A. PETERFALVI

Prof. Dr. Attila Péterfalvi, *Parliamentary Commissioner of Data Protection and Freedom of Information*

THE LEGISLATION OF THE RIGHT FOR PROTECTION OF PERSONAL DATA AND THE RIGHT TO DISCLOSURE OF INFORMATION OF PUBLIC INTEREST IN HUNGARY

The circumstances of the evolution of legal regulation for data protection and freedom of information and the circumstances of the formation of the Ombudsman's Office are well known. The Constitution enacted after the change of regime in 1989 guaranteed the right to protection of personal data and freedom of information as a constitutional right. After that, three years were to pass before the relevant statute was enacted and three further years before the Parliamentary Commissioners who were to supervise the enforcement of this constitutional right would be confirmed in their positions. Although the process for preparation of the DP&FOI Act started in the mid 1980s and the Government requested the Minister of Justice in January 1989 to introduce the necessary bill by the end of December 1990, Act LXIII of 1992 on the Protection of Personal Data and the Disclosure of Information of Public Interest (henceforth the "DP&FOI Act") was only promulgated on 17 November 1992. The deadline (1 October 1993) for the Commissioners' elections passed without avail. Although the President of the Republic heard the candidates, their election by Parliament was unsuccessful. Finally, the Parliamentary Commissioners took up their positions on 30 June 1995.

The preparatory drafts of the next significant amendment to the DP&FOI Act commenced in 2001. Due to the legal harmonisation programme of the Government, the revision of the DP&FOI Act was planned in the legislation programme of the second part of 2001, in the interests of precise harmonisation with the 1995 Directive. The materials that were produced during the preparation of the proposal were sent at the end of March 2001 to the first Hungarian Data Protection Commissioner. Considering that it was not a worked-out draft, the Commissioner did not make any remarks. Meanwhile Dr. Lбszly Majtйnyi's term had run out. At the end of July, the Ministry of justice sent the draft of the "Act on the Protection of Personal Data and Access to Data of Public interest" to the Parliamentary Commissioner for Human Rights who had been substituting for the Data Protection Commissioner. The proposal contained basic changes to the original conception. It planned to codify the rules of the protection of personal data and the access to data of public interest in two separate Acts; it introduced new concepts in connection with the processing of personal data; and it provided for several new tasks for the Commissioner (investigations of automated individual decisions; issuing binding decisions by ordering the blocking, deletion or destruction of unlawfully processed data; participation in the legal proceedings; prior checking; as well as the right to form opinions on legislative proposals concerning data of public interest).

In 2001, the Commissioner proposed an important amendment to the legislator in the interests of the enforcement of data protection and freedom of information: "Over the almost six years since I took up my position as Data Protection Commissioner, I have often had to face the fact that the deficiencies of our rules weaken sanctions under criminal law as one of the major guarantees of privacy and freedom of information. This is because the Criminal Code, in providing assurances for these two fundamental rights, assigns excessively broad limits to criminal liability by imposing sanctions on acts that could well be tackled by means other than those of criminal prosecution. In addition, the notions used by the Code do not precisely correspond to the dogmatics of data protection law"[1]. The Commissioner issued a

Recommendation to the Minister of Justice in which he stated that no illegal control of data should carry a punishment under the Criminal Code unless using such force was inevitably called for and justified. The terminology of the Criminal Code should be aligned with that of the Act in the interests of promoting uniform legal practice. Felonies involving personal data should not be discussed in the same section as felonies involving data of public interest. The Commissioner proposed that the definition of such felonies should be reclassified as misdemeanours. Following that, the legislator mitigated the strictness of this crime, but did not elaborate the conditions for applying sanctions. Therefore the Commissioner initiated the amendment with the Minister of the Interior in 2003, asking again for the possibility to punish the violation of data protection, at least as an offence if there were a minor violation. Relating to his examinations concerning the Internet, he proposed to the legislator to harmonise the transborder data-flow with the Directive 94/46/EC. For the introduction of the electronic freedom of information, he asked for the legislation to prescribe the list of data of public interest which must be published. According to him, it would be important to create the legal conditions for protection against attacks from hackers, the regulations for spam and the rules for processing traffic data[2].

In the Government's Work Plan for the second half of 2002, the revision of the DP&FOI Act could also be found. The first version was much modified after a broad discussion, but the Government still proposed the version of two Acts. In his opinion on the drafts, the Commissioner stated that "the categories and some rules surely will have an effect on developing the legal culture, but the draft gives no answer to the question why it is necessary to separate these rights into two statutes, by abandoning in this way the Hungarian method of regulation which is, incidentally, very well recognised abroad. We also criticise the fact that the draft intends to abandon the logic of the Act and the relevant EU Directive, that is to say that W condition for lawful data processing is the con-sent of the data subject or the ordering of an Act"[3].

This idea of separation emerged in the proposals up until 2003. Although neither the Commissioner's Office nor the new Commissioner after his 2002 election ever considered this concept well-founded, it was not enough to convince the Ministry of Justice. In fact the reason for abandoning this idea was that a pro-found codification was needed but because of the short time-limits and the large number of tasks about EU accession, it was not possible. Nevertheless, it is important to mention that this proposal was the basis and starting point for the subsequent amendments to the DP&FOI Act in 2003.

The year of 2003 – as far as legislation was concerned – was the year of data protection and freedom of information. After a long preparatory work, after many consultations, and revisions, a new Data Protection Act came into being. The Act on Secrecy was the result of a long legislative process too, and the Act on the so-called "Glass-pockets Programme" also came into force.

The amended DP&FOI Act[4] mainly extended the Chapters regarding data control and invested the Commissioner with new powers and competences. It was reasonable to determine – taking the Directive into consideration – the personal and objective scope, as well as the territoriality in the amended Act. Therefore the scope of the DP&FOI Act now covers all personal data processing and data transfer within the territory of Hungary, regardless of the citizenship, place of residence, or seat of the data controller/processor. The provisions of the Act apply to data processing and data transfer operations whether they are performed by an automated process or by manual processing, but not where data is processed by a natural person exclusively for his own purposes.

Due to the new rules of the DP&FOI Act, the scope of special data was amended in respect of trade union membership, although the Commissioner had already classified it as special data in his practice, because it might refer to a political opinion. In the second group of special data (personal data concerning health, addictions, sex life, or criminal record), the opinion of the Data Protection Committee of the Council of Europe was taken into consideration: the amended DP&FOI Act accordingly includes personal data relating to criminal offences, rather than personal data concerning criminal records. To this category belong such personal data that might be related to the data subject and that was obtained by organisations authorised to con-

duct criminal proceedings or investigations or by criminal institutions during or prior to criminal proceedings in connection with a crime or criminal proceedings; and data concerning criminal records.

The definition of data public on the grounds of public interest was introduced as a new definition which now means any data not regarded as personal data that are managed by a state or local public authority or agency or by any other body attending to public duties specified by law and is not to be disclosed for the benefit of the general public.

As a principle according to the amended DP&FOI Act, personal data may be processed if the data subject has given his consent, or decreed by law, though the amended Act did not include any rule in connection with the consent or the making of such statement. The Commissioner in his case-law has consistently applied the provisions of the Directive, which provides for the fact that the consent has to be freely given, and amount to a specific and informed indication of the data subject' wishes. Due to the 2003 amendment, the said provision has now been included in the amended DP&FOI Act. The data subject has the right to object to the processing of his personal data, and may request the ending of such operation or erasing/removal of such data.

In according with the demands of the 1995 Directive, the amended DP&FOl Act has been modified with a general enumeration, which includes that personal data may be processed – either with the data subject's consent or when ordered by a legal rule – in particular, where it is necessary: for the performance of a task of public interest; for the data controller to perform his obligations prescribed by an Act; for the data controller or data recipient third person to perform their official duties; for the protection of the vital interests of the data subject; for the meeting of the obligations laid down in the contract between the data subject and the data controller; for the assertion of a legitimate interest of the data controller or a third person; or for the lawful operation of social organisations.

In order to fulfil the requirements set out in the Directive, the amended DP&FOI Act now provides that criminal personal data – for the purpose of performing the State's tasks of criminal investigation, crime prevention, as well as public administration and judicial tasks, and data files pertaining to minor offences, civil actions and non-litigious cases – may only be processed by state or local government organs.

The data subject retains the right of self-determination regarding his own data: he may thus decide on the delivery of his data, may request its rectification and – with some exceptions – may ask for the deletion of his data. After the 2003 amendment, the deletion of personal data may also be ordered by the Data Protection Commissioner and the Municipal Court of Budapest. The data subject must be informed of any rectification or deletion. Such information may be dispensed with if, in view of the purpose of processing, no legitimate interests of the data subject are thereby infringed. The rights of the data subject may be restricted by an Act. After EU accession, the abovementioned right may be restricted by an Act for important economic or financial interests of the European Union.

In order to comply with the Directive, a new rule was introduced into the DP&FOI Act, namely the right to object to data controlling or processing. Such right may be exercised when data controlling serves the sole interest of the data controller or a third person, that is to say the data control/transfer occurs for the purpose of, e.g., direct marketing, public opinion research or scientific research. The Act itself renders it possible to exercise this right to object: it sets out the time-limits regarding the procedure and the obligations of the data controllers in connection with the right to object. If the data subject is not able to exercise his right, he may institute court proceedings.

Previously there were few examples of requesting the Commissioner to give his opinion before the data controller would commence its activity: after 1 January 2005/6, it became mandatory in the case set out in section 31 of the amended DP&FOI Act. The major data controller (national authorities, or national labour or criminal data registry, financial organisations or public utility providers as well as telecommunications service providers) must notify the Data Protection Commissioner of their intention to process technically new data files or to apply a new technical data processing technology 30 days prior to commencing such activities and, if the Commissioner so decides, he may perform a prior check. On the basis of the check,

the Data Protection Commissioner may call on the data controller to change the range of data to be processed or the method of technical data processing.

Upon observing any unlawful processing of data, the Data Protection Commissioner is to call on the data controller to discontinue the data processing. If the data controller or technical data processor fails to discontinue the unlawful processing (technical processing) of personal data, the Data Protection Commissioner may order in a decision the blocking, deletion or destruction of unlawfully processed data, prohibit the unlawful processing or technical processing of data, and suspend the transfer of data to foreign countries. The data controller, the technical data processor or the data subject may request judicial review from the Municipal Court of Budapest against the decision of the Data Protection Commissioner.

The amended DP&FOl Act leaves several questions open. The procedural rules of acting as a public authority are not determined. There are no such rules which would lay down the method and the formal criteria for ordering, blocking, or suspending, although these rules are indispensable. It is still a question as to what happens if the data controller neither stops the unlawful data processing, nor requests a judicial review, considering that the Commissioner does not have any further authorisation beyond the ordering (e.g., imposing a fine, ordering enforcement). The amended DP&FOI Act does not provide for in what kind of proceedings the matter should come before the Municipal Court of Budapest for trial. In 2004 there were two occasions when the data controller filed a case against the Commissioner. In the first case, the data controller withdrew his action, the other case is still pending. The case was filed due to the general rules of the Code on Civil Procedure because of the violation of personal rights; the data controller was holding the position of the plaintiff while the Commissioner was protecting the rights of the data subjects as the defendant. So the revision and the amendment of these rules is needed, with the result that the necessary actions should take the form of administrative proceedings.

The abovementioned major data controllers are required to appoint an internal data protection officer and draw up their internal data protection and data security rules. State and local government data controllers are also required to adopt data protection and data security rules.

In 2003, Parliament also adopted the "Glass-pockets" Programme which amended 19 Acts[5]. The purpose of the new Act was to ensure the Publicity, Transparency and Control of the Appropriation of Public Funds and the Use of Public Property. After many consultations, all of the Commissioner's remarks were incorporated into the Act. The Act (and its implementing Decree) made headway in the field of freedom of information because the legislator ended the contradiction between the definition of business secret and data public on the grounds of public interest. Through the introduction of the definition of data public on the grounds of public interest, the legislator extended the freedom of information to the organs of private sector which are in a business or financial relationship with government. The Act also contained the obligation that publication on the website referred to a broad range of data of public interest relating to government; as well as all organs in government being required to appoint a person or an entity bearing the special knowledge needed in order to publish the data of public interest.

The Ministers and chapter-holders must prepare an action plan. Such plan is intended to inform the citizens clearly and authentically; to examine the scope and range of data, and whether or not they should be published; and to make proposals regarding those Acts which should be amended in order to comply with the obligation of publishing data of public interest. Lastly the Ministers and chapter holders have to consult with the Minister of Finance on the supplementary financial contributions when executing the tasks required by the Action Plan[6].

As the result of long preparation work, Act LIII of 2003 on the Amendment to Act LXV of 1995 on State and Official Secrets (the "Secrets Act") also entered into force in 2003[7]. With EU accession, it was necessary to modify the system of secrets classification, that is to say, to introduce the four-level, damage-based classification system together with the repeal of the automatic nature of the classification system, while implementing the EU classification system into Hungarian law. The EU did not consider it to be reasonable to accept a large volume of highly-classified data, and therefore those provisions which had required such classification needed to be repealed.

With the introduction of the four-level, damage-based classification system, the number of the types of the secrets has not been altered: however there are more levels of protection available, the state secret being classified now as "Strictly Confidential!" The classifier decides on whether a piece of data should be classified as a state or official secret, and decides on the choice of the most suitable classification from the point of view of the protection of the relevant data; this method therefore amounts to a flexible tool to assist in observing the rule for proportional cost of the protection. The Commissioner was of the opinion that the amendments to the text, which were built at the last moment, might be questioned from the point of view of data public on the grounds of public interest and might lead to inconsistency in the secrecy rules. "The main concept in the correction of secrecy rules was to repeal those provisions which required the classification automatically. The purpose was partially achieved. Act CXXV of 1995 on the National Security Services still includes "ex lege" provisions which give rise to classification of secrets. [Sections 30(4), and 42(1), and the questionnaire of the national security control in the annex are such.]"

The annex unnecessarily determines the criteria of the classification of "Strictly Confidential" because this-and only this-classification can apply to every state secret. And it may lead to problems in the scope in that the criteria of the classification as state secret do not coincide with the definition of the state secret in the Act. The inner coherent problems of the rules may obstruct the classification of data as state secrets, although the constitutional criteria for restricting publication exist.

It is doubtful that the official secret – due to the concept of the legislator – is able to play the part of the "soft state secret, "as there is no difference in the grading between state and official secrets, but – regarding the different protected subject of the rules – there is a difference in quality"[8].

One of the reasons for the amendment of the DP&FOI Act in 2005 was the unconstitutional regulation of "data that relates to the decision-making process or for internal use only." The Constitutional Court in Decision 12/2004 (IV.7) AB held that the legislator did not guarantee, to an acceptable constitutional level, the safeguards of the right of access to data of public interest. As a result of this Court Decision, it was no longer reasonable to restrict the right of access to data (of public interest) when it only served the interests of making the decision.

The definition and the scope of "data relating to the decision-making process and for internal use only" is incorrect and indeterminate, therefore the application of these definitions mean an unnecessary and ill-proportioned obstruction on the fundamental right to freedom of information. Regarding this, the Constitutional Court held that the legislator did not differentiate between the restriction on the publicity of data relating to the decision-making process before or after the decision, since the data controller only has to claim that the data relates to the decision-making process and it is only for internal use. The fact that such data came into being during the day-to-day activities of an organ performing public duties, and it is in connection with the decision-making process, is not an adequate reason to lock it away from the public. When examining data for internal use, other subjective factors may be taken into consideration, as the data is not protected due to the contents, but due to the intention of the "creator" of such data. "On the one hand, such restriction is possible if section 19(1)-(3) of the DP&FOI Act applies;, on the other hand, when access to the data would threaten the legal order of operation or the performance of the sphere of tasks and powers, without unauthorised external influence of the organ. The viewpoints of the organs and persons performing public duties may not be preferred against a fundamental right. Section 19(5) would suit to requirements of the Constitution if the legislator clearly sets the purpose of the restriction of freedom of information, adequately determines the scope of data to be locked away from the public, and restricts the recognition of data of public interest in a necessary and proportionate measure."[9] Another problem is that the restriction of the publicity set out in section 19 (5) of the DP&FOI Act may be sustained for an indeterminate period of time, as its span has to be counted from the start of the data control (the storage is also considered to be data control). The Constitutional Court ruled in its Decision that the legislator did not guarantee the content revision on the restriction of freedom of information, and the possibility of the effective legal remedy. Due to the DP&FOI Act, the legal remedy refers only to formal aspects in the Act.

"The compelling reasons for limitation of publicity and/or the lack of legal redress of its revision, enable the unjustified limitation of access to data of public interest, i.e. of the constitutional right concerning publicity of data public on the grounds of public interest, depending on the discretional decision of the organ processing the data."

The amendment to the DP&FOI Act in 2005[10] was justified by the abovementioned Decision of the Constitutional Court, the abolition of the unconstitutionality being manifested in failure. At the same time it was a good opportunity to introduce precise definitions connected to processing of and access to data of public interest, as well as the rules of the powers and procedural rights of the Data Protection Commissioner.

The 2005 Amendment Act refined the definition of data of public interest. It made clear that any knowledge or recorded information – irrespective of the data carrier or of the manner in which it was processed together with the independent or collected character of the data – was to be regarded data of public interest. The definition of data public on the grounds of public interest has also changed: it means any data, not falling within the definition of data of public interest, the making public or accessibility of which is provided for by an Act.

The right of access to data of public interest can be limited because of legal proceedings and, following the amendment of the DP&FOI Act, this limitation has now been extended to binding administrative proceedings.

Following the 2005 legislative amendment, the DP&FOI Act defines the personal data of persons exercising public duties – related to the tasks of these per-sons – as data public on the grounds of public interest and has made the access to it free to anyone. At the same time, in the case of public servants and civil servants, there are some data which still cannot be accessed (e.g. the public servant, civil servant register). The explanation for this is that the "Act" in the definition of data public on the grounds of public interest does not refer to the DP&FOI Act, and neither the Act on Public Servants, nor the Act on Civil Servants provide for the publicity of or access to these data.

The 2005 Act amending the DP&FOI Act gave a content definition to the scope of data which fall under the automatic limitation of publicity. The access to data which have been prepared before the decision-making by an organ or person exercising public functions in its/his scope of duties and powers as well as the data "establishing the decision", can be limited for ten years. The notion "establishing the decision" refers to the aims of the preparation or the recording of data, there-fore its applicability does not depend on the fact whether there has actually been a decision made or not on the basis of data establishing it. Following the decision-making, the request to access can only be refused by the head of the organ according to the Act, if he can prove that the access to data would endanger the lawful functioning of the organ or the conduct of the scope of duties and powers of the organ, free from any external unauthorised influence.

According to the amended DP&FOI Act, everyone may request access to data of public interest in any form (orally, in writing or electronically). The access to data of public interest published electronically cannot be bound to registration; personal data can only be processed to the extent which is indispensable from a technical point of view. In the case of a request on the basis of the purpose-bound nature of data processing, only those personal data can be processed which are necessary to the paying of the costs and the fulfilment of the request.

The amended DP&FOI Act further elaborated the powers of the Data Protection Commissioner. On the basis of the DP&FOI Act, the Commissioner represents the Republic of Hungary in the joint supervisory bodies of the European Union. The amendment of the DP&FOI Act unambiguously clarified the procedural question not then settled: as a result, the Data Protection Commissioner makes a decision after his investigation concerning unlawfully-processed personal data, the judicial review of which can be initiated according to the rules on administrative proceedings in the Code on Civil Procedure.

In 2005 with the legal regulation of electronic freedom of information[11], citizens can more easily and more efficiently access data of public interest. The Act on Electronic Freedom of information provides for the obligation of electronic publishing of data of public interest and data public on grounds of public interests and its content, makes the legislative procedure more open with the help of the Internet, ensures access to the digital version of legal rules, and

enables access to the anonymised decisions of the Supreme Court and the Courts of Appeal.

The provisions of the Act on Electronic Freedom of information will take effect gradually so as to give enough preparation time for each organ/organisation bound by the Act. It is the obligation of the organs bound by the Act to maintain a website, and to update data of public interest published there. The requirement for electronic dissemination extends to all those data which serve the entering into contact with the organs exercising public functions, the making use of their services, and the transparency of their operation/financial management. Of course, the obligation of dissemination does not exempt the organs exercising public functions from making available their specific data of public interest to the person so requesting.

The Act on Electronic Freedom of Information provides that draft legislation is to be published on the website of the relevant Ministry with information on the status of the negotiations, in order to ensure the publicity of the legislative procedure. There are species of regulative subject-matter and interests which supersede the required publicity of the legislative procedure, and here publishing can be omitted: these are listed by the Act. It cannot be expected from the citizen using Internet that he knows which Ministry is responsible for which draft legislation and therefore the database of draft legislations has to be published on the Government's website.

The third field which is regulated by the Act on Electronic Freedom of Information is the publicity of legal rules, which is realised in the sense that the authentic text of the legal rules is available on the Internet for everyone. The Act provides for the obligation of publicity on the Internet of the Hungarian Official Gazette (Magyar Kцzlцny) and of the Official Journals of the Ministries. For the practical application of the published legal rules and for learning the case-law of the Supreme Court and the Courts of Appeal, the decisions on the merits of the court cases must be made available electronically (the Act exempts some decisions from the obligation of publication). The access to the published decisions can-not be limited, but the decisions published have to be anonymised in order to protect rights to informational self-determination and personality rights.

The Europol and the Schengen Conventions

The transposition and application of these two Conventions into Hungarian legislation was not without difficulties from the point of view of the establishing of an independent national supervisory authority. Because of the uncertainty of the procedural powers, conflicts of competence arose between the Europol Data Protection Supervisor and the Data Protection Commissioner during Hungary's representation in the European Union. The introduction of the legislative procedure was therefore reasonable and it shows how this problem has been settled in the end and to what extent this has resulted in the change of powers of the Data Protection Commissioner.

The Data Protection Commissioner in his 1997 Annual Report outlined three organisational solutions for the Hungarian management of the international police, and law-enforcement information system regarding EU membership and with it accession to the Europol and Schengen Conventions. The task could have been fulfilled by the Data Protection Commissioner, who could have guaranteed the utmost independence. At that time the Commissioner did not find this solution expedient because "The soft powers of the ombudsman would have to be accomplished by hard administrative powers, which in the case of a parliamentary supervisory organ is a question concerning the system and balance of branches of power and gives rise to concerns about the organisation of the State and the Constitution"[…][12].The second solution was the establishment of a central government organ supervising administrative data processing, which would have been expensive and bureaucratic as it would have meant an organisation split on different decision-making levels, and, as a result, its operation would not have been efficient enough. The third solution was that more organs of public authority, independent from the police, would have to be established in different administrative branches and sectors.

In the 1998 Annual Report, the Commissioner urged the fulfilment of legislative tasks connected to the EU law-enforcement information system, because the Europol and Schengen Conventions require the setting-up of a national information subsystem, the data protection supervision of which has to be carried out by an independent supervisory organ. Pursuant to

the elaborated draft legislation, the supervisory organ would be under the supervision of the Government, which solution brought into question its independence to a great extent.

Act LIV of 1999 entered into force in 1999 as the result of legislative work relating to the accession to the EU law-enforcement information network[13]. The earlier draft bill (according to which the supervisory organ to be established was to have been under the supervision of the Government) had been modified in a way that the Data Protection Supervisor appointed by the Prime Minister was responsible for the data protection supervision of the data-transferring activities of Europol. The setting-up of an independent national authority had also not been realised with this legal provision because the employer's right, in connection with the public servant legal relations of the Data Protection Supervisor (with the exception of appointment and removal), was exercised by the Minister of the Interior; therefore the position had been integrated into the structure of the Ministry of the Interior. The 1999 Act addresses the most important questions connected to data protection only generally, and does not even determine the scope of data which can be processed by the international Law Enforcement Co-operation Centre („ILECC"). The Commissioner objected to the draft legislation of the Ministry of the Interior on the functioning of the ILECC because "this organisation – according to the aim of the Act – is not an organisation entirely co-ordinating the international functioning of the police and other law-enforcement organs, but an organisation processing two definitely separated databases, which are not at all, or hardly known, today. The ILECC can only perform the exchange of information between the centres of Europol and Interpol and their national units, offices with very strict data protection control. Any further exchange of information delegated to the ILECC conflicts with the provisions of the Act, questions the obligation of tracing and controlling the data transfers, and can make the operation of the 'independent' Data Protection Supervisor formal[14].

During the amendment of the DP&FOI Act in 2005 and in order to comply with Article 24 of the Europol Convention, section 24 of the DP&FOI Act was supplemented with the provision according to which the Data Protection Commissioner represents the Republic of Hungary in co-operation with organs and persons determined by a separate Act in the joint supervisory bodies of the European Union. This provision amended section 11(3) of Act LIV of 1999[15] so that the Data Protection Commissioner now co-operates with the Data Protection Supervisor in fulfilling this representation.

The draft Decision of the Council on the establishment, operation and use of the second generation Schengen Information System („SIS II") and the draft Regulation of the European Parliament and of the Council provides that the independent supervisory authority – appointed on the basis of article 28(1) of the 1995 Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data – supervises the lawfulness of the processing of personal data in SIS II on the territory of the Member State. The Office of the Data Protection Commissioner disposes over the organisational independence and powers which the Directive requires. The Data Protection Commissioner participated in the meetings of the joint supervisory bodies as an observer, in his capacity as the appointed supervisory authority.

Act XIV of 2006 promulgated the Europol Convention[16]. The Convention states that, in the field of police co-operation, particular attention is to be paid to the protection of individuals' rights especially to the protection of personal data. Section 14 of the 2006 Act repeals sections 11-15 of Act LIV of 1999[17], which provided for the legal status of the Data Protection Supervisor, as well as section 16 of the 1999 Act which states that the Data Protection Commissioner is responsible for the tasks under Article 23 of the Convention.[18] Regulation 648/2005/EC of the European Parliament and the Council provides for the application of the data protection Directive for data-processing in connection with the Community's Customs Code: therefore, in this field too, the national data protection authorities exercise supervisory tasks.

The powers of the Ombudsman

Looking at the development of the DP&FOI Act, it is notable that the "soft" Ombudsman powers and role without binding effect have changed to a considerable extent during the last 11 years. Today the Commissioner can order the blocking, suspension and deletion of data, i.e.,

he disposes over decisive authoritative powers. The analysis thereof, to what an extent the Data Protection Commissioner and his Office fits into the institution of the ombudsman with these new powers, as a result of the significant amendments of the Act, could be the subject matter of a specific essay. Experts of informational fundamental rights share different views on this solution. Time has passed by and the experience gained since the amendment of the DP&FOI Act has been too short to declare unambiguously whether the change has taken us into a good or bad direction.

One can however state that, despite of the existence of strong powers, the Office of the Data Protection Commissioner does not function as an "authority," and even the Commissioner is very cautious about using his powers in this matter. Following the legislative procedure, it is clear that the initiative to establish the independent national supervisory authority outside the Ombudsman institution failed. The reasons for this are very complex and the analysis of them can-not be accomplished in this essay. The Annual Reports of the Commissioner also reveal that, with the development of the information society, ever more significant data concentration efforts appear both on the side of the State and of the private sector and the fight against these have not always been successful. One also has to mention that the amendments to the DP&FOI Act were closely connected to EU accession, to the harmonisation of the national legislation with the acquis of the European Union: therefore these changes were not mere considerations, their implementation was obligatory. The Data Protection Commissioner and his supervisory tasks and powers and their transposition into Hungarian legislation are not unfamiliar to the solutions applied in the other Member States of the European Union.

---

[1] Annual Report of the Parliamentary Commissioner for Data Protection and Freedom of Information 2001, page 153.

[2] 2099/2002. (III.29.) government resolution

[3] Annual Report of the Parliamentary Commissioner for Data Protection and Freedom of Information 2002, page 128.

[4] Act XLVIII of 2003 on the Amendments to Act LXIII of 1992 on the Protection of Personal Data and the Disclosure of Information of Public Interest (the "amended DP&FOI Act").

[5] Act XXIV of 2003 on the Amendment of Specific Acts related to the Publicity, Transparency and Control of the Appropriation of Public Funds and the Use of Public Property.

[6] After the adoption of the „Glass-pocket Programme," the Government adopted Government Decree 95/2003 (VII.15) Korm. on the Amendment of Government Decree 217/1998 (XII.30) Korm. on the Functioning of Government, together with Government Decision 1096/2003 (VII. 15) on the Tasks serving the Modernisation of the Government's System of Information and Functions deriving from the „Glass-pockets" Programme in the Application of Public Funds, as well as on the Publicity of the Application of Public Property, on its Clarification, and on the Extension of the Scope of Supervision/Controls/Checks.

[7] Act LIII of 2003 on Amendments to Act LXV of 1995 on State and Official Secrets („the amended Secrets Act").

[8] Annual Report of the Parliamentary Commissioner for Data Protection and Freedom of Information 2003, Budapest, at page 165.

[9] Decision 12/2004 (IV.7) AB.

[10] Act XIX of 2005 on the Amendment to Act LXIII of 1992 on the Protection of Personal Data and the Disclosure of Information of Public Interest.

[11] Act XC of 2005 on Electronic Freedom of Information.

[12] Annual Report of the Data Protection Commissioner 1997, Budapest, at page 33.

[13] Act LIV of 1999 on Co-operation and Exchange of Information in the Framework of the European Union law-enforcement information network and of the International Criminal Police Organisation.

[14] Annual Report of the Parliamentary Commissioner for Data Protection and Freedom of Information 1999, Budapest, at page 158.

[15] On Co-operation and Exchange of Information in the Framework of the Law-enforcement Information Network of the European Union and the International Criminal Police Organisation.

[16] On the Promulgation of the Convention based on Article K.3 of the Treaty on European Union on the establishment of a European Police Office (Europol Convention) and its Protocols and on the Amendment to Act XXXIV of 1994 on the Police.

[17] On Co-operation and Exchange of Information in the Framework of the Law-enforcement Information Network of the European Union and the International Criminal Police Organisation.

[18] Article 23 of the Convention states: "Each Member State shall designate a national supervisory body, the task of which shall be to monitor independently, the permissibility of the input, the retrieval and any communication to Europol of personal data by the Member State concerned and to examine whether this violates the rights of the data subject."

Резюме

В статті розглядаються обставини, що спонукали до еволюції у врегулюваннях питань щодо захисту даних, свободи інформації, та обставини, які спонукали до формування Омбудсменського інституту. Конституція, прийнята після змін у 1989 р., визначила право на захист персональних даних і свободи інформації, як конституційне право. Але минуло три роки, перш ніж був затверджений відповідний Статут, і ще три роки перш ніж було створено парламентську комісію, яка повинна була забезпечувати дотримання цього конституційного права. Хоча робота з підготовки законопроекту про свободу інформації почалася в середні 80-х років, остаточно закон було прийнято лише в 1992 р., після чого Парламентська комісія приступила до виконання своїх обов'язків.

Ключові слова: захист даних, закон про свободу інформації, кодифікація роботи, ратифікація, конвенція, директива, інтеграція критеріїв, омбудсмен, контролер даних.

Резюме

В статье рассматриваются обстоятельства, которые привели к эволюции в вопросах касающихся защиты данных, а также обстоятельства предшествующие формированию Омбудсменского управления. Конституция, принятая после изменений в 1989 году, определяет право защиты персональных данных и свободы информации, как Конституционное право. После этого пройдет три года, прежде чем соответствующий Устав будет утвержден, и еще три года, прежде чем будет создана парламентская комиссия, задача которой контролировать исполнение этого конституционного права. Хотя работа над данным законопроектом началась в середине 1980-х, принят он был 1992 г., после чего, парламентская комиссия приступила к своим обязанностям.

Ключевые слова: защита данных, закон о свободе информации, кодификация работи, ратификация, коньенция, директива, интеграция критериев, оибудсмен, контролер данных.

Summary

In the article examined the circumstances that led to the evolution in the settlement of issues concerning data protection, and the circumstances of the formation of the Ombudsman's Office. The Constitution enacted after the change of regime in 1989 guaranteed the right to protection of personal data and freedom of information as a constitutional right. After that, three years were to pass before the relevant statute was enacted and three further years before the Parliamentary Commissioners who were to supervise the enforcement of this constitutional right would be confirmed in their positions. Although the process for preparation of the Act started in the mid 1980s, he was only promulgated in 1992, then Parliamentary Commission to commence his duties.

Key words: data protection, law right to disclosure of information, codification of work, ratifying, Convention, directive, integration criteria ombudsman, data controller.

Отримано 1.03.2010