles of natural law are known to all: "Everyone shall be given his due, the wretched shall be subordinated to the valuable and justice shall be honoured."
"Natural law is nothing other than the light of the mind flowed into us from God. Thanks to this light, we recognise what we need to do and what we have to avoid. God gave us this light and this law upon Creation." This latter thought comes from St Thomas Aquinas, which then appears in the catechism of the Catholic Church: according to their teaching on natural moral law "Natural law (...) is inscribed and carved into every single human soul because it is the human mind itself, which obligates to do good and prohibit sin. This requirement of the human mind however would not have the power of law, if it was not the voice and interpreter of a higher mind to whom we have to subordinate our mind and freedom."

After such antecedents, the Corpus Iuris Canonici also declares that "no one shall have his good reputation, which he deserves, unlawfully impaired, nor shall he have his right to the protection of privacy restricted."

This spiritual-intellectual heritage permeates later legal thinking, so that the general expectations be incorporated in constitutions and human rights charters centuries later. Although the protection of personal data and the freedom of information were not expressly included in the earlier documents, their germs can definitely be found. Legal development in Hungary also shows a very gradual evolution in this field.

Although a reduced form of data protection – according to which computerized data processing may not infringe the rights of persons – was incorporated in the Civil Code as early as in 1977, legal protection has not become a living practice. In any case, it directed attention to the fact that the spreading of computers involved new dangers.

After the change in regimes, Hungarian society had to become acquainted again or rather had to start becoming acquainted with fundamental rights. People felt the absence of a number of fundamental rights on their skin, such as the restriction of travelling abroad, the curbing of the possibilities of association and assembly with Draconian stringency.

Following the change in regimes, Eastern Europe also moved towards constitutional democracy. The defunct communist dictatorships were replaced by democratic constitutional states, whose internal order was determined by the supreme law of the country, the Constitution. When fundamental rights were incorporated in the Constitution, the state appeared both as addressee and as obligee, as guarantor at the same time, because on the one hand, it protects the freedom of the individual against the unlawful intervention of the state, and on the other hand, it provides appropriate orientation for developing legal order. There is multifaceted interaction between the two functions.

According to the classical liberal approach, fundamental rights are first and foremost rights of protection, which obligate the state to negative action or, to put it more accurately, to refrain from all action. With the process of

the liberal state being transformed into a social state, the emphasis on the positive nature of the fundamental rights important to the community increase in parallel. The so-called rights of protection in subjective public law protect the personality carrying the fundamental right against both the state and the non-state. The reason for this is that the state's monopoly of power deprives the individual of effective protection apart from the specific case of lawful self-defence.

The fact that the private sphere has become the central category of personality protection is no accident, because in the modern age this is the area which remained under the sovereignty of the individual and which he tries to protect from all external intervention.

The relationship between the Hungarian regulation of the two freedoms corresponds to the theory of the positive and negative notion of freedom referred to above, which could be characterised more accurately by saying that privacy, the protection of personal data means the negative, the protection of freedom from something, while freedom of information is the positive, the freedom to do something.

The "counterpart" or complementary of the right to the protection of personal data is the principle of the accessibility of data in the public interest. Modern legal regulation ties these two areas together in order to express their bond and their common role in the maintenance of a democratic informational equilibrium on the one hand, and in order that exercising one right should not be able to provide grounds for referring to the exemptions of the other, on the other hand, if this is contrary to the purpose and spirit of the regulation. Let us put it this way: personal data are the data of the individual, while the data in the public interest are the data of everyone. In the first case, the right of protection and in the second case, the right of access are self-evident.
In its decision 34/1994 (VI. 24.) AB on the freedom of information, the Constitutional Court declared that "this fundamental right therefore enjoys – in the context of the evaluation of the constitutional constraints – at least as much constitutional protection as the 'parent right', the freedom of expression. Open, transparent and controllable activity by the public powers, in general the operation of the state agencies and of

the executive power in front of the public is one of the cornerstones of democracy, the guarantee of constitutional state. Without the proof of the public, the state becomes a 'machinery alienated' from its citizens, its operation becomes incalculable, unforeseeable and expressly dangerous because the lack of transparency in the state's operation constitutes a particular threat to constitutional freedoms."

In the years of socialism, the model enforced was that of the transparent citizen and untransparent state; an absolute turnabout of this was needed. This led to the adoption of the Privacy Act.

Upon the change in regimes, new rights appeared on the horizon. We had to start the study of the catalogue of fundamental rights from the very beginning. During the period of Soviet occupation, this catalogue continued to expand beyond the iron curtain and was supplemented with rights, which were practically unknown to everybody in the eastern bloc apart from the theoretical scholars of legal science.

Hence, society had to become acquainted with new rights, such as the data protection and the freedom of information. Learning what in fact this would change in people's everyday lives was gradual.

The Constitutional Court deducted the right to the protection of personal data from human dignity. It defined the right as a right to informational self-determination; according to the interpretation of the Constitutional Court, the essence of the right to the protection of personal data was that the data subject himself had disposal over his personal data. Law may, in exceptional cases, order the mandatory processing of personal data, but only within stringent constitutional constraints. In this specific context, the requirement to protect human dignity can perhaps best be formulated, if we demand that the data subject should throughout remain the subject and not be the object of the processing of the data linked to him. This requires the obligation to provide information and a fair exercise of the rights on the part of the controller, while the data subject has the right to obtain information on the processing, he has the right to rectify erroneously recorded data and he may initiate the erasure of unlawfully stored data from the controller.

The definition of the place of the freedom of information among fundamental rights was first included in the 1992 decision of the Constitutional Court, according to which "the freedom of expression has an outstanding role among the constitutional fundamental rights, in fact it is the 'parent right' of several kinds of freedoms, the so-called fundamental rights of 'communication'. The specifically named rights stemming from these include the freedom of speech and the freedom of the press, which embraces the freedom of all media as well as the right to be informed, the freedom to obtain information."

As my colleague Zsuzsa Kerekes put it: "Substantive and procedural guarantees of the right to be informed, i.e. the freedom of information, is built up by the state primarily elsewhere in the case of access to the data, not particularly with respect to the press but to anyone." Here appears the germ of the idea that the freedom of the press and the freedom of information are different constitutional rights because the former is a classical freedom (freedom from state intervention), while the latter is the right to something. the right to having access to information held by the state. However, the exploration of the content of this difference was not carried out in the subsequent practice of the Constitutional Court. Since the entry into force of the act in Hungary, freedom of information means that everyone has a subjective right to access data in the public interest.

Adoption of the Data Protection Act constituted a radical change in public access to public affairs because it terminated the information monopoly of the press by requiring listed agencies to disclose data in the public interest upon the request of anyone. As this right is due to everyone, the restriction of the freedom of the press may be concomitant with restricting the right to expression, but it is not related to the freedom of information, i.e. the right to access data in the public interest.

Therefore, freedom of information guarantees the requirement of the transparency of the state, while data protection provides for the protection of citizens against the state and others. Today, both these values are both building blocks of the modern constitutional state.
What is the role of the data protection commissioner in this and how did his function change since the birth of the institution?

As László Sólyom put it in his welcoming address written for the spring conference of the European Data Protection Authorities organised in Budapest in 2006, "the data protection commissioner has been the democratic depositary and developer of data protection in Hungary at all times. This entity undertook the most conflicts with government agencies and other powers and with every one of these battles contributed to making people aware of data protection and the right to access files and made the importance of these freedoms obvious." Among the other commissioners, the data protection commissioner has to undertake a particularly active role, which the President of the Republic described as the "passionate will to enforce the rights of data protection and freedom of information able to survive even under the consolidated conditions of a constitutional state, which so much characterised the age of heroes preceding democracy. Or, to sum it up from the opposite side: this is the area where the attitude, which has regard only to its own official or business interests keeps on living in the most undisguised, even deliberate manner which, conscious of its presumed right, does not recognise the people's fundamental right to human dignity from which the rights to data protection and to access information directly stem."

This statement was made in view of the experience from practice, even though originally the data protection commissioner was intended to have the role of a classical ombudsman. This, however, failed at the very beginning, because as the other ombudsmen may investigate only the work of the authorities, the data protection commissioner may check every data processing. And "every" covers the whole of public administration and the private sector.

Providing an opinion on bills has been among the tasks of the office right from the start. Here, we can report on significant development too, as the number of commented bills has been increasing continuously and with it, the significance of this activity is also reinforced. In the welcoming address referred to, the President of the Republic underlined that "in Hungary, where there is no control by the constitutional court in specific cases, the recommendations of the Hungarian data protection commissioner generated a case law, which provides detailed guidance for the interpretation of the fundamental rights to data protection

and the freedom of information. The commissioner also provides an opinion on the bills affecting his scope of operations. This activity may be set circumspectly in parallel with preliminary judicial review by the Constitutional Court."

Our accession to the European Union also necessitated the additional reinforcement of the responsibilities of the data protection commissioner. The EU Directive on data protection requires that an independent authority monitor the enforcement of the right to the protection of personal data. It also stipulates that he should be able to enforce his decisions through decisions of the authority with a view to protecting the rights of citizens, if necessary. If the addressee of the decision does not comply with the decision voluntarily, the decision of the data protection commissioner may be enforced similarly to other administrative decisions and it may be attacked in front of a court.

This is another peculiar role because the data protection commissioner or rather the office of the data protection commissioner has thereby become an authority with administrative powers, which is not included in the initial instrumentarium of the ombudsman. It should be mentioned that only two such decisions were made over the past years, so it has not really become reality that the work of the data protection commissioner would have the nature of an authority.
To illustrate to what extent the responsibilities of the data protection commissioner have changed relative to the original idea, let me refer to the concomitant factors of joining to Schengen zone.

Schengen is a small wine-making town in Luxembourg close to the German-French-Luxemburg triple point border. Its name became known when Germany, France and the Benelux states executed the Schengen Agreement on board the Princess Marie-Astrid anchoring just there on the River Moselle crossing the town on 14 June 1985. The Schengen Agreement was about the full termination of customs and passenger traffic controls on the border and about the introduction of extra freedoms relative to the acquis communitaire.

On 19 June 1990, the Agreement was expanded with the Schengen Convention implementing the Schengen Agreement, which determines the process of implementation.

Due to the Maastricht Treaty of 1992, internal and judicial affairs also became part of the policies of the European Union, while the Amsterdam Treaty of 1997 corrected the cumbersome decision-making process and transferred a number of issues under the Community pillar; this is when cooperation under Schengen also became Community policy, at the same time, the Schengen Information System (referred to as SIS in the jargon) has remained within the intergovernmental framework.

SIS is a system for registering persons and objects that are wanted, which makes up a European network built on the independent national data bases of the Member States. Any Member State may obtain information from the system, but they cannot alter the entries and data of other Member States.

In accordance with the general data protection principles, the Schengen Convention implementing the Schengen Agreement recognises the right of persons, who are the data subjects

- to obtain information on the data stored about them in SIS,
- to request the rectification or deletion of erroneous data,
- to turn to the court or the competent authority requesting the rectification or erasure of data, or a decision on compensation.

On 14 November 2007, the European Parliament voted for Hungary's (and eight other EU Member States) accession to the Schengen Zone, which was thereby expanded to 3.6 million square kilometres, so from 21 December Hungary has been responsible for defending 15 percent of the Central-Eastern border of the zone.

In a few weeks' time, the Schengen acquis, which can be described as "the disappearance of borders" was also implemented in Hungary, which event was of outstanding significance for the citizens, the government agencies as well as the Office of the Data Protection Commissioner.

As from Hungary's accession to Schengen, if anyone wishes to obtain information whether his data are included in SIS or request the rectification or erasure of his data in SIS, he has to contact the SIRENE Office of the National Police Headquarters, or the data protection commissioner with the request. If he deems that the information received from the SIRENE Office is inadequate, the data protection commissioner can be of assistance in such a case.

As to the future of the institution of the data protection commissioner, in addition to playing the classical ombudsman's role, it is expected that it will become increasingly involved in the decision-making process, even if not by bringing direct decisions, but much more by providing consulting services. This is more than desirable in the case of major programmes, such as the e-government, as the legal risks of data protection have to be explored already in the design and preparatory phase and guarantees have to be found to prevent infringements.

However, no additional expansion in the powers of the data protection commissioner can be expected, which I do not consider necessary because the existing instruments provide an adequate elbowroom, we need to make an efficient use of the powers we currently have. I am convinced at the same time that the data protection commissioner can successfully take action to protect personal data and to provide access to data in the public interest in the future, if he can act with the authority of the ombudsman and work on the protection of the rights entrusted to him in cooperation with the actors concerned."

Changes in the legal regulation of data protection in Hungary – 2011[72]

In 2011, the new Fundamental Law provided not only for the rights, but also for the institution protecting those rights:

72 Dr. Attila Péterfalvi: A magyar adatvédelmi jogi szabályozás változásai, in Állam és Jog – Kodifikációs kihívások napjainkban. Magyar Jog- és Államtudományi Társaság – Gondolat, Szeged-Budapest, 2013, pp 99-115.

"Article VI
(1) Everyone shall have the right to have his or her private and family life, home, communications and good reputation respected.

(2) Everyone shall have the right to the protection of his or her personal data as well as to access and disseminate data in the public interest.

(3) The application of the right to the protection of personal data and to access data in the public interest shall be supervised by an independent authority established by a cardinal act."

The Fundamental Law was followed by the second Hungarian Data Protection and Freedom of Information Act, Act CXII of 2011 on the Right to Informational Self-Determination and the Freedom of Information (hereinafter: Privacy Act). The second Data Protection Code lays particular emphasis on legal protection by the authority. A joint starting point of the previous and the new act is the protection of the dignity and personality of man. The fundamental goal of data protection is to enable the individual to have disposal over his data, to be entitled to the appropriate protection and in this way to enable the development of a relationship of trust based on legal regulation between the controller and the data subject, which is part of the requirement for fair data processing. Another objective of data protection is to guarantee legal remedy and legal certainty for every citizen. The protection of data serves not only data subjects, but through it the interest and good reputation of the controller organisations also, which is an element of goodwill so important in economic relationships. Beyond ensuring compliance, the appropriate protection of personal data also protects the organisation and increases its external acceptance. Over and above this, the specification of the conditions and rules of transborder movement of data is also a cardinal issue in the regulation of data protection with a view to facilitating economic activities. By renewing the rules in force for the protection of personal data and the accessibility of data in the public interest, the new act guarantees calculable and effective legal protection for the data subjects, transparent rules for controllers that are easy to follow and the framework of efficient and lawful operation for government agencies.

Advocacy institution

In 2011, Parliament adopted a new Fundamental Law, which provides that the application of the right to the protection of personal data and to access data of public interest shall be supervised by an independent authority established by a cardinal act.

With the entry into force of the Fundamental Law in Hungary, the system of ombudsmen was also radically transformed. A system of four parliamentary commissioners of equal rank (one general and three separate commissioners) was replaced by a so-called single commissioner system. Beside the foundation of the institution of the commissioner of fundamental rights, the priority powers of the former two separate commissioners (for the protection of the rights of ethnic minorities and the rights of future generations) were retained in the position of deputies. The Office of the Data Protection Commissioner as a special ombudsman was terminated without legal successor and its powers were taken over by an independent organisation to be set up according to the Fundamental Law, under the name of the Nemzeti Adatvédelmi és Információszabadság Hatóság (Hungarian National Authority for Data Protection and the Freedom of Information, hereinafter: NAIH or Authority).

The EU directive also requires Member States to have an authority taking action with full independence to supervise the application of the legal regulations concerning the processing of personal data. There is, however, no norm whatsoever which would require the Authority to be a supervisory agency of Parliament, or the head of the supervisory agency should be elected by Parliament. In the course of the operation of the institution of the commissioner, it was proven by now that an ombudsman's powers, of procedures and instruments no longer provide sufficient elbowroom and possibility for investigating and sanctioning data protection infringements. With the spread of information technology and the resultant social changes (using the Internet, social media, e-mail, digitalisation, broadband mobile communication) and in the new situation created by globalisation, action needs to be essentially more efficient and more forceful than the ombudsman's system set up in the mid-1990s in view of the fact that the number of threats that may

jeopardise fundamental rights increased further and citizens have landed in an even more exposed situation. With the wide dissemination of the latest technologies a person leaves a digital footprint, of which he is not and could not have been aware, and it excludes the possibility of the user enforcing his rights knowledgeably. Appropriate response has to be found for this new challenge and this response in Hungary is a new form of organisation, the data protection authority, which merges the mediator's functions, acting as an intermediary between citizens and the state and economic actors, while it can effectively enforce its decision, if necessary. So, instead of the institution of the ombudsman, it was necessary to face the new challenges and set up a national authority capable of providing appropriate responses to them.

The independence of the Nemzeti Adatvédelmi és Információszabadság Hatóság

The Nemzeti Adatvédelmi és Információszabadság Hatóság is independent because in accordance with the provisions of the Fundamental Law and the legal regulations pertaining to it,

- in terms of its organisation and procedures, it is subordinated only to the laws, and its tasks may be specified only by law,
- it cannot be instructed within its tasks,
- it has to produce and disclose a report on its activities by 31 March of every year, which it has to send also to Parliament (it met this obligation in full as early as in 2012),
- it is separated organisationally within the system of public administration,
- it is a central budgetary body with chapter authorisations,
- it bears an independent title within the budgetary chapter of the Parliament, the expenditure and revenue totals of its budget may only be reduced by Parliament,
- the appointment of the president of the authority for nine years guarantees that he can carry out his work through several governmental cycles over the long run, free from political, economic or any other influence,
- only the president of NAIH has the authority to engage and dismiss NAIH's staff (Parliament maximised the headcount of the organisation in

59; another novelty is that the president of the Authority may appoint inspectors for priority tasks requiring higher professional qualifications and meeting higher standards up to 20 percent of the headcount, whose remuneration may be higher; all of the inspectors of the Authority and the vast majority of the managers, the data protection experts and administrative staff used to work as civil servants for the terminated Office of the Data Protection Commissioner).

The procedures of the Authority

Among the Authority's procedures, the Privacy Act regulates the investigative procedure, the Authority's data protection and secret supervisory procedure, the right of the Authority to launch litigation, the management of the data protection records and the conduct of the data protection audit. In addition, Chapter VI contains certain other rules linked to the Authority's procedures, such as the provisions concerning processing and confidentiality. The various types of procedures, to which the act summarily refers as the procedures of the Authority, are separate from one another, they are different in nature and are only partially linked to one another.

We need to speak of the actual "basic procedure" first, which is the investigative procedure that may be launched exclusively based on a complaint. The Act on the General Rules of the Procedures of Administrative Authorities and Services does not govern the procedural order used by the ombudsman, and extending to both informational rights, but supplemented with enforceability by the courts and the possibility of drafting public reports. Anyone may initiate inspection by the Authority, not the data subject only. As a main rule, the merits of every complaint must be investigated, with the exception of the cases specified by law. The latter cases include, first and foremost, if there is a court procedure in the case on which the complaint was based, or if a final court decision had been made on the matter. If the data subject has the opportunity to turn directly to the court because of an infringement, he himself may decide which forum to choose for the protection of his legitimate interests, but the Authority may not take action in parallel with the court procedure. An argument definitely for a decision to opt for NAIH may be that NAIH's procedure is free of charge, it is rapid, very simple to initiate, it is informal

and does not require legal representation or specialised knowledge.
The ombudsman-type instruments are available to the Authority in every case when there is an infringement or direct threat of an infringement in relation to exercising the rights to the processing of personal data and to access data in the public interest or data accessible on grounds of public interest. Using these instruments, the Authority may call upon the controller or its supervisory body, if there is any, to rectify the infringement or to terminate the direct threat of an infringement. In addition, it may put forward recommendations to the body authorised to legislate.

If the complaint is found well-grounded, instead of using the ombudsman-type instruments, it may conduct an administrative procedure in the fields of data protection and secret supervision. It is an important condition that the Authority may launch its data protection procedure only ex officio. The act specifies the cases when launching such a procedure is mandatory, for stringent action is warranted in cases affecting a wide range of people, or sensitive data, or cases involving a high risk of damage or major infringement of interests. At the same time, it is possible to ask for direct legal remedy from the courts against the decision (the logic of Hungarian protection of fundamental rights requires it in every case). A novelty of the act is that if the Authority establishes the unlawful processing of personal data, it may levy a fine of as much as ten million forints. The fine may be levied several times, if the controller fails to comply with the decision. Nevertheless, it can be stated that the Authority is not a "fine factory" and its objective is not to increase the revenues of the central budget but to have an open dialogue and cooperation with controllers, processors, citizens, governmental and non-governmental organisations in order to protect the rights.

The Authority may not conduct an Authority-type procedure in relation to the right to access data in the public interest or data accessible on the grounds of public interest, unless it is related to the unlawful classification of national classified data. In such cases, the Authority only has the opportunity to conduct ombudsman-type inspections; if it is unsuccessful, a report may be drafted or ultimately it may turn to the courts. In addition, the applicant may enforce his rights to access data in the public interest and data accessible on the grounds of public interest directly in front of the courts according to the law.

The novelties of the regulation

In line with the European consensus, the concepts of the data protection law are stable, relatively constant and they did not play the main role in terms of the amendments introduced by the Privacy Act. A new element among the interpretative provisions is the notion of the data subject. The legislator separated the definitions of the data subject and of personal data, this duality, however, does not impede the application of the law and in practice we meet the same notion of personal data as in the course of the application of the previous Privacy Act.

The change in the notion of personal data merits particular attention: among the definitions, we need to take into account Section 4(3) of the Privacy Act, according to which "in the course of processing, data shall retain their personal character as long as their connection with the data subject can be restored. The connection with the data subject shall, in particular, be considered restorable if the controller is in possession of the technical means necessary for the restoration". This rule may have surprised many because it may seem that it narrows down the notion of personal data and hence the range of data subject to protection by the Privacy Act, but the new definition cannot be interpreted by fully taking it out from the given context. If the purpose of the operations carried out on the data is to draw conclusions with respect to specific natural persons and to make decisions, then the controller may not refer to a narrower rule because the purpose of the operation is to make or prepare for a decision affecting the situation of the individual. If these cases were exempt from the scope of the law, the individual would land in a more exposed situation enjoying less protection. Obviously, that could not be the purpose of the legislator.

In relation to the principles of processing, the Privacy Act stipulates purpose limitation, underlining it as the first one in combination with the principle of data quality, which is one of the most important internationally developed principles of processing. In compliance with the principle, only those personal data can be processed, which are indispensable for the discharge of the tasks and powers of the controller. The principle of data minimisation warrants that in view of the purpose of processing, only the narrowest justified range of data can be processed and in relation to

this, it must be ensured that there should be a possibility to identify a given person based on the data only for the period of time necessary for the purpose of storage. The requirements of purpose limitation and data minimisation extend to all phases of processing. This provision excludes processing for hoarding.

In general, the greatest attention is paid to the new legal bases and professional circles expect clear guidance on it: what is it that can be done on this basis and what is it that constitutes the limit to the new legal bases. Pursuant to Section 6(1) of the Privacy Act: "Personal data may be processed even if obtaining the consent of the data subject is impossible, or would imply disproportionate costs and the processing of personal data a) is necessary to meet the legal obligations of the controller, or b) it is necessary to enforce the legitimate interests of the controller or a third person, and the enforcement of such interests is proportionate to the restriction of the right to the protection of personal data". In relation to this regulation, it is necessary to call attention to the fact that it is applicable only in a relatively narrow circle, after careful consideration and the application of the legal basis does not exempt a controller from informing citizens of the circumstances of processing in every possible way and in the case of a concrete request, from enabling the exercise of the data subject's rights. It should also be mentioned that according to the new rule, a person above the age of 16 may independently provide for the processing of his/her personal data; earlier, the law made this possible only from the age of 18 upon reaching majority.
The legislator ensures the enforcement of the principle of data security by stipulating more specific requirements. The principles include "privacy by design" pursuant to which the enforcement of data protection criteria must be built into the design process. Data security requirements include the prevention of unauthorised data entry, the prevention of using automated processing systems by unauthorised persons with the help of data transmission equipment – i.e. the prevention of hacking and cracking, the control of data transmission, logging the events, restorability in the case of breakdowns and the reporting obligation in the case of errors arising in the course of automated processing (internal documentation of data protection incidents).

In terms of citizens' rights, the new regulation introduced more transparency rather than novelty. Operation as an authority, however, opens up new vistas in the field of the enforceability of the rights, strengthening the position of the data subjects. In terms of data subjects' rights, the act stipulates more detailed requirements than the previous regulation with regard to the obligation to provide prior information. The other rights and possibilities for the enforcement of rights due to the data subject based on the right to informational self-determination, supplemented with the possibility of the procedure of the data protection authority, continued to be maintained.

Informational self-determination can be exercised if data are collected from the data subject and the data subject is aware of it. Being aware, however, is not the same as giving consent and particularly not the same as giving consent after being informed. Therefore, irrespective of whether the provision of the data is voluntary or mandatory, the data subject may bring an informed decision only if he is aware of the consequences of refusing to provide data. Since the act clearly states that the controller is subject to the obligation of providing information in advance, including the legal regulation applicable to the provision of the data, the purpose of processing as well as the identity of the controller. The data subject must be informed about who the controller of the data is and what other controllers may have access to the data by way of transmission. The controller's obligation to provide information serves the enforcement of the rights of the data subject. Information must be provided in an easy-to-understand form. The act sets forth special provisions for simplicity and lifelike regulation for the case of mandatory processing with regard to the information as well as for the case when personal information is impossible or it would involve disproportionate costs.
In relation to access to data in the public interest, the regulation has become more lifelike: as against the earlier unfulfillable requests, it provides protection to prevent the paralysis of the operation of an organisation through the submission of masses of requests. Over and above the case of classified data, it is possible for the legislator to restrict access to data in the public interest by law for certain special purposes. The act expanded the range of purposes allowing for lawful restriction with interests linked to the protection of the environment and nature conservation, as well the

right to intellectual property. The act retains the old system with regard to access to data for the preparation of decisions. As a general rule, data used as grounds for a decision may not be accessed for maximum ten years; the controller, however, may allow access to the data in individual cases. If, however, the decision was already made based on the data in question, the controller may refuse to make the data accessible only on the basis of the reasons listed in the act, and in such a case the burden of proof is on the controller with respect to the grounds of the reasons for rejection. The basis for rejection must be interpreted narrowly.

Changes of fundamental significance in data protection

Following the establishment of the Authority, the Act on Informational Self-Determination and the Freedom of Information was amended once in a significant way in 2015: Act CXXIX of 2015 amended and expanded the rules of the authority's procedure in the review of secrets with a view to terminate anti-constitutionality manifested in omission as established by Constitutional Court resolution 4/2015 (II. 13) AB. Besides this, Parliament amended the Privacy Act in a few cases; most of these amendments concerned the freedom of information through the introduction of new legal institutions, such as the rules of establishing cost reimbursement and the rules pertaining to invoice level checks.

Regulation (EU) 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 personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) brought about changes of fundamental significance in the field of data protection, which created uniform regulation in the EU, replacing the system of national regulations of different contents.

GDPR is only one of the elements of the new data protection regime in the European Union; in addition, the Commission and the Council adopted the Directive pertaining to the protection of personal data processed for the purposes of prosecution (Directive (EU) 2016/680 – Prosecution Directive). Whereas GDPR was made directly applicable all over the EU from 25 May 2018, Member States had to transpose the Directive into their national

legal regulations by 6 May 2018.

The third element of the reform – Regulation on Electronic Communications (ePrivacy) – has not been adopted to this day.

3. Dr. Tamás Bendik: The birth of GDPR and its impact on the Hungarian legal system

Dr. Tamás Bendik: He began his professional career at the Ministry of Justice, Between 2012 and 2018, he represented Hungary in the data protection working group of the Council of the European Union and in the data protection expert group of the European Commission. Currently, he is strategic chief counsellor to the President of the Hungarian National Authority for Data Protection and the Freedom of Information.

1. The regulatory environment of GDPR[73]

1.1. The antecedents of the data protection reform

The legal history of data protection legislation in the European Union began, on the one hand, with data protection codification in the Member States in the 1970s (the first comprehensive data protection regulation was adopted in Hessen in 1970, followed by Sweden in 1973, the Federal Republic of Germany at the Federal level in 1976 , France in 1977, and then the regulation enacted in the United Kingdom in 1984) and, on the other hand, with the international legal acts adopted by international organisations in the 1980s, which place particular emphasis on the protection of fundamental rights; the principles and regulatory directions set forth in these constituted the basis of Community (EU) law harmonisation [see on the one hand, the guidance of the Organisation of Economic Cooperation and Development (OECD) adopted in 1980[74] and the Convention of 28 January 1981 concerning the protection of individuals during the machine processing of personal data adopted in Strasbourg (hereinafter: Data Protection Convention of the Council of Europe). The OECD guidelines were amended for the first time in 2013[75]].

73 Dr. Tamás Bendik: A GDPR szabályozási környezete. In: Attila Péterfalvi - Balázs Révész-Péter Buzás (ed.). Magyarázat a GDPR-ról. Budapest, 2018. Wolters Kluwer Kiadó, pp. 25-35. (Manuscript closed: 1 September 2018)

74 http://www.oecd.org/sti/leconomy/oecdguidelinesontheprotectionofprivacyand transborderflowesofpersonaldata.htm

75 With respect to the amended guidelines, see The OECD Privacy Framework. OECD Publishing. 2013. http://www.oecd.org/internet/leconomy/oecd_privacy_framework.pdf

The primary motivation behind Community legislation – stemming from the goals of the European integration, which are fundamentally of an economic nature – is not so much the reinforcement of the protection of fundamental rights but the dismantling of the barriers to the functioning of the internal market [cf. the provision serving as the legal basis for the enactment of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 (hereinafter: Data Protection Directive) [Article 100a of the Treaty establishing the European Community (hereinafter: ECT) set forth by Article 2(54) of the Treaty of Amsterdam] and Recital (9) of the Data Protection Directive]. hence the objective of the Community legislator to facilitate the free flow of personal data among the Member States –in a way that is not impeded by the data protection requirements of different nature and content specified in national legal systems. This regulatory need led to the enactment of the Data Protection Directive, which was the central and the first, historically significant legal act of in this legal field within the European Union's regime relating to the protection of personal data prior to the adoption of the data protection package.

In addition to the economic goal referred to, at the same time one can draw conclusions concerning the intention of the EU legislator as the Data Protection Directive recognised and supported the national legislative measures providing a higher level of protection for the privacy of data subjects than what was set forth in it, in addition to the law harmonisation objective. Recital (10) of the Data Protection Directive stipulates that the approximation of [national] laws "must not result in any lessening of the protection they afford, but must, on the contrary, seek to ensure a high level of protection in the Community".

In spite of this, the European Court of Justice (hereinafter: ECJ or the Court) arrived at the conclusion in the decisions made in the Lindqvist case (Lindqvist decision of 6 November 2003, C-101/01, ECLI:EU:C:2003:596, 99) and in the joint cases ASNEF and FECEMD, (decision in the joint cases ASNEF and FECEMD of 24 November 2011, C-468/10 and C-469/10, ECLI:EU:C:2011:777, 32.) that the Data Protection Directive fundamentally implemented a full unification of the law, thus in particular with regard to the legal basis of processing, providing no elbowroom for the Member State legislators to deviate from it. This, however, did not prevent Member

States in transposing the provisions of the Data Protection Directive into their own legal systems with substantially different content, providing different levels of protection in every Member State, which differences and their legal and economic effects later appeared as one of the main motivating factors of the data protection reform.

The obligation of the Member States to ensure that the requirements of the Directive are to be supervised by an independent supervisory authority can be assessed as a significant achievement of the Data Protection Directive. This legal institution subsequently served as an example for the development of the data protection regime of the Council of Europe, strengthening the mutual interaction and convergence of the data protection regimes established by the European Union and the Council of Europe [Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (hereinafter: CE Data Protection Convention) promulgated by Act VI of 1998 and its Additional Protocol regarding supervisory authorities and transborder data flows (hereinafter: Additional Protocol to the CE Data Protection Convention) promulgated by Act LIII of 2005].

The addressees of the Data Protection Directive were the Member States, consequently, the activities of the institutions and organisations serving the operation of the Union performing administrative tasks, including the processing of personal data, were outside its personal-organisation scope. In addition, the conditions for the institutionalised supervision of the data processing operations of the EU institutions were not ensured within the framework of the Data Protection Directive.

Although the regulatory hiatus was in part managed by the Treaty of Amsterdam [pursuant to Article 286(1) of the consolidated version of TEU "from 1 January 1999, Community acts on the protection of individuals with regard to the processing of personal data and the free movement of such data shall apply to the institutions and bodies set up by or on the basis of this treaty"], additional provisions incorporated in a secondary EU legal act proved to be indispensable for the clear specification of the obligations of controllers and processors and for the efficient enforcement of the protection of the data subjects' rights [TEU Article 286(2) also stipulated the obligation concerning such legislation].

Regulation (EC) 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data was adopted following these antecedents. The main achievement of this regulation was that it established the institution of the European Data Protection Commissioner, supervising the data processing operations of the EU institutions and bodies, which institution continues to perform activities decisive for the data protection legislation and its application in the European Union. Prior to the data protection reform, this Regulation was supplemented by Decision 1247/2002/EC of the European Parliament, of the Council and of the Commission of 1 July 2002 on the regulations and general conditions governing the performance of the European data protection supervisor's duties.

The pillar structure created by the Treaty of Maastricht extended the responsibilities and powers of the European Union to areas through further deepening European integration, to which the Data Protection Directive was not applicable. Information exchange among Member States within the framework of cooperation under justice and home affairs constituting the third pillar (police and judicial cooperation in criminal matters) could not be implemented in the absence of the transmission of personal data as the conditions set forth in the Member State legal systems concerning the processing of personal data not regulated by EU law constituted a material impediment for such data exchange.

The next station of EU data protection law harmonisation just one-and-a-half decades after the establishment of the pillar structure focussed on the dismantling of this material barrier. It specified the fundamental requirements concerning the processing of personal data with respect to activities belonging to the third pillar: Council framework decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

With respect to framework decision 2008/977/JHA, its scope and the consequences of specifying it should be underlined. The framework

decision was applicable only to the processing of those personal data, which constituted the subject matter of information exchange by Member States with other Member States or with EU institutions and the scope did not extend to the processing of data, which the law enforcement agencies of the Member States collected and processed in the course of their activities subject to the objective scope of the framework decision, irrespective of such an exchange of information [Framework decision 2008/977/JHA Article 1(2) and Recitals (7) and (9)].

In contrast to the Data Protection Directive, the framework decision clearly specified its minimum harmonisation character at a normative level, stating that the Member States could enact and apply provisions ensuring levels of protection higher than that provided by the EU data protection requirements [Framework decision 2008/977/JHA Article 1(5) and Recital (10)].

The legal acts referred to constituted only the backbone of the EU data protection regime and were the source of horizontal requirements restricted to the objective scope as indicated.

The incremental nature of the processing of personal data related to certain fundamental legal relationships necessitated the incorporation of specific data protection requirements into EU legal norms regulating activities, implementing the processing of personal data, just as in the case of the legal systems of the Member States [see, for instance, Chapter VI of Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (hereinafter: Europol Regulation)], as well as the enactment of independent sectoral acts – as ***lex specialis*** acts relative to the Data Protection Directive –aimed expressly at the establishment of a data processing and data protection regime related to the activity of the regulated sector.

Of the latter, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and

the protection of privacy in the electronic communication sector has been of outstanding significance with regard to its role in the development of EU data protection law. This directive focusing on "the processing of personal data related to the provision of publicly available communication services through public communication network" contains sector specific data protection requirements, including those related to the security of services and personal data, which served also as a preview of Regulation (EU) 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 (hereinafter: GDPR). As a sectoral norm, Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communication services or of public communications networks and amending Directive 2002/58/EC (Data Retention Directive) was enacted partly in connection with this subject matter and partly in connection with the third pillar (law enforcement activity). The providers of publicly available electronic communication services or of public communications networks had to retain data about communication, location data, and related data necessary for the identification of the subscriber or the registered user in order that they could be used later by law enforcement agencies in the course of their activities. However, the provisions of the directive did not comply with the requirements set by the Court of Justice of the European Union for the restriction of the right to the protection of personal data by way of legislative measures, thus the Court declared it invalid in its judgment of 8 April 2014 (see Judgment in the case of Digital Rights Ireland and Seitlinger & Co. of 8 April 2014, C-293/12 and C-594/12, ECLI:EU:C:2014:238, 6-7).

Finally, the delegated and implementing acts issued by the European Commission constituted an important part of the regulatory system preceding the data protection reform. These included in particular the decisions aimed at establishing the appropriate level of protection guaranteed in third countries over which the Court of Justice of the European Union exercised control, which was decisive in terms of the subsequent content of the data protection reform [see: EUB Judgment

of 6 October 2015 Schrems, C-362/14, ECLI-EU:C:2015:650 (hereinafter: Schrems judgment), which established the invalidity of 2000/520/EC Commission Decision of 26 July 2000 on the adequacy of the protection provided by the "safe harbour" privacy principles and related frequently asked questions issued by the US Department of Commerce].

1.2. The data protection reform

1.2.1. The impact of the Treaty of Lisbon on the Data Protection Regulation in the European Union

The entry into force of the Treaty of Lisbon and the amendment to the founding treaties based on its provisions can be regarded as the point of departure for the reform of the data protection regime in the European Union presented above, applicable until May 2018. These amendments significantly affected the EU regulations concerning the protection of personal data from several aspects.

First and foremost, it should be underlined that although the Charter of Fundamental Rights of the European Union (hereinafter: Charter) has not formally become part of the founding treaties, however the amendments adopted with the Treaty of Lisbon gave it the same legal value as the treaties had [Treaty on the European Union (hereinafter: TEU) Article 6(1)]. Its significance is that Article 8 of the Charter guarantees the right to the protection of personal data as an independent fundamental right and specifies the related fundamental principles and requirements.

Secondly, the Treaty of Lisbon stipulated the right to the protection of personal data also in the founding treaties and within the framework of ordinary legislative procedure authorised the Council and the European Parliament to enact secondary legal acts. The authorisation provided the legal basis for the legal acts adopted under the data protection package [Treaty on the Functioning of the European Union (hereinafter: TFEU) Article 16].

Third, the Treaty of Lisbon terminated the system based on the classification of EU policies into pillars, which put an end to the possibility of enacting earlier sources of law for the regulation of EU policies belonging under the second and the third pillars, including the subject matter regulated by framework decision 2008/977/JHA and instead the sources of law under the first pillar became the instruments of regulation (regulation, directive, decision). In terms of the EU data protection law, the Treaty of Lisbon and raising the Charter to the rank of a treaty gave a hitherto unparalleled chance and opportunity for the harmonisation of the data protection regimes of the Member States, for the unification of law. However, the possibility for the development of a uniform regime was qualified by the fact that, on the one hand, TFEU Article 16(3) and TEU Article 39 themselves stipulated that special rules needed to be enacted in the field of the joint foreign and security policy (earlier second pillar), authorising the Council only to enact legislation in the form of decisions and, on the other hand, the Member States declared in Declaration 21 on the protection of personal data in the field of judicial cooperation in criminal matters and police cooperation annexed to the closing declaration of the intergovernmental conference adopting the Treaty of Lisbon – that in the subject matter subject to the former third pillar special rules may be necessary for the protection of personal data and the free flow of personal data due to the specific nature of these areas.

1.2.2. The preparation and submission of the data protection package

As presented before, the Treaty of Lisbon established the legal conditions for the review of the EU data protection regime and soon it was followed by the formulation at political level of the need for such a review. The Stockholm Programme[76] can be regarded one of its most significant milestones, in which the European Council invited the Commission to assess the EU data protection regulation and subject to the result of such an assessment, to submit "legislative and non-legislative" initiatives. At the same time, the European Council declared that one of its objectives was that "on a broader front the Union must be a driving force behind the

76 The Stockholm Programme – An open and secure Europe serving and protecting the citizens, HLC 115, 4.5.2010, p. 10.

development and promotion of international standards for personal data protection based on relevant EU instruments on data protection and the 1981 Council of Europe Convention and in the conclusion of appropriate bilateral or multilateral instruments". This goal became decisive in the course of the negotiations aimed at the modernisation of the data protection requirements of the Council of Europe as detailed below, as well as with regard to the results of such negotiations.
Then, in order to clarify the direction and content of the review of the EU data protection ***acquis***, the European Commission in charge of the preparation of the legislative proposal organised consultations and conferences focusing on general and certain specialised areas and professional organisations, it conducted reconciliations with the EU institutions affected by the legislative procedures and prepared an impact assessment to examine regulatory alternatives {for the summary of the impact assessment, see the Commission's Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data [COM(2012) 11 final][77] (hereinafter: GDPR proposal) 2-5}.

Following these antecedents, the European Commission submitted its package of legislative proposals, the so-called "data protection package" on 25 January 2012. The data protection package consisted of a policy communication presenting the objectives to be achieved through the regulation {Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Safeguarding privacy in a connected world, a European data protection framework for the 21st century [COM(2012) 9 final][78]}, and two legal acts to be enacted in two different sources of law, on the one hand, with regard to the processing of personal data, a proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and the free flow of such data [General Data Protection Regulation] and, on the other hand, a proposal for a directive of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data by the competent authorities

77 https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52012SC0073&from=HU
78 https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52012DC0009&from=HU

to prevent, investigate and detect criminal acts, to conduct criminal procedures or to implement criminal sanctions and the free flow of such data {GDPR proposal; and the Commission's proposal for a directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and the free movement of such data [COM(2012) 10 final][79] (hereinafter: proposal for a directive on criminal affairs)}.

1.2.3. Conduct of negotiations of the data protection package

Pursuant to TFEU Article 16(2) both legislative proposals had to be negotiated and adopted in the course of generally accepted, ordinary legislative procedures after the Treaty of Lisbon. Accordingly, the Commission sent the proposals to the co-legislators, the European Parliament and the Council, and negotiations were conducted in these institutions in parallel. In relation to the legislative proposals, opinions were issued by the European Data Protection Supervisor (Opinion of the European Data Protection Supervisor on the data protection reform package)[80], the Committee of the Regions[81], the European Economic and Social Committee[82], and the European Union Agency for Fundamental Rights (Opinion of the European Union Agency for Fundamental Rights on the proposed data protection reform package)[83].

At expert level, Council negotiations began in the Data Protection and Information Exchange working group (DAPIX) of the Council under the leadership of the Danish Presidency. The outstanding significance of the proposals is indicated by the fact that the reports related to the results of the negotiations and – because of the need for conceptional and

79 https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52012PC0011&from=HU
80 https://edps.europa.eu/sites/edp/files/publication/12-03-07_edps_reform_package_enpdf, summary of the opinion in Hungarian: https://eur-lex.europa.eu/legal-content/HU/TXT/?u-n=O-J:C:2012:192:TOC; second position taken by the European Data Protection Supervisor, concerning the political compromise developed by the co-legislators: https://edps.europa.eu/sites/edp/files/publication/15-10-09_gdpr_with_addendum_hu.pdf.
81 HLC 391., 18.12.2012, pp. 127-133.
82 HLC 229., 31.7.2012, pp. 90-97.
83 http://fra.europa.eu/en/opinion/2012/fra-opinion-proposed-eu-data-protection-reform-package

theoretical guidance beyond the professional level – the proposals were regularly on the agenda of the competent political decision-making forum of the Council, the Council for Justice and Home Affairs, throughout the legislative process[84]. In the European Parliament, the Committee on Civil Liberties, Justice and Home Affairs conducted a detailed examination of the elements of the data protection package; the Parliament adopted its first reading position at its plenary session of 12 March 2014[85]. Following the decision of the European Parliament, the political pressure on the Council to complete the negotiations became increasingly intensive, yet the governments of the Member States arrived at an agreement concerning the proposal for the regulation only at the 5-6 June 2015 session of the Council for Justice and Home Affairs and the proposal for the directive at its session of 8-9 October 2015 and adopted the so-called general approach.[86]

In possession of this agreement, the negotiations between the co-legislators began with the participation of the Commission in order to work out the amendments submitted in relation to the legislative proposals, i.e. the finalised content of the legislative acts. As a result of the intensive negotiations, political agreement was reached among the co-legislators[87] by the end of 2015. Following the review and correction of legal acts by lawyers and linguists, the Council formally adopted its first reading position in a written procedure on 8 April 2016[88] enabling the European Parliament to decide on the adoption of the legal acts constituting the elements of the data protection package, closing the legislative process at its plenary sessions of 14 April 2016.

84 See in this context the press releases of the Council about the agenda items discussed at the meetings of the Council for Justice and Home Affairs, e.g. Council document 17315/12: http://europa.eu/rapid/press-release_PRES-12-509_hu.htm?locale=hu; Council document 7215/13: http:/data.consilium.europa.eu/doc/document/ST-7215-2013-INIT/hu/pdf

85 On the proposal for the General Data Protection Regulation see HL C 378, 9.11.2017, pp. 399-492; with regard to the proposal for the Data Protection Directive for Criminal Affairs, see HL C 378, 9.11.2017, pp. 496-545.

86 See the documents adopted by the Council, on the proposal for the General Data Protection Regulation: Document 9398/15: http://data.consilium.europa.eu/doc/document/ST-9398-2015-INIT/hu/pdf; with regard to the proposal for the Data Protection Directive for Criminal Affairs: Document 12555/15: http:// http://data.consilium.europa.eu/doc/document/ST-12555-2015-INIT/hu/pdf

87 See Council Document 5455/16: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?u-rl=CONSIL:ST_5455_2016_INIT&from=EN

88 For the outcome of voting see Council Document 7920/16: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?url=CONSIL:ST_7920_2016_INIT&from=EN

1.3. The new data protection acquis

As a result of the legislative procedure, which lasted more than four years, the legal acts enacted as part of the data protection reform of the European Union became parts of the EU ***acquis*** following their execution by the President of the European Parliament and the President of the Council on 27 April 2016 and their promulgation in the Official Journal of the European Union on 4 May 2016 as follows:[89]

- Regulations (EU) 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)
- Directive (EU) 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 (hereinafter: Criminal Affairs Directive).

GDPR entered into force on 24 May 2016, however, it became applicable in the legal systems of the Member States only after a preparatory period of two years from 25 May 2018. The Criminal Affairs Directive also entered into force on 5 May 2016 and the Member State legislators also had two years to transpose the provisions of the directive into Member State law [GDPR Article 99(1)-(2), Criminal Affairs Directive Article 63(1) and Article 64].

Following the adoption of the data protection package, the delegated and implementing acts that supplement GDPR, including the General Terms and Conditions of Contract between the controller and the processor, and the requirements enacted by the European Commission establishing the conditions of the lawfulness of data transmission to third countries and international organisations as well as the requirements concerning Codes of Conduct and certification [e.g. GDPR Article 28(7), Article 40(9), Article

89 OJ C 58, 15.2.2018. pp. 252-252.

43(8)-(9), Article 45(3) and (5), Article 46(2)(c)-(d), Article 92 and Criminal Affairs Directive Article 36(3) and (5), Article 50(8)] will continue to have outstanding practical significance.

Although legislation related to the delegated and implementing acts referred to has not yet been carried out, it should be noted that the majority of the delegated and implementing acts adopted prior to the data protection reform will remain in force even after GDPR becomes applicable [GDPR Article 45(9)].

1.4. The future of Data Protection Regulation in the European Union

Although the first stage of the EU data protection reform was closed with the adoption and entry into force of the data protection package, the review of the EU data protection ***acquis*** continues to remain on the agenda of the EU legislators.

In order that the EU ***acquis*** guarantee the right of EU citizens to the protection of their personal data based a uniform and coherent regulation, on 10 January 2017, the Commission submitted its legislative proposal drafted as a result of the review of Regulation 45/2001/EC on the protection of individuals with regard to the processing of personal data by the EU institutions, bodies, offices and agencies and on the free movement of such data and repealing Regulation 45/2001/EC and Decision 1247/2002/EC { Commission Proposal for a regulation of the European Parliament and of the Council, Regulation on the protection of individuals with regard to the processing of personal data by the EU institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC [COM(2017) 8 final]}[90]. The primary purpose of the proposal was to extend the achievements of the data protection package to data processing by EU institutions and bodies and to develop a legal regime applying a uniform set of requirements.

The legislative procedure was largely closed by June 2018[91], the co-

90 European Commission document COM(2017) 8 final: https://eur-lex.europa.eu/legal-content/HU/TEXT/PDF/?url=CELEX-52017PC0008&from=HU

91 See Council document 9296/18 and the draft therein: https://eur-lex.europa.eu/legal-content/EN/

legislators arrived at an agreement, so following its promulgation, the new regulation aligned with the achievements of the data protection package replacing Regulation 45/2001/EC and Decision 1247/2002/EC will become applicable to processing by EU institutions and bodies and the supervision of such processing. The novelty of the new regulation is that the range of processing legal relationship subject to its force are extended and an independent chapter will contain the rules, which are to be applied as ***lex generalis*** for the processing of the operative data of the EU agencies, performing activities regulated under TFEU Part Three Title V Chapter 4 (Judicial cooperation in criminal matters) and Chapter 5 (Police cooperation).

In addition, the legislative procedure aimed at the enactment of a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC is also in progress, which proposal was submitted by the European Commission on 11 January 2017 { Commission Proposal of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) [COM(2017) 10 final][92]}. The purpose of the proposal is to re-regulate the data processing activities of the electronic communications sector aligned with GDPR as a lex specialis norm relative to it. Similarly as in the case of GDPR, the Commission's legislative proposal recommends that instead of a directive as the source of law for the earlier regulation of this area, the planned regulation should be developed in the directly applicable form as a regulation by mitigating the Member States' legislative elbowroom.

Discussions of the proposal are in progress, not even the European Parliament has adopted its first reading position, thus the final content of the elements of the new regulation and the date of the entry into force and the date of applicability of the new provisions are yet unknown.

TXT/PDF/?url=CONSILST_9296_2018_INIT&from=EN

92 European Commission document COM(2017) 10 final: https://eur-lex.europa.eu/legal_content/HU/TXT/PDF/?url=CELEX-52017PC0010&from=HU

It is expected that the Data Protection Convention of the Council of Europe will also become part of the EU ***acquis*** in the near future. The negotiations aimed at the "modernisation" of the Convention have been taking place essentially simultaneously with the data protection reform of the EU, as a result of which the Member States of the Council of Europe agreed on the text of the supplementary protocol amending the Convention[93], and it was adopted by the Ministerial Committee of the Council of Europe on 18 May 2018 and it is open for signing from 25 June 2018[94].
The purpose of the supplementary protocol is that, with the entry into force of the amendments therein, the Data Protection Convention of the Council of Europe should provide a modern agreement capable of handling the technological challenges of the 21st century, which is a general agreement with an objective scope extending to every data processing operation, termed as an ***omnibus*** agreement, that has an international legal binding force applicable also to areas of law outside the scope of EU law, such as, for instance, processing for national security purposes.

Although several states outside Europe (such as Tunisia, Senegal, Uruguay)[95] acknowledged the mandatory force of the Data Protection Convention of the Council of Europe in force, the entry into force of the supplementary protocol under international law opens up the opportunity for international organisations to accede to the "modernised" convention; the Council of the European Union made its intention clear about accession by adopting the mandate[96] given to the European Commission for the negotiations on the supplementary protocol.

In view of the fact that the text of the data protection package and of the supplementary protocol was drafted in parallel and that in addition to the Member States of the European Union, the European Commission also participated in the negotiations on the supplementary protocol,

93 For the text of the supplementary protocol, see Council of Europe document CM(2018) 2-final: https://search.coe.Int/cm/Pages/result_details.aspx?Object ID=0900001680ff4e
94 See the decision made by the Ministerial Committee at its session of 18 May 2018. Council of Europe document CM/Del/Dec(2018)128/5.
95 Signing the Council of Europe Data Protection Convention or recognising its mandatory force is accessible here: https://www.coe.Int/en/web/conventions/full-list/-/conventions/treaty/108/signatures
96 See Council document 7234/3/13 REV 3 EXT 1 containing the published Article 1 of the text of Council decision determining the negotiating mandate p. 3: http://data.consilium.europa.eu/doc/document/ST-7234-2013-REV-3-EXT-1/hu/pdf

the data protection package and the supplementary protocol contain a harmonised set of requirements, the European Union's accession to the amended convention will have no effect on the content of the legal acts adopted within the framework of the EU data protection package and it is not expected to necessitate their amendment or supplementation.

Legislative steps taken to date within the framework of the data protection reform of the European Union revealed that the structure of the EU data protection ***acquis*** has not changed relative to the earlier regulation. A separate legal act will continue to contain the general set of requirements of data processing legal relationships in the Member States and the requirements concerning processing by the law enforcement agencies of the Member States and the data protection norms applicable by the EU institutions and bodies, even though these norms rely on the same legal basis of TFEU, thus the legal conditions for regulating them in the same legal act prevail.

Although the EU data protection reform is more ambitious in terms of the standardisation of the law than the earlier regulation, the elbowroom provided for the Member States' legislators in GDPR and the minimal harmonisation character of the Directive for Criminal Affairs continue to carry the possibility of different sets of requirements in every Member State.

In this regard, the law applying and law interpreting activity of the European Data Protection Body will be particularly emphatic, against which the development of the EU-wide uniform application of the law is now a legal requirement through the cooperation and consistency mechanism provided for in GDPR.

Naturally, the other depositary of the uniform application of the law continues to be the Court of Justice of the European Union. Its role is outstanding in harmonising the legal acts of the Member States with GDPR, particularly because GDPR has been formulated in a manner that offers interpretations of the law leading to the application of potentially different legal consequences.

2. The relationship of Member State law and GDPR – the role of the Privacy Act in the changed regulatory environment[97]

2.1. The framework of legal instruments of data protection regulation

The fundamental change arising from the enactment of GDPR is a consequence not of the content of the legal act, but of the legal nature of the instrument chosen by the EU legislator as the means of regulation. With regard to the legal relationships regulated by it, regulations are directly applicable sources of law in the legal systems of the Member States (TFEU Article 288), so in a typical case it results in fully uniform legal regulation with respect to all the addressees subject to it.

The fact that the EU legislator opted for the regulation as the source of law arose primarily from the conviction that one of the most important reasons for the substantial differences in the data protection requirements of the Member States was the nature of the source of law (GDPR Recital (9)).

The data processing legal relationships are incremental relative to the individual fundamental legal relationships; at the same time, their nature affecting the vast majority of legal and living conditions resulted in different courses of law development in the legal systems of the individual Member States, which resulted in the less than full implementation of the Commission's intent reflected in the legislative proposal, namely the possible fullest consistency of the EU legal requirements concerning the protection of personal data, was not fully implemented in the enacted regulation for reasons to be discussed in detail below.

In terms of the source of law of the Directive for Criminal Affairs, the data protection reform did not result in changes of merit relative to regulation by Framework Decision 2008/977/JHA. With regard to character, there is no difference between the framework decision or the directive as sources of law with respect to the entry into force of their requirements. The only reason for using a directive for regulation instead of the earlier legal framework is that after the entry into force of the Treaty of Lisbon and the termination of the pillar structure, primary EU law no longer provides an opportunity for the enactment of framework decision as a source of law. In

97 Dr. Tamás Bendik: A tagállami jog és a GDPR viszonya – az Infotv. szerepe a megváltozott szabályozási környezetben. In: Attila Péterfalvi-Balázs Révész-Péter Buzás (ed.): Magyarázat a GDPR-ról. Budapest 2018, Wolters Kluwer Kiadó, pp. 37-47. (Manuscript closed: 1 September 2018)

addition, the EU legislator maintained the minimum harmonisation nature of the regulation of this area of the law, which provides the opportunity for the Member State legislators to determine a higher level of protection for fundamental rights and more stringent conditions for data processing than that provided for in the directive [Directive for Criminal Affairs Article 1(3)].

There was, however, a substantial change relative to framework decision 2008/977/JHA in that the Directive for Criminal Affairs is applicable not only to the processing of personal data constituting the subject matter of data exchange among the Member States, but to all processing activities carried out by the competent authorities of the Member States for the purposes of the prevention, investigation, detection or prosecution of criminal offences, or the execution of criminal penalties, irrespective of the source of the processed data [Directive for Criminal Affairs Article (1) and Article 2(1)].

2.2. Sovereignty transfer and legislation by Member States

2.2.1. Legal relationships outside the scope of EU law

The legal acts defining the foundations and functioning of the European Union – the treaties – qualify as international treaties from the viewpoint of international law [cf. the definitions in Article 2(1)(a) of the Treaty on Contract Law done in Vienna on 23 May 1969, promulgated by law decree 12 of 1987 and in Section2(a) of Act L of 2005 on the Procedure Related to International Treaties]. With the conclusion of these international treaties, the Member States of the European Union agreed to exercise certain of their powers in issues subject to their jurisdiction together with the contracting parties, the other Member States, through the mechanisms and institutions determined in the treaties [***Article (E)*** of the Fundamental Law provides authorisation for this sovereignty transfer or power transfer with respect to Hungary]. Consequently, the subject matters with respect to which EU Member States did not transfer their sovereignty to the institutions of the Union, remained within the powers of national legislation and law enforcement.

The legislative powers of the European Union are restricted as to the protection of personal data. In subject matters that are not subject to EU law, neither the Charter, nor the treaties, nor secondary EU legislation enacted on their basis can be applied. Although this follows from primary EU law, the EU legal acts adopted in the data protection package also stipulate this restricted scope [GDPR Article (2)(2)(a), Directive for Criminal Affairs Article 2(3)(a)].

From the viewpoint of EU law, therefore, the Member State legislator has the opportunity – and also the constitutional obligation typically arising from the fundamental legal character of the right to the protection of personal data – to regulate the data processing legal relationships of subject matters and activities outside the scope of EU law.

The identification of these areas, however, points beyond the simple step of applying or interpreting the law. Neither the EU treaties, nor the secondary EU legal acts contain an exhaustive list that would accurately and comprehensively identify the subject matters that are subject to, or outside the scope of, EU law. Even the Recitals of GDPR and the Directive for Criminal Affairs mention activities related to national security as an example of such subject matters [GDPR Recital (16), Directive for Criminal Affairs Recital (14)].

So, the Member State legislator has the opportunity to enact rules with respect to the data processing activities in areas of the law outside the scope of EU legislation. However, if it interprets these powers extensively, and this interpretation fails to agree with the interpretation of the Court of Justice of the European Union, such regulation will not comply with EU law. Doubtless, such a situation gives rise to legal uncertainty, in relation to which there are good grounds to expect legal disputes between the Member States and the Commission, particularly in border areas which seek to regulate data protection legal relationships subject to the scope of EU law for purposes outside EU legislation (such as national security, defence).

2.2.2. Self-restriction by EU legislator

Since the entry into force of the Treaty of Lisbon, the European Union and the Member States have ***shared competences*** with respect to the internal market and the fundamental rights [TFEU Article 4(2)(a) and (j)]. This means that in addition to the European Union, the Member States also have legislative powers in these fields (in contrast to the exclusive competences regulated in Article 3 of TFEU), but only if the Union has not exercised its powers or expressly waives exercising it.

Just as the Data Protection Directive, both GDPR and the Directive for Criminal Affairs restrict their own material scope "to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data, which form part of a filing system or are intended to form part of a filing system" [Data Protection Directive Article 3(2), GDPR Article 2(1), Directive for Criminal Affairs Article 2(2)].
In view of the fact that neither the Charter, nor Article 16 of TFEU, which is the legal basis for secondary legislation, contains such restrictions, there are good grounds to question whether the acts adopted in the data protection package are fully compliant with primary EU law in this regard as they do not provide for the protection of the fundamental rights of data subjects in the area outside this material scope.

Another question is to what extent does the provision which distinguishes the applicable provisions based on the devices used for data processing comply with the purpose set in the course of EU legislation emphasised as one of the values of the data protection package and expressly specified in GDPR Recital (15), namely that the regulation should be technologically neutral (cf. for instance the press release of the European Commission following the adoption of the data protection package[98]).
Although it is obvious that the significance of data processing operations not regulated by secondary EU legislation as a result of the self-restriction referred to is meagre as such operations only include operations carried out manually (e.g. hand-written notes and letters), as a result of which personal data do not become part of a filing system, nor is there any

98 http://europa.eu/rapid/press-release_STATEMENT-16-1403.hu.htm

intention to do so, the assumption that even this type of data processing operation may cause infringement for the data subject whether intended by the controller or because of a negligent action cannot be disputed on good grounds, in relation to which EU law provides no defence, rectification or any right for the data subject or possibility of legal remedy. (Such an infringement could be, for instance, hanging on the notices board of the kindergarten sensitive data on the health condition of children, their medication, food or other allergies, collected from the parents at a kindergarten parents' meeting.)
It should be noted that although the Council of Europe Data Protection Convention, which can be regarded as the preview of EU data protection regulation, itself restricts "its own material scope to the automated folders of personal data and the automated processing of personal data", it expressly enables the contracting parties to undertake obligations to apply the convention "also to folders of personal data not processed by mechanical devices" through a unilateral international legal act, a statement to be deposited with the secretary general of the Council of Europe [Council of Europe Data Protection Convention Article 3(2)(c)]. And EU law does not exclude this possibility either.

2.3. Legislative elbowroom provided by GDPR

The fact that the source of law comprising the general data protection provisions is a regulation renders the related Member State regulatory techniques fundamentally different from that required by the earlier source of law being a ***directive.*** The addressee of the directive's provisions is the Member State and not the entities subject to its jurisdiction. Consequently, the Member State must incorporate the directive's requirements into its internal law also in terms of content. In contrast, the directly effective and applicable rules of a regulation are typically enforced with the same uniform content in every Member State, they cannot be repeated in internal law. Member States must ensure the unimpeded applicability of the rules of the regulation, partly by deregulating their internal legal rules in conflict with the content of the regulation and partly by taking the supplementary legislative and other measures indispensable for the enforcement of the regulation (e.g. establishment of the data protection supervisory authorities in the Member States, appointment of their

leaders, ensuring its conditions of operation).
However, soon after the commencement of the discussion of the legislative proposals it became clear that a "full" unification of the law extending to the public as well as the private sector will not take place [see Note, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (16140/14)[99]]. The European Commission did not receive uniform support from the Member States conducting negotiations in the Council whether to include the general data protection requirements (to be applied equally to data processing legal relationships in the public and the private sector) in a regulation as the source of law in EU legislation, instead of the earlier directive, so the decision on this was postponed by the Council to a later stage of the negotiations.[100]

Although this issue was decided in the course of the negotiations based on the majority of the Member States in favour of using a regulation as the source of law[101], it also became clear that the initial Commission legislative proposal had to be supplemented with ***flexibility clauses*** or opening clauses at several points for the sake of reaching a compromise, which provide opportunities for both the EU and the Member State legislators to maintain or enact data protection rules which in some cases may deviate from the general EU requirements and in other cases supplement them [cf. e.g. GDPR Recital (8), Article 8(2) and (3), Article 8(1), Article 9(4), Article 23, Chapter IX].

The dozens of flexibility clauses incorporated into GDPR affect a substantial part of the meritorial, material legal requirements of the regulation[102], not merely through data processing operations carried out by the public sector[103], influencing their scope and application and fundamentally

99 http://data.consilium.europa.eu/doc/document/ST-16140-2014-INIT/hu/pdf
100 http://data.consilium.europa.eu/doc/document/ST-16525-2012-REV-1/hu/pdf
101 See Council document 16140/14 point 2: http://data.consilium,europa.eu/doc/document/ST-16140-2014-INIT/hu/pdf
(150)
102 For the list of the more important flexibility clauses, see Paul Voigt – Axel von dem Bussche: The EU General Data Protection Regulation (GDPR): A Practical Guide. Springer International Publishing, 2017. pp. 220-222.
103 Ibid p. 219.

questioning the realisation of the expectations concerning the uniform application of EU regulations and law enforcement.

2.4. The role of the Privacy Act in the altered regulatory environment

2.4.1. General characteristics of the Hungarian Data Protection Regulation

The Fundamental Law and the international legal obligations undertaken by Hungary obligate the Hungarian legislator to guarantee the enforcement of the right to the protection of personal data as a fundamental right in all the legal relationships subject to its jurisdiction [Fundamental Law Article I(3), Article VI(3), Article Q(2); Articles 1 and 8 of the Convention on the Protection of Human Rights and Fundamental Freedoms signed in Rome on 4 November 1950, promulgated with Act XXXI of 1993; Council of Europe Data Protection Convention and its Additional Protocol].

Consequently, law-level legal regulations stipulate the rules concerning the guarantees for the enforcement of the right to the protection of personal data, seeing it as a fundamental right, the set of conditions applicable to the processing of personal data, the range of obligations for the controller and the rights of data subjects and furthermore, the rules concerning the responsibilities and powers of the institution set up to supervise the enforcement of this fundamental right.

Prior to and after Hungary's accession to the European Union until the sources of law of the EU data protection ***acquis*** – the Data Protection Directive and Framework Decision 2008/977/JHA obligated and authorised the Member State legislator to develop a set of data protection norms in their internal law, in view of the fact that these sources of law were not directly applicable, this system of legal regulations traditionally consisted of a central, horizontally applicable – ***omnibus –*** normative act extending to all data processing legal relationships and sectoral legal regulations applicable with regard to certain special data processing legal relationships [Act LXIII of 1992 on the Protection of Personal Data and the Accessibility of Data in the Public Interest (hereinafter: Act on the Protection of Personal Data and the Accessibility of Data in the Public Interest), the Privacy Act and e.g. Act XLVII of 1997 on the Processing and Protection of Health and Related Personal Data (hereinafter: Health Data Act)].

The Hungarian legislator was unable to maintain this set of internal norms, because the legal acts adopted under the framework of the data protection reform of the European Union had a different character in terms of the source of law than before the reform. While the Act on the Protection of Personal Data and the Accessibility of Data in the Public Interest and the Privacy Act complied with the law harmonisation obligations stipulated by both the Data Protection Directive and the Framework Decision 2008/977/JHA within their respective sets of norms, the Hungarian regulatory environment had to be reviewed because of the directly applicable normative requirements of GDPR.

In the course of this review, the legislator had to develop the Hungarian regulatory environment, taking the constitutional and international legal framework referred to above into account, so as to meet the following requirements:

1. Deregulation of the subject matter exhaustively regulated by GDPR in the legal relationships subject to the scope of the regulation;
2 Regulation of the provisions indispensable for the direct applicability of GDPR;
3 Transposition of the provisions of the Directive for Criminal Affairs into Hungarian law and the full regulation of its legal institutions in internal law;
4 Ensuring the set of conditions in the data processing legal relationships outside the scope of EU law subject to Hungarian jurisdiction;
5 Regulation of the provisions stemming from the constitutional and international legal requirements supplementing GDPR and the Directive for Criminal Affairs as enabled by EU law;
6 Ensuring the harmonisation of the special sectoral normative requirements regulating data processing legal relationships with the provisions of GDPR and the Directive for Criminal Affairs.

Parliament reacted to the regulatory need specified in points 1-5 with the enactment of Act XXXVIII of 2018 on the Amendment of Act CXII of 2011 on the Right to Informational Self-Determination and the Freedom of Information related to the data protection reform of the European Union and the amendment of other related laws (hereinafter: Amendment Act). The Amendment Act entered into force on 26 July 2018, more than two

months after GDPR became applicable; the vast majority of its provisions modified the requirements of the Privacy Act as detailed below.

The review of special data processing of legal relationships and the comprehensive amendment of the normative acts regulating them did not take place until the closure of the 2018 spring session of Parliament.

2.4.2. Implementing GDRP

Member State legislators do not have the possibility of repeating the rules of GDPR in and the regulation of the subject matter exhaustively regulated by the regulation in their internal law, because the rules of GDPR are directly applicable. In view of this, the ***omnibus*** character of the Privacy Act became unsustainable.

Because of this, the Amendment Act amended the provisions establishing the scope of the Privacy Act so that, with respect to the data processing legal relationship subject to the scope of GDPR, they do not subordinate all the norms of the Privacy Act to GDPR, only certain exhaustive provisions were to be applied in addition to the rules of GDPR, as their supplement [Privacy Act Section 2(2), Section 77/A].

In relation to these requirements, the following needs to be noted.

In view of the fact that the Privacy Act stipulates the legal provisions ensuring the enforcement of the fundamental right to the protection of personal data, together with the other fundamental right regulated in Article VI(3) of the Fundamental Law, which is the right to access and disseminate data in the public interest (freedom of information), the application of these provisions had to be ensured due to the requirements of GDPR (GDPR Articles 85 and 86), with regard to the legal relationship subject to the scope of GDPR (Privacy Act, certain provisions of Section 3, Privacy Act, Chapters III and IV, Annex 1).

The provisions of the Privacy Act on the establishment of the data protection supervisory authorities, ensuring the guarantees of their independence, the framework of discharging their responsibilities and powers (primarily

in terms of procedural law) and those which contain the guarantees of the enforcement of the data subjects' right to legal remedy by the courts can also be regarded as indispensable for the implementation of GDPR (GDPR Chapters VI-VIII and Privacy Act Section 23, Chapter V and certain provisions of Chapter VI).
The Hungarian legislator also has a legislative obligation in relation to establishing a mechanism for the "supervision of data processing operations carried out by [the courts] in the course of discharging their judicial tasks", in view of the fact that GDPR (and the directive for criminal affairs) excludes the competence of the data protection supervisory authorities with regard to this supervision, yet the substantive rules of GDPR are applicable to these activities [GDPR Recital (20), Article 55(3); Directive for Criminal Affairs Recital (80), Article 45(3)]. To handle this regulatory obligation, the Amendment Act opted for establishing an independent legal institution, the so-called data protection objection related to the data processing operations concerned and the Privacy Act regulated the procedural provisions concerning its administration in a separate chapter (Privacy Act Chapter VI/A).

In addition to the legislative steps aimed at the implementation of the regulation presented above, the Amendment Act made use of the elbowroom provided by GDPR itself for the Member State legislator at several points. Within the framework of this elbowroom, it specified the minimum requirement of normative provisions regulating data processing legal relationships called for by legal regulation, the so-called mandatory data processing activities, in accordance with Hungarian data protection legal doctrine addressed to the legislator in accordance with the constitutional requirements concerning the restriction of fundamental rights by way of legislative measures [GDRP Article 6(1)(c) and (e), 6(2) and (3), Privacy Act Section 5(3) and (5)].

Furthermore, it should be underlined at this point that the Amendment Act maintained the earlier regulatory approach of the Privacy Act, so it continues to call for the application of the rules concerning the conditions of processing special data as a main rule regarding the processing of personal data related to criminal affairs [Privacy Act Section 5(7)]. The reason for this is that although the General Data Protection Regulation

does not regulate "decisions related to the establishment of criminal liability and personal data related to criminal acts" (GDPR Article 10) not as personal data belonging to "special categories of personal data" (GDPR Article 9), it renders their processing conditional upon the enactment of Member State legal provisions "providing appropriate guarantees". However, GDPR itself does not define the character and content of such guarantees, so the Privacy Act settles this issue essentially with a content corresponding to the regulation prior to the data protection reform in accordance with the provisions of Article 6 of the Council of Europe Data Protection Convention.

2.4.3. Transposing the Directive for Criminal Affairs

As shown earlier, prior to the data protection reform of the European Union, unlike EU legislation, the Privacy Act regulated the general provisions applicable to data processing operations subject to Hungarian jurisdiction functioning as a Code, so its provisions served compliance not only with the data protection directive but with Council Framework Decision 2008/977/JHA as well.

Although the structure of the Directive for Criminal Affairs and most of its definitions and legal institutions are identical with GDPR in terms of their content and text, the Directive for Criminal Affairs – unlike GDPR – is not in effect and it is not directly applicable in internal law with the exception of the prevalence of specific conditions stipulated in EU judicial practice. As a consequence, the law harmonisation obligation binding the Hungarian legislator with respect to the Directive for Criminal Affairs compels it to transpose the full range of these legal institutions and definitions into internal law and regulate them at the level of law due to Article I(3) of the Fundamental Act.

At the same time, legislators in Member States have significant elbowroom with respect to the transposition of the Directive for Criminal Affairs. On the one hand, this elbowroom permits the regulation of the provisions of the directive either by a central norm to be applied to all data processing legal relationships subject to it, or settle them separately in sectoral regulations; on the other hand, the minimum harmonisation character of the directive also allows for providing „guarantees granting a higher level of protection" than those set forth in the provisions of the directive [Directive for Criminal Affairs Article 1(3)].

In view of the fact that the nature of the obligation for law harmonisation did not change with the adoption of the Directive for Criminal Affairs relative to Council Framework Decision 2008/977/JHA, the Amendment Act maintained the earlier regulatory approach and inserted the provisions of the Directive for Criminal Affairs into the Privacy Act, and called for the continued application of the provisions of the Privacy Act with respect to the processing operations subject to the Directive for Criminal Affairs, i.e. processing for law enforcement within the meaning of the Privacy Act (Privacy Act Section 3(10a)). Utilising the elbowroom provided by minimum harmonisation character of the directive, it also maintained „guarantees granting a higher level of protection", retaining a stricter set of conditions for certain legal institutions relative to the directive, overtaking the data protection reform [see, for example, Privacy Act Section 5(7) with respect to processing criminal personal data].
So, the Privacy Act regulates the full range of the legal institutions under the Directive for Criminal Affairs, it is applicable as ***lex generalis*** for processing legal relationships subject to the directive, which is identical to the previous regulatory concept, where in addition to these norms the regulation of legal provisions applicable to specific processing legal relationships also prevail in this area of the law. With this general regulatory demand, the Privacy Act strives to specify the broadest possible range of provisions to be applied – in the absence of provisions specifying sectoral regulatory deviations – for the data processing legal relationships. It follows from this endeavour and based on experience from previous legislation and law enforcement, that the Privacy Act provides background rules to an even greater extent relative to earlier regulations, thus, for example, it determines the interval at which the need for processing should be regularly reviewed [Directive for Criminal Affairs Article 5; Privacy Act Section 5(5)], the detailed conditions under which the data subjects' rights may be restricted and the underlying reasons of the restrictability [Directive for Criminal Affairs Article 13(3), 15(1), 16(6);, Privacy Act Section 16(3), 21(3)].

2.4.4. Regulating legal relationships not regulated by EU law

As presented earlier, the EU data protection provisions cannot be applied to certain legal relationships involving the processing of personal data

due partly to regulatory categories not affected by the Treaties, and thus remaining subject to the exclusive jurisdiction of the Member States, and as a consequence of the self-restrictions by legal acts adopted within the framework of the data protection reform. With respect to these categories, the regulatory powers of the Hungarian legislator and its regulatory obligation arising from the Fundamental Act has survived.

On the one hand, based on the consideration that the Privacy Act should retain its code character even in the changed regulatory environment, and in view of the identical features of the data processing legal relationships linked to Hungary's external and internal security (e.g. the activities of public authorities involving the restriction of fundamental rights, regulated in detail by law), with regard to data processing for national security purposes (Privacy Act Section 3(10b)) and data processing for defence purposes (Privacy Act Section 3(10b)), as legal relationships within the circle of activities outside the scope of EU law [GDPR Article 2(2)(a); Directive for Criminal Affairs Article 2(3)(a)], the Amendment Act – as a general rule – called for the application of the set of rules concerning processing for law enforcement purposes, i.e. all the provisions of the Privacy Act [Privacy Act Section 2(3)].

Following from this regulatory solution, the Privacy Act specifically denotes the objective scope of every provision that deviates from the general scope in regard to which this uniform approach is not realized because the given provision serves exclusively the purpose of meeting a regulatory requirement that prevails with respect to one or other of the types of processing legal relationships [e.g. Privacy Act Sections 7, 10(2) or 25/E(4) and 25/J(9)].

As indicated earlier, the legislator of the European Union continued to insist on the approach even after the EU data protection reform which excludes the application of the EU legal acts with respect to data processing operations ***not*** done by automated means that focus on personal data that ***do not*** constitute part of a registration system and which ***are not*** be made part of a registration system [GDPR Article 2(1) of, Directive for Criminal Affairs Article 2(2)].

However, Hungary availed herself of the opportunity provided by the Council of Europe Convention on data protection when acknowledging its binding scope, and undertook the obligation in a declaration considered as a unilateral international legal act to apply the provisions of the Council of

Europe Convention on data protection to files of personal data processed with non-automatic means (Act VI of 1998Section 3). In line with this undertaking, the Hungarian legislator set the objective scope of both the in the Public Interest and the Privacy Act for data processing operations done generally and horizontally by automatic means as well as manually until the Amendment Act enters into force. [See: Act on the Protection of Personal Data and the Accessibility of Data, the text of Section 1/A(2) in force on 31 December 2011, Privacy Act, the text of Section 2(2) in force on 25 July 2018.]

The change in the source of law nature of the EU data protection *acquis* – and the resultant change in the scope of the Privacy Act – necessitated modification with respect to these data processing operations. With regard to the fact that the differentiation between the data processing relationships regulated and not regulated by EU legislation is based only on the mode and the method used to execute the data processing operations – the implication of the aspect in regard to the relevant fundamental right can be justifiably challenged – the Amendment Act rendered EU legal and internal legal systems of norms concerning data processing operations by automated means applicable to the latter relationships also.

Thus, in accordance with this concept, the Privacy Act maintains the previous regulatory approach and – without differentiating the automated and the manual data processing operations – provides for the enforcement of the provisions of the Privacy Act to the full range of data processing operations for criminal, national security and defence purposes [Privacy Act Section 2(3)]. As to all other data processing operations – that would be subject to GDPR based on their specificities apart from the mode of data processing, but which are outside the scope of the Regulation based on Article 2(1) – the Privacy Act ex lege calls for the application of the substantive legal provisions of GDPR [Privacy Act Section 2(4)]. This regulatory solution makes it possible for enforcement bodies subject to Hungarian jurisdiction to apply uniform data protection provisions within the framework facilitated by EU and international legal capabilities with respect to data processing operations irrespective of the means or methods used by the controllers and processors employed for data processing.

Finally, as regards the legal relationships not regulated by the EU legislator, the provisions of the Amendment Act are to be highlighted as regulatory

novelties that provide legal instruments for settling the fate of personal data after the death of the data subject, both for the data subject and his close relatives. Considering that a data subject ceases to be an entity upon his death, mutatis mutandis, he cannot be party to a data processing relationship from his death. So, the scope of the general regulation does not extent to regulating the fate of the personal data of the deceased, although it specifically indicated in this respect the regulatory elbowroom for legislators in the Member States [GDPR Recital (27)]. This regulatory elbowroom was utilised by the Hungarian legislator also with a view to meeting the regulatory needs signalled by Hungarian enforcement practice [Recommendation by the Hungarian National Authority for Data Protection of Freedom of Information on the fate of online data after death[104]] by creating specific legal institutions hitherto unheard of in Hungarian law, but experience about their practical application are obviously not available yet (Privacy Act Section 25).

104 https://www.naih.hu/files/Ajanlas_online-adatok-halal-utani-sorsarol.pdf

Literature:
European Union Agency for Fundamental Rights:

Handbook on European data protection law – 2018 edition. Publications Office of the European Union, Luxembourg, 2018

Orla Lynskey:

The Foundations of EU Data Protection Law. Oxford University Press, Oxford, 2014.

Alexander Roßnagel – Maxi Nebel:

Due Neue Datenshutz-Grundverordnung – Ist das Datenshutzrecht nun für heutige Hereausförderungen gerüstet? Fraunhofer-Institut für System- und Innovationsforschung ISI, 2016 [Date of access: 10.08.2018.]

https://www.fru.privatheit.de/foru-privatheit-de/publikationen-und-downloads/veroeffentlichungen-des-forums/positionspapiere-policy-paper/PlicyPaper-5-Die-neue-DSGVO_1.-Auflage_Mai_2016.pdf

John Tomaszewski:

„Opening Clauses" and the GDPR – It Might Not Be As Easy As We Though; 03.07.2017. [Date of access: 09.08.2018.]

http:/www.globalprivacywatch.com/2017/07/opening-clauses-and-the-gdpr-it-might-not-be-as-easy-as-we-thought/

Paul Voight – Axel von dem Bussche: The EU General Data Protection Regulation (GDPR): A Practical Guide. Springer International Publishing, 2017.

Contents

National Authority for Data Protection and Freedom of Information

1055 Budapest, Falk Miksa u. 9-11.
Postal address: 1363 Budapest, Pf. 9.

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

Published by: National Authority for Data Protection and Freedom of Information
Publisher: Dr. Attila Péterfalvi, President