CONCEPT FOR HUNGARY'S ACT ON ELECTRONIC FREEDOM OF INFORMATION

Prepared by the
EÖTVÖS KÁROLY
PUBLIC POLICY INSTITUTE

on commission of the
Ministry of Informatics and Telecommunication

June 2004

INTRODUCTION

Commissioned by the Hungarian Ministry of Informatics and Telecommunication in the fall of 2003, the Eötvös Károly Institute prepared a study exploring the options of implementing electronic freedom of information in Hungary. Beside analyzing international models and experiences, the study examined the existing practices of electronic freedom of information in Hungarian legislation and legal practice, taking a look at provisions mandating electronic disclosure and the posting of public information on national and local government sites. The main objective of the study was to survey Hungarian and international practices and report on the status of informational rights, in order to conclusively demonstrate the need for regulating electronic freedom of information on the legislative level, as necessitated by changing social and economic conditions as well as civil rights and obligations. In June 2004, the Ministry hired the Institute to prepare the concept for a bill on electronic freedom of information, using the findings of preliminary studies conducted by the Institute. The Ministry would then use the concept to draft the bill to be submitted to Parliament for debate and adoption. The Eötvös Károly Institute duly prepared the concept as ordered, in collaboration of the following experts:

László Majtényi, head of the research team
Zsolt Bártfai
András Jóri
Zoltán Miklósi
Gábor Polyák
Éva Simon
Máté Szabó
Iván Székely
Ilona Varga.

We are also indebted to Zsuzsa Kerekes and Judit Szoboszlai, who contributed to the preliminary studies.

I. A BRIEF OVERVIEW OF THE REGULATORY CONCEPT FOR THE ACT ON ELECTRONIC FREEDOM OF INFORMATION

1. THE NEED TO REGULATE ELECTRONIC FREEDOM OF INFORMATION AND ITS GUIDING PRINCIPLES

2. PROVISIONS INVOLVING FREEDOM OF INFORMATION ON THE DISCLOSURE PRINCIPLE

3. ELECTRONIC APPLICATIONS FOR DATA OF PUBLIC INTEREST

I. A BRIEF OVERVIEW OF THE REGULATORY CONCEPT FOR THE ACT ON ELECTRONIC FREEDOM OF INFORMATION

1. THE NEED TO REGULATE ELECTRONIC FREEDOM OF INFORMATION AND ITS GUIDING PRINCIPLES

1.1 The necessity of regulation

When the National Assembly adopted Act LXIII of 1992 on the Protection of Personal Data and the Disclosure of Data of Public Interest (hereinafter: "DF&FOIA", short for Data Protection and Freedom of Information Act) Hungary was deservedly seen in a pioneering role. In fact, the country had preceded many long-established democracies in 1989 as it became one of the first nations in the region to enshrine freedom of information as a constitutional right. This revolutionary step was followed by the creation of the DF&FOIA, which spelled out the rules of implementing and enforcing that right. Since then, a new phenomenon, the so-called electronic freedom of information has quickly gained ground as a cardinal issue for international legal practice. After its initial landmark law, however, Hungary has fallen behind global standards in legislating for freedom of information and developing its computer infrastructure.

Electronic freedom of information does not only supply an access route to public information, but may well be the ultimate tool in actually implementing freedom of information itself as a vital step in the democratic process. On the other hand, some inequity of access seems inevitable, although it is certainly possible to minimize it. This may result in a deficit of democracy.

The institutions of democracy are endangered as they are by the increasingly intricate and, especially for outsiders, obscure operation of public administration. This tendency gives rise to social spaces that lack any measure of transparency for the unitiated. Now, those who cannot keep track of public information in the labyrinth of files will eventually despair and lose all opportunity and courage to participate in public affairs. Consequently, all informational liberties are based on the central ideal of the inscrutable citizens and transparent government. This twofold claim follows directly from Hungary's 1989 Constitution, which enshrined privacy and freedom of information. The call for the division of informational power provides a solid theoretical and institutional background for guaranteeing informational rights. Clearly, separation of powers is an ideal that must be applied to informational as well as other forms of power. Under this principle, taken in its most readily understood form, any and all newly emerging form of power must be immediately checked by creating appropriate counterbalances.

No doubt, the revolution in information technology will have an impact on the way the political system works, and will sooner or later come to affect the system itself and its constituent parts. The first step on this road is e-government, which is taking shape in Hungary and elsewhere as we speak. The most important benefit of e-government is better dissemination of and access to information–in other words, ease of communication. It may seem that this in itself does not raise informational rights to a truly new qualitative level, although it certainly brings fundamental changes and must not be underestimated. For instance, the electronic submission of applications may generate excess clerical work, but it spontaneously makes for a type of interactivity that would be inconceivable with conventional, paper-based correspondence. These obvious advantages notwithstanding,

electronic administration and the electronic freedom of information that it may easily–albeit not necessarily–entail must be seen as precursors rather than substantive components of an e-democracy that may or may not come to pass. If it does, it will mean a radical step allowing the en-masse adoption of citizens into the fold of democratic discourse and civic life.

The Constitution recognizes freedom of information as a human rather than a civil right. Under § 61 of the Constitution, everyone in the Republic of Hungary has the right to access and disseminate data of public interest, and the law concerning the disclosure of public information requires two-thirds majority in the Parliament to pass. This law provides in detail for the procedure of handling petitions for data of public interest, the most popular method of accessing public information. Essentially, a petition is submitted by the client to the organization in control of the data being sought. The organization is liable to satisfy such requests in an easily understood form as promptly as possible, but not later than in 15 days of receiving the petititon. The petititoner is entitled to a copy of the document or its part, subject to a fee but irrespective of the technical means of storage and retrieval. The head of the agency may charge a fee, but only up to the actual cost of the disclosure. It is accepted practice, however, not to charge a fee unless the petition has unusually high cost implications.

Upon request, the agency must inform the petitioner about the cost of disclosure in advance. Petitioners must be notified of rejected petitions in writing in eight days, explaining the grounds of rejection. Organizations in charge of data of public interest must report rejected petitions and the basis of rejections to the Data Protection Commissioner annually. The client has the right to go to court over a rejected petition for disclosure within 30 days of being notified. The burden of justifying the rejection rests with the agency. If the agency is a national one, the lawsuit will be heard by the county or capital city court. In other cases, the venue is a local court or, in Budapest, the Pest Central District Court. The court jurisdiction depends on the seat of the agency. Cases involving rejected petitions for disclosure are heard with special dispatch.

Electronic freedom of information makes sense not just for the mandatory posting of information but also in the context of disclosure on request. Electronic freedom of information must be regulated in such a way as to enable electronic petition for disclosure. When a considerable portion of the communication between citizens takes place electronically, it stands to reason to expect the government to allow the use of electronic channels for communicating with its organs and agencies. As an added benefit, electronic disclosure expedites the work of the front office.

In Hungary, freedom of information already enjoys a measure of enforcement in the electronic domain, despite a lack of dedicated regulation, Essentially, the agencies we have looked at make an honest effort to post as much public information as possible on their sites–not only driven by a desire for a high-tech image but also because they have recognized the efficiency of this new form of disclosure. At the same time, one cannot pass in silence over the fact that data controllers tend to be rather whimsical in deciding which of their data to post electronically. They are no less arbitrary in their habits of answering electronic petitions. Some agencies refuse to deal with e-mails altogether, even if they consist of simple inquiries by curious citizens. Others answer e-mails just as scrupulously as they would any letter received by conventional mail.

It is the assumption of this Concept that the law must be enacted for the purposes of enforcing the fundamental right to the access and dissemination of public information, as guaranteed

under § 61 of the Constitution. We therefore propose that electronic freedom of information should be regulated by amending the DF&FOIA, whereby the relevant passages of this existing law would be modified and supplemented, without changing the fact that the protection of personal data and the disclosure of public information are provided for by one and the same piece of legislation.

In addition to measures designed to enforce freedom of information, the regulatory concept addresses some of the provisions of the DF&FOIA that are not confined to issues of electronic freedom of information, in order to deal with loopholes, gaps and ambiguities identified in the course of a decade of experience with using this normative text.

The regulation must also take into account Directive 2003/98/EC of the European Parliament and of the Council on the re-use of public sector information (the "Directive"). The provisions of the Directive are closely related to the issue of freedom of information. However, their purpose is not so much to ensure access per se as to level the playing field for business organizations and other entities within the Union in exercising their options guaranteed under national laws for the specific re-use of information. In the standardized internal market of the Union, the main goal is "to facilitate the creation of Community-wide information products and services based on public sector documents, to enhance an effective cross-border use of public sector documents by private companies for added-value information products and services and to limit distortions of competition…" (Preamble, Section 25).

1.2 Regulatory principles

The Concept of the bill is based on the following principles, some of which should be incorporated in the language of the law to facilitate interpretation.

1.2.1 The principle of disclosure

As a point of departure, the Concept uses the basic tenet of the philosophy of freedom of information, which regards information handled by public agencies and officials as accessible for anyone by default, that is, allowing for certain exceptions as may be specified by law. However, universal access means more than just rendering information accessible to the applicant upon request. Just as importantly, it implies unsolicited general disclosure of information of broader social interest and consequence. The institution of disclosure moves public data controllers to positive action, motivating them to voluntarily making available as much information as possible. In essence, the principle of disclosure specifies the notion, often articulated in international documents and professional legal literature, that public agencies are liable to take a proactive role.

1.2.2 The protection of freedom of information in its conventional forms

Enshrining electronic freedom of information by legislative means serves the broadest possible enforcement of civil rights, rather than their restriction. Therefore, mandating electronic access should not be allowed to prevent the exercise of access to public information in conventional ways. It is therefore vital to ensure the functional equivalence of the two channels of communication, including the citizen's discretion to choose the format or data

carrier, as well as the medium for receiving the information sought. In this latter respect, the Concept allows for a certain measure of imbalance. We recommend that agencies be obliged to supply data stored exclusively in the digital domain in printed form upon request (except of course special databases that are unfit for such conversion by their very nature), but not the other way round. In other words, it should not be made mandatory for agencies to digitalize paper-based information.

This same principle is served by another proposed measure, which would prevent agencies from construing their compliance with the mandatory posting requirement as an excuse for refusing individual requests for disclosure. To put it in different words, the maintenance of a homepage should not be seen as a disjunctive alternative of answering individual calls for public information.

1.2.3 The principle of technology independence

The electronic freedom of information implies the right to access data of public interest by electronic means. The law must not stipulate any one technology or network platform for that access.

It is equally obvious that making disclosure mandatory on every conceivable electronic platform, including e-mail, the web, SMS, WAP, and in the future even digital television, would impose an excessive burden that no agency of public administration could possibly shoulder. In reality, it is possible to ensure electronic disclosure by providing a single channel of electronic communication. At the same time, it is preferable during implementation to accommodate the expectations and actual capabilities of data seekers by concentrating development efforts on solutions easily accessible to most people without making a major investment in technology. This criterion also goes a long way toward guaranteeing the judicious use of public funds. Whenever some new technology becomes available at a lower cost for a broader group of users, it must be enabled as a means of accessing public information.

Crucially, the principle of technology independence implies that electronic disclosure must always use the most common format that is user friendly and intuitive for the most citizens. As an exception to the rule of technology independence, the authors of this Concept recommend that applicable agencies be required on a mandatory basis to post all information specified on disclosure lists on their web site. This requirement is justified by the need to facilitate universal access, and to improve the efficiency and standardization of disclosure.

1.2.4 The principle of equal opportunity and government subsidy of access

To uphold the freedom of information, it is not enough for the government to refrain from infringing on people’s rights. The government must actively provide for the conditions under which it becomes possible to exercise that fundamental right.
The Concept identifies a number of ways of ensuring equal opportunity in this field: by declaring that public information posted on the web is available free of charge; by mandating the government to ensure access to electronically disclosed public information free of charge for disadvantaged groups and to maintain an assistance service; by requiring handicapped access to web sites; and by requiring the option of accessing information in foreign languages.

As a token of equal access, public agencies should be required to post their basic information in the languages of Hungary's ethnic minorities.

1.2.5 The protection of personal data while implementing freedom of information

The fundamental right to have access to data of public interest accrues to everyone under the Constitution of the Republic of Hungary. Petitioners, therefore, need not justify their petitions to have access to information. Formulating the beneficiaries of the freedom of information in this way implies the right of anonymous access, that is, that the citizens must be guaranteed anonymity in the process of accesing information concerning the activities of public authorities and officials. Although the amendments required on this count are justified in part by the emergence of electronic tools such as the management of log files and the use of cookies, the special requisites appearing in the electronic context can be readily converted into rules of general application. We believe that the protection of privacy is imperative throughout the process, whether disclosure takes place by mandatory posting or upon request.

2. PROVISIONS INVOLVING FREEDOM OF INFORMATION ON THE DISCLOSURE PRINCIPLE

2.1 Providing for the method of disclosure

One purpose of legislating for electronic freedom of information is to make electronic disclosure mandatory in addition to conventional modes of disclosure. Regarding the law's approach to electronic disclosure, four solutions are theoretically conceivable:

a) The law requires disclosure in a form that is universally accessible to everyone, without specifying the actual mode of disclosure.
b) The law requires disclosure and mentions the electronic medium as a possible solution.
c) The law makes it mandatory to disclose public information in a number of ways, including the electronic.
d) The law requires data to be disclosed electronically.

The authors of this Concept recommend concurrent disclosure, the solution under clause c) above. Enacting a provision along these lines would not prejudice the obligation of agencies under § 19 (2) of the prevailing DP&FOIA. Instead, it would simply supplement that passage by making electronic disclosure mandatory. We prefer this solution on the grounds of protecting conventional freedom of information. If the electronic were the only mandated manner of disclosure, the line that separates those who use the Internet from those who do not would become a line of demarcation between citizens with and without access to data of public interest.
As part of providing for the method of disclosure, the following passages, or language similar in meaning and substance, could be incorporated in the DP&FOIA:

National agencies, local governments, and offices of public administration on the county/capital city level shall maintain a web site and post all such information free of charge and universally accessible as defined in the disclosure lists under § 19/B.

Agencies not subject to the web site requirement shall have the option to transfer the data defined in the Appendix to the Act to their supervising agencies for disclosure. The supervising agencies shall take the necessary measures to disclose the information thus received.

The agency generating the data (the appointed information officer) is liable for the accuracy and currency of the posted information, while the continuous accessibility of the data is the responsibility of the organization in charge of actually posting the information. The disclosure of data specified on the disclosure lists does not prejudice the obligation of public agencies under § 20.

The rules of disclosure for the courts shall be provided by the law on disclosure in justice.

2.1.1 Mandatory homepage maintenance

The law on electronic freedom of information must require certain organizations to maintain their own web sites on the Internet. On this one count, the principle of technology independence must take second place, since the law will specifically point to the Internet as

the medium of choice. In the absence of this restriction–that is, if the law simply required posting in some electronic medium or another–the various agencies could adopt their own preferred solution (for instance, data could be recorded in electronic carriers that would then be sent to public libraries). This could easily prevent the broadest possible access to the information in question.

The mandate to maintain a homepage does not necessarily imply an autonomous, independent site. Agencies subject to the provision could team up to cooperate on maintaining a shared site, provided that the data of public interest remain discrete or separable with respect to each agency. In other words, it should remain clear at all times which data belong to which agency, and the person looking for information should be conveniently directed to the appropriate domain. This could be an especially attractive solution for small communities where the maintenance of an independent site is often beyond the means of the local government.

2.1.2 Who should be subjected to the disclosure obligation?

Pursuant to the current version of the DP&FOIA, every agency of the national and local governments, as well as every organization exercising a public function as defined by law, is liable to periodically post a certain range of data of public interest, without being requested to do so. With respect to this general obligation, the interests of access and transparency in government warrant the specification of the subjects of this obligation as broadly as possible. By contrast, it makes sense to draw a smaller circle for those required to post public information electronically. In other words, we believe that the obligation should not be applied indiscriminately to all persons and agencies fulfilling public functions.

An exception should be made for the courts due to their special function and legal status. In respect of the courts, the law must assign the authority to set down the rules of disclosure and homepage maintenance to a separate Act providing for disclosure in judicial affairs.

As a rule of thumb, agencies of the government with nationwide jurisdiction should be required to maintain their own web site. Exemptions from this obligation–for instance for local governments and offices of public administration–can be defined according to additional criteria. Beside ensuring electronic access to public information, this concept enables solutions matched to the diversity of various sectors, including the option for local agencies to post their information on the site of the central organization to which they report or, if justified by the distinctive features of the sector in question, on their own site. Considering that every agency in charge of public information is solely responsible for the truthfulness, accuracy, and up-to-date status of the data generated by them or arising through their activities, we are of the opinion that agencies not liable to maintain a web site should be subjected to the obligation to report the relevant data to their supervisory agencies which will then post the information on their behalf.

Extending the web site requirement to agencies with smaller than nationwide jurisdiction seems reasonable given the special nature of their connection with citizens and the position they occupy in the government apparatus. We think the county/capital offices of public administration should be subjected to the requirement not simply because of the diversity and extension of their powers, but because they come into contact with a large number of citizens on a daily basis. We are therefore in favor of the idea that all local governments should be required to maintain their own site on the Internet.

By way of counterargument, one could point to the excessive burden this requirement would impose on local governments. Conceding to this point of view, we suggest to leave open the option for local governments to cooperate on maintaining a shared site, but not to make an all-out exemption from the web site obligation.
As a matter of course, defining the web site requirement in this way does not in the least prevent any agency, organization or institution from running its own site without being required by law to do so. The more comprehensive disclosure obligation pursuant to § 19 (2) of the DP&FOIA can be satisfied electronically by any entity.

2.1.3 Updates

The liability to keep information up to date should be made part of the disclosure and web site obligations. This requirement seems particularly warranted in the medium of the Internet. Looking at the sites maintained by national and local government agencies, we often encounter obsolete content, when the point of electronic posting is precisely to facilitate updates and actualizations on an ongoing basis. Consequently, we recommend that the law should make it mandatory to keep posted information up to date. This would be the liability of the organization that generated the information in the course of their proper activities. Conceivably, the law could even stipulate a tight deadline for posting after the information has been generated or altered, in order to ensure the currency of government data on the web.

2.1.4 Site availability

Mere posting on the Internet does not necessarily amount to the information actually being transmitted to the public. Non-indexed content cannot be accessed by Internet browsers and search engines, and a reluctant agency can easily hide contents behind a misleading domain name or even allow another entity to use it. This creates an unwelcome opportunity for agencies to effectively withhold information while formally complying with the posting requirement. To prevent such loopholes, some countries have adopted electronic freedom of information legislation requiring site operators to notify the public about the option and method of accessing their information electronically. Our Concept seeks to achieve this by means of a meta-database of public information, and by proposing to make agencies liable for keeping their sites available. The precise content of this requirement, including availability in line with prevailing norms of Internet use and a standardized domain policy, will be shaped in the process of implementing the new law, in the context of a ministerial decree authorized by it.

2.1.5 Eliminating technical obstacles

It follows from the special nature of the type of disclosure in question that access to posted information may be temporarily impeded by technical problems. The elimination of such problems must be provided for as part of regular site maintenance. We recommend that the site operator/poster be made liable for regular maintenance to ensure the constant availability of the site.

2.1.6 Equal opportunity on web sites

It is vital to consider enacting provisions imposing further requirements on agencies subject to the web site obligation, in order to ensure equal access to data of public interest by minorities and disadvantaged groups. We have addressed this issue with a focus on the handicapped as well as national and ethnic minorities.

2.1.6.1 Handicapped access to sites

It is important to realize that the Internet may contribute to reducing inequalities in society, but the Internet will not redeem its promise of the "emancipation of information" unless it remains an available tool for the handicapped and the needy.

In drafting the concept for a law on the electronic freedom of information, we have taken into account the provisions of Act XXVI of 1998 on the Rights and Equality of the Disabled, which identify communication as a major target area for improving equal opportunity. Pursuant to § 6 (1) of this Act, persons with disability, and their relatives and helpers must be ensured access to pubic information. Recognizing the significance of unimpeded access to information, the Act makes it a point to define the criteria for information to be regarded accessible. Under § 6 (2), information cannot be deemed accessible for the person with disability unless he or she can perceive the information and is ensured the opportunity of proper interpretation. The same law also requires that people with a major communication impediment be ensured the right conditions for bilateral exchange while using public services. In other words, the disabled are entitled to informational equality in their interactions with public authority [§ 7 (1)-(2)]. The point to be made here is that ensuring an obstacle-free interface on sites containing public information goes a long way toward equal opportunity.

The law on electronic freedom of information could supplement the DP&FOIA by a provision requiring the government to support obstacle-free access to data of public interest, but we do not see the need for any further amendment of the DP&FOIA in this field, if only because electronic freedom of information seems sufficiently guaranteed by the provisions cited above. In fact, if the law went so far as to stipulate technical parameters for obstacle-free sites, this would be antithetical to the principle of technology independence.

2.1.6.2 Equal opportunity for national and ethnic minorities

We will now address the topic of ensuring equal opportunity for the national and ethnic minorities, underlining the added benefit of electronic freedom of information in facilitating minority participation in civic discourse and public affairs, and enhancing the representation of minority interests.

§ 53 of Act LXXVII of 1993 on the Rights of National and Ethnic Minorities enumerates the criteria for the use of minority languages that will guarantee equal opportunity in electronic freedom of information. This Section provides, among other things, that the local community government must accommodate the request of the local minority board to post measures and notices, and make official forms available, not only in Hungarian but also in the native tongue

of the given minority, in identical form and content. We interpret the phrase “identical form” as applying to the electronic media as well.

2.1.7 Protecting personal data while accessing posted information

The protection of privacy remains an issue of concern when citizens exercise their right to access public information electronically, since the server running the agency’s site automatically stores the visitor’s IP address, choice of browser, and type of operating system. These are known as turnover data, and governed by sectoral rules set down in § 13/A of Act CVIII of 2001 on Certain Issues Relating to Electronic Commercial Services and Services Concerning the Information Society (the E-Commerce Act).

As a general rule, no registration or other form of identification of the visitor may be required as a condition of accessing public information.

The E-Commerce Act sufficiently provides for the rules of processing data in connection with visitor access. Turnover data may not be used for any purpose other than that of statistics, and placing cookies is regarded as unacceptable practice.

The law on electronic freedom of information should prohibit the collection and processing of personal data–except for turnover data–in connection with access to public information posted on the Internet. Since turnover data are inevitably acquired by the server operator, it is necessary to specifically state that these data may not be linked to personal information.

> *In connection with publicly posted information, agencies defined under § 19 (1) may not process personal data except to the extent that is technically and strictly necessary for them to meet their disclosure obligation. These data shall not be linked to such other data as may be suitable to personally identify the visitor to the site.*

2.2 Types of data subject to disclosure

Beyond stipulating the requirement for maintaining web sites and ensuring access to the public data posted thereon, the law must define the types of data to be posted by the agencies in such a way as to ensure access to them on a continuous basis. The electronic disclosure obligation must extend to data of public interest that help the visitor to establish contact with the agency and use its public services efficiently, and which serve their transparent and democratic operation, access to information vital for forming their judgment in public affairs, the efficient and transparent use of public funds, and the scaling back of corruption. As a bonus, posting on a mandatory basis relieves agencies of the duty to physically satisfy individual requests for public information.

In compiling disclosure lists, we can rely on international models–the United Kingdom and Estonia come to mind as representing best practices–and of course on our own experiences while surveying the domestic situation. In order to steer clear of ambiguities, it will be vital for the law to expressly state that data subject to mandatory posting do not include all data of public interest, and that therefore the disclosure lists do not waive the obligation to release other data of public interest per individual request under § 20 of the DP&FOIA.

An Appendix to the Act should specify the types of data subject to mandatory disclosure (generic disclosure list). No disclosure list shall feature state secrets or office secrets.

Authorized by law or with the consent of the commissioner for information rights, the head of the agency may order the organization, its subordinated agencies, or certain divisions thereof, to post additional data (special and unique disclosure lists). If the agency operates as a body, it shall determine and amend special and unique lists as a body.

Based on the statistical analysis of requests for data of public interest not featured on the disclosure list, the head of the agency shall annually review that list and amend it with a data type for which at least 10% of all data requests to the site have been received. In all other cases, supplementing the list remains optional.

By properly applying the preceding paragraph, the minister and the board of the local government shall ensure or propose amendments to the special disclosure list.

The commissioner for informational rights may also propose special and unique disclosure lists and amendments to them, and may approve list forms of his own design or prepared by others for specific types of public agencies. Narrowing down a disclosure list is subject to the Commissioner's approval.

If requests for a certain type of information total at least 10% of all requests for disclosure received by an agency, the Commissioner may order the disclosure of certain data of public interest on a mandatory basis. The agency must be ensured the right of legal redress if it contests such instruction issued by the Commissioner, or his refusal to approve a disclosure list.

Appendix to Act LXIII of 1992

Data subject to mandatory electronic disclosure

I. ***Data pertaining to organization and personnel***

1. *The agency's full official name, seat, mailing address, telephone and fax number, e-mail and web address;*
2. *Organizational structure broken down into individual units, along with their position in the hierarchy of command and management, and the specific tasks assigned to them;*
3. *Name, rank, and contact information (telephone and fax number, e-mail address) for the agency's senior and subordinated executive officials;*
4. *If the organization functions as a body, the number and composition of the board, together with the name, rank, and contact information of the members;*
5. *The name and contact information (mailing address, telephone and fax number, e-mail and web address) of other public agencies supervised by or reporting to the agency in question;*
6. *The name, address, contact information, range of activities, and authorized representatives of business organizations in which the agency has a controlling majority interest or in the management of which it participates, along with the size of the agency's stake in that organization;*
7. *Public foundations founded by the agency (name, seat, charter, name of the executives of the managing organization);*

8. All data as per clause 1 of the entity to which the agency reports or which exercises the rights of legal supervision over the agency in question.

II. *Data pertaining to activities and operations*

1. Major laws and regulations providing for the agency's functions and powers, along with additional legal tools of state governance, internal policies (such as the policy of organization and operation or the working order), broken down as necessary by unit of organization. The number and exact title of nationwide legal norms; a link to a version stored in a central location; and the full effective text of local statutes;
2. Information about the agency's tasks and activities in the languages of national and ethnic minorities;
3. Voluntarily assumed tasks of the local government;
4. The name of the agency with powers to act in administrative and other official matters with respect to each case group/type; the name of the agency actually acting in the case if the power is assigned; the territory of jurisdiction; required documents, processing fees, and basic rules of procedure; the method, place and time of submitting the application or document instating official action; office hours when clients are received;
5. Official resolutions and associated court verdicts that must or may be disclosed under separate laws;
6. The name and substance of services provided by the agency or funded from public funds; the mode of using those services and the fees charged, with any discounts as applicable;
7. List of databases and records maintained by the agency, along with the data of records subject to being reported to the Data Protection Register under § 28 of the DP&FOIA; the types of data collected and processed by the agency as part of its core activities, as well as the mode and costs of accessing those data;
8. Data in possession of the agency pertaining to the environment, pollution levels, activities of environmental protection, and the impact of environmental factors on human health;
9. The title and topic of publications issued by the agency, with availability and price if applicable;
10. If the agency operates as a body, the mechanism of preparing for decisions, the mode of civil contribution and feedback, the date, place and publicity of the meeting if not restricted by law; the resolutions passed; session minutes and summaries; distribution and other data of votes;
11. Bills and draft regulations and associated submissions;
12. Documents submitted to the public session of the local board of representatives;
13. Concepts, plans and tenders developed by the agency, and the announcement of tender results with an explanation;
14. Instructions and recommendations for other agencies reporting to the agency in question, as well as initiatives submitted to its own supervisory agencies, with the responses to these;
15. Findings of reviews and audits of the agency;
16. Indicators for gauging the performance and capacity of the agency, and their changes over time;
17. The name and contact information of the official or unit responsible for informational rights, and the procedure of managing requests for disclosure;
18. Statistical data pertaining to the agency's activities, and their changes over time;

19. Data pertaining to the agency that are subject to statistical reporting;
20. The special disclosure list applicable to the agency.

III. ***Data pertaining to finances and businessmanagement***

1. The agency's annual budget; reports on the use of the budget, submitted periodically as required by separate laws;
2. Collective data about the number of staff and personnel benefits disbursed, as well as the remuneration and benefits paid to each senior official defined in separate laws, as well as the types and collective amount of benefits extended to other employees;
3. The name of recipients of development funds disbursed from the agency's budget, with the objective, total amount, and place of implementation of the support program (§ 15/A of the Budget Act);
4. Title and subject of contracts paid from public funds (over the amount specified by separate laws) for procurements, construction projects, services, sale or lease of assets, assignment of assets or rights of material value, and concessions, along with the names of the parties, the total value of the contract, and its term if executed for a definite period of validity;
5. Public data as defined in the Concession Act (announcement of tenders, bidders' information, tender results);
6. Expenditures for functions not belonging to the agency's core activities, including in particular support of civic organizations and of the professional associations, unions, cultural, social, and athletic activities of agency employees and beneficiaries, as well money paid for functions performed by foundations;
7. Data as defined in the Procurements Act (announcement of tenders, bidders' information, tender results, and the contract signed as a result).

2.2.1 Disclosure lists

The legal definition of the type of data subjected to mandatory electronic posting without request is best conceived in the form of disclosure lists. Standard data subject to posting can be divided into two groups. One contains data whose disclosure is mandatory for every institution (mailing and e-mail address, structure, provisions regulating operation, internal policies etc.). The other group consists of data subject to disclosure by the given agency. These in turn can be "special" data (for instance those applying to all agencies within the same sector) or "unique" data (e.g. the relevant data of the agency being currently audited by the State Audit Office). Nevertheless, the law should not be expected to match the logical structure of the data in its entirety, but the disclosure lists must provide for generic and special data types, as well as those whose disclosure is mandatory for the given agency only.

The generic disclosure list featured in the Concept has been compiled with a view to the data types illustrated by a few examples under § 19 (1)-(2) of the DP&FOIA, as well as considering the relevant provisions of other laws, particularly Act XXXVIII on the National Budget and its Implementation Decree. We suggest that the generic disclosure list be annexed to the DP&FOIA in the form of an Appendix.

In addition to the generic disclosure lists, a number of other statutes provide for the disclosure of certain types of data on the web sites of public agencies. These rules, however, tend to

apply to specific groups of government agencies. Consequently, it is not possible, nor indeed necessary, to take up these data types in the generic disclosure lists.

This latter circumstance–that is, the fact that the disclosure obligation is often stipulated for specific groups of data and agencies–inevitably influenced the development of rules governing special disclosure lists. The British model, whereby agencies of the public sector design and post their own special disclosure lists with the approval of the information commissioner, cannot be adopted into the current legal framework in Hungary as the exclusive solution. Aware of this situation, we propose that the legislation should allow special disclosure lists to be defined by laws and regulations or by the head of the agency in question. Under the current version of the DP&FOIA, the Data Protection Commissioner reviews bills and draft regulations with disclosure implications. This means that the Commissioner's opinion can be accommodated even if the content of the special disclosure lists is to be defined by laws and regulations. By the same token, the Commissioner for Informational Rights should be authorized by the law to make a proposal with administrative force for supplementing existing lists.

2.2.2 Ensuring a dynamic transition

Generic and special disclosure lists reflect the decisions made by legislators and the public agencies themselves as to what types of data should be disclosed on a mandatory basis. It is imperative to ensure that data of public interest that are not initially subject to the disclosure requirement but have been the target of large numbers of disclosure requests be eventually posted on the web on a mandatory basis, and that the disclosure lists be amended accordingly. Superficially, this stipulation may be seen as an undue burden for agencies. In reality, it means just the opposite: the relief of paperwork involved in satisfying individual requests for disclosure.

The Data Protection Commissioner (more properly called the Commissioner for Informational Rights) should be empowered by the law to instruct agencies, with binding administrative force, to post or supply data of public interest. On the other hand, the law must uphold the agency's right to seek remedy in court against the Commissioner's decision.

2.3 Access to posted data

As we have seen, genuine access depends to a great extent on the practical opportunity and actual ability of people to take advantage of it. This implies that the government must find a way to financially assist the implementation of this fundamental right.

The state promotes equal opportunity by ensuring access to electronically posted public information free of charge for disadvantaged groups, and by maintaining an assistance system.

In the estimation of this Concept, the law on electronic freedom of information should not stipulate the rules of ensuring access beyond the means already mentioned. The government should remain free to decide whether to allow the use of communal computer centers as access points free of charge for everyone (knowing that they will be used mostly by the needy anyway), or whether to reserve this privilege for certain social groups as a tool of affirmative

action. If it decides to make access to public information on the web free of charge as a rule, it may still charge a fee for using the Internet for other purposes, and for associated services such as scanning, copying, printing, or faxing documents and images.

At local access centers, a network assistant may be appointed or hired to help citizens' access public information (which, as we have seen, cannot be regarded as truly accessible unless it is perceptible and interpretable for the citizen). Taking possession of information posted in the electronic media requires special skills. Those citizens who do not speak the language of information technology and are digitally illiterate will be barred from access to data of public interest on the Net. The assistance scheme we propose could be an effective tool of removing obstacles and offsetting cultural disadvantages between various social groups.

2.4 Meta-data, meta-databases, and information radar systems

In accessing public information electronically, the citizen is faced with three challenges:

- He must find the data he is looking for;
- He must judge the located information in terms of quality, relevance, and compatibility with his search criteria;
- He must interpret the information in the broader context, orienting himself in the entire network of data of public interest.

In this connection, Article 23 of the Directive provides that *"Member States should therefore ensure that practical arrangements are in place that help re-users in their search for documents available for reuse. Assets lists, accessible preferably online, of main documents (documents that are extensively re-used or that have the potential to be extensively re-used), and portal sites that are linked to decentralised assets lists are examples of such practical arrangements."*

The three challenges described above can be met through three, partially interdependent information technology solutions. Under this Concept, the legal measures providing for these solutions should incorporate the following language or something similar in substance.

> *The Government shall create and operate a central electronic list of all web sites, databases, and records maintained by agencies of nationwide powers and containing data of public interest. The Government shall further set up a Standardized Public Information Search Engine (PISE) to ensure integrated and equal public access to electronically stored data of public interest according to standardized criteria.*
>
> *The agencies in control of public information (the "data custodians") are responsible for sending the parameters of their sites, databases, and records to the operator of the central electronic list, and to update these data on a regular basis. The agencies are also responsible for the truthfulness and periodic update of the data of public interest forwarded to the PISE. Naturally, the PISE will be open to other information that is not strictly public in the legal sense but simply beneficial for the public, especially from local government sites.*
>
> *The maintenance of databases and lists of records does not exempt any agency from the electronic posting requirement, any more than does the simple fact of reporting to the PISE.*

The lists shall be available for access around the clock and free of charge on the sites of the operating organizations.

2.4.3 Information radar system

No data is in itself significant without a context that confers meaning upon it. This context is assembled from the knowledge and experience of the data seeker or information obtained elsewhere, and in part from the way in which data of public interest are interrelated with one another on several tiers of hierarchy. A database is constituted by a combination of the data themselves and the logic of the operating mechanism. This means that the database has its own internal relations. If these relations are missing or unknown, this makes it difficult or downright impossible to interpret the data. The meta-data describing the structure of each database could be encapsulated by a network of helper units, designed to facilitate the use and interpretation of the data in question. However, the ultimate purpose of the electronic freedom of information is to bring ease of access and transparency not only to specific data and databases, but also to the relations obtaining between various data of public interest in their interconnectedness.

Harmonization with the Directive demands the user interface to exist in English in addition to the main Hungarian version. It is important to point out that a radar system can be useful for accessing more than just data of public interest in the strict legal definition of this term; it should serve just as well to locate other types of information of potential concern for society that are not formally qualified as “data of public interest” subject to disclosure by law. This distinction is realized in the Hungarian language by juxtaposing the term *közadat* (“data of common concern”) to the original legal category of *közérdekű adat* (“data of public interest”).

3. ELECTRONIC PETITIONS FOR DATA OF PUBLIC INTEREST

3.1 Enabling electronic petitions for information

The regulation of electronic freedom of information must provide for the opportunity of applying for information through the electronic media. Implementing this option in practice entails the mandatory requirement for agencies in control of public information to render their relevant data accessible in the electronic domain. In this connection, the new law must uphold the principle of technology independence, and should incorporate the following measures:

> *Petitions for data of public interest may be submitted in any form or format, including but not limited to the electronic.*
>
> *The agency in possession of the public information sought shall provide the option of electronic petition through technical solutions that will enable the largest possible number of citizens to actually take advantage of this format.*
>
> *The agency shall facilitate electronic petition so that citizens can exercise their right of access conveniently and instantly any time, without any special skills.*

The law must enshrine guarantees for the actual availability of the electronic option for citizens. However, the law cannot possibly provide for the technical means of access in all of its minute details (for instance, it obviously cannot stipulate a certain format for the e-mail address), if only because of the diversity of potential solutions. To make up for this deficiency, the law must provide that petitions may be submitted in any format, thus preempting the need to acquire special skills and hardware. Furthermore, the law may require the maintenance of the electronic option around the clock, during and outside business hours, which obviously implies quality criteria for the service (constant availability).

Without an express provision articulating this requirement, the data controller is also expected to supply an e-mail address that is easy to remember or infer, and to post this address on its site in an easily visible fashion. Interpreting the precise content of this requirement will be the job of regulators drafting the implementation decree for the Act, and of the agencies themselves as practitioners of the law. Finally, the legislation should stipulate sanctions for breaching this requirement.

3.2 Confirmation requirement

In order that the petitioner may ascertain receipt of his petition, and that the agency may be held to the processing deadlines, it is vital for the law to require the agencies to confirm receipt of petitions. This is a crucial guarantee of electronic freedom of information, because confirmation is not simply a technical issue, due to the unreliability of electronic correspondence and the calculation of deadlines. In our opinion, the law should provide for this guarantee as follows:

> *The agency in control of data of public interest or the addressee of the petition shall confirm to the petitioner by electronic mail the receipt of the petition promptly, but no later than on the next business day, when the petition has been filed and entered in its*

system. The rights of the petitioner in connection with the petition shall begin to accrue when the confirmation notice has been sent.

According to this Concept, it is not necessary for the law to stipulate actual involvement of office personnel in sending off the confirmation, but it may leave open the option for the automatic generation of such messages. The detailed rules here should be codified in the agencies' internal policies regulating the processing of documents. We also believe it is necessary to require the proper entry and filing of received petition on the record, so that the parties may keep track of the history of communication regarding the electronic petition for data of public interest.

3.3 Response requirement

In our opinion, it is not necessary for the law to expressly and separately mandate the agency receiving a petition for data electronically to reply to the applicant, since this liability is implied in the general response requirement articulated in § 20. What is not so clear is which agency is liable to satisfy the request, and what to do when the petition has been sent to the wrong agency. These questions could be clarified by enacting the following provision:

The agency receiving a petition of which it is not the intended recipient shall notify the petitioner of this fact and offer help with delivering the petition.

It will be indispensable to address the situation when the petitioner sends the request to the wrong agency. In such cases, it stands to reason to require the actual recipient to inform the petitioner about the proper controller of the information sought, and the ways in which that information may be obtained.

In the name of implementing what we may call "single-window freedom of information," we must ensure that the petitioner obtain meaningful information even if the particular data sought is managed by an agency other than those of the central administration.

3.4 The form and format of satisfying petitions

Neither the electronic nor the conventional method of petition necessarily implies that the reply be given electronically. The petitioner must be reserved the option of receiving the reply in writing on paper or in any other format, even if the petition itself has been submitted electronically. Requests to this effect may not lead to discrimination, except in the sense that they may entail different costs. Moreover, forwarding documents by conventional means necessitates the handling of personal data (such as mailing address) that do not arise in the course of electronic correspondence. The personal data of the petitioner may never be processed in excess of what is strictly necessary to satisfy his request.

The agency in control of the data sought shall satisfy the petition for the data–if practicable, accommodating the request of the petitioner–in a format, whether printed, electronic, or otherwise, that the petitioner can readily decipher and interpret. The agency shall not refuse requests for information in the form of a certified official document.

If the information is communicated in the electronic domain, it is not necessary to regulate the format on the legislative level. The only requirement here is for the data to be interpretable by the petitionr without any undue expenditure of skill or energy (more often than not, this will mean simple text files or the html format). The regulation should enable the petitionr to specify the format of the electronic document to be received, to the extent that this does not impose an undue burden on the agency. As a means of avoiding superfluous conflict, only reasonable requests should be accommodated on a mandatory basis. For instance, electronic disclosure may be prevented if the information sought is simply unavailable in the electronic format, and it is not feasible–possibly because of the vulnerability of the document–to digitalize it by reasonable effort. In such cases, the agency should be free to satisfy petitions in a format other than the one requested.
The overwhelming majority of petitions do not require the all-out certification of the information supplied. Consequently, there is no need to stipulate certain types of electronic signature for certain types of electronic documents. The thing to keep in mind is that, in case of a dispute, without legal and technical guarantees it is not possible to determine with absolute certainty whether the information has been effectively supplied to begin with, or whether it has been meaningful in its content. The internal policies of processing and filing documents, along with measures for monitoring compliance with those policies, obviously solve some of these difficulties.

As we have mentioned, the petitioner must be ensured the option to request the disclosure in the form of a certified official document. This becomes especially significant when the use of the acquired information confers some right or obligation upon the petitioner. The data controller may not refuse such requests, but it should be free to decide whether to satisfy them in the electronic or the conventional format.

Considering the nature of the electronic domain, we do not deem it necessary to regulate the content of disclosures specifically in this medium.

3.5 Paying the costs

Although the existing rules can be adequately applied to issues of paying the costs of disclosure, in light of some practical difficulties of legal interpretation it would seem to make sense to further clarify and fine-tune the applicable provision of the law (see also clause XXX).

3.6 Liability

The liability of the agency in control of data of public interest can be clearly established with reference to the general liability provisions of the Civil Code, so there is no need to incorporate special provisions on this issue in the DP&FOIA. It is not necessary to apply regulations more stringent than the general norms of liability.

3.7 Ensuring equal opportunity

The equal opportunity principle of the Concept should be embodied in a provision declaring that

Access to data of public interest may not in itself be denied because the request has been worded and submitted by a person whose native tongue is other than Hungarian, in his native language or a language that he understands.

3.8 Protection of personal data while applying for disclosure

Priority considerations demand the enactment of the following language, or provisions of similar meaning and substance:

If the petitioner so demands or such a need may be inferred from the circumstances of the petition, the petitioner shall remain personally unidentifiable. At the very least–and unless provided otherwise by law–the personal data of the petitioner shall be anonymized directly as soon as the request for the data has been satisfied.

For purposes of recouping its costs, the agency may process the petitioner's personal data, but not in excess of the extent sufficient and necessary for identifying the petitioner.
Access to data of public interest may not be denied for the sole reason that the petitioner refuses to supply his personal data.

3.8.1 Anonymity upon receiving information

In the course of petitioning for data of public interest, the petitioner establishes contact with the agency. In the process, the petitioner's consent to the processing of his minimally required personal data must be assumed. Honoring the principle of purposefulness in processing personal data, § 5 (2) of the DP&FOIA declares that "*The personal data processed must be essential for the purpose for which it was collected, it must be suitable to achieve that purpose, and it may be processed to the extent and the duration necessary to achieve that purpose.*"

This means that the agency receiving a petition for data may not process the personal data of the applicant beyond the extent indispensable for satisfying the request. The criteria of "necessary extent" as defined in § 3 (6) of the DP&FOIA serves the economy and judicious use of information, and mandates the data controller to eschew processing personal data in the course of processing the petition itself. In the event that this is not practicable, the data controller must minimize the extent of using the petitioner's personal data. The purpose of processing "necessary" data ceases to exist as soon as the request has been satisfied. Sections 3 and 5 of the DP&FOIA make it clear that, beyond that point, the agency may not continue processing the petitioner's data. An exemption must be made for data of public interest supplied in return for a fee, where the rules of accounting and other regulations require additional processing.

3.8.2 Ensuring the anonymity of petitioner

§ 19 (1) of the DP&FOIA requires agencies to minimize their use of petitioners' data acquired in the course of processing petitions for data of public interest. Ensuring the anonymity of petition is a vital guarantee of the right to informational self-determination. The current version of the DP&FOIA neither explicitly prohibits nor provides for such anonymity. What really matters is that no petition for data of public interest may be denied on the grounds that the petitioner has failed to identify himself or herself by name.

4. AMENDING THE DP&FOIA FOR HARMONIZATION

In addition to the need to provide for the electronic freedom of information, the amendment of the DP&FOIA is timely for other reasons as well. Most importantly, the Hungarian Constitutional Court allowed the National Assembly until December 31, 2004, to legally and precisely define the notions of "document for internal use" and "preparatory document." Moreover, an amendment seems to be in order in light of Hungary's obligation to harmonize its law under Directive 2003/98/EC of the European Parliament and of the Council on the Re-Use of Public Sector Information.

In what follows, we discuss the proposed amendments in the sequence followed by the DP&FOIA.

4.1 The mandate to implement the Directive

Crucially for Hungary, Article 1 paragraph (3) of the Directive states that "*This Directive builds on and does not affect the existing access regimes in the Member States. This Directive shall not apply in cases in which citizens or companies have to prove a particular interest under the access regime to obtain access to the documents.*" In other words, the Directive generally provides measures for situations falling under the freedom of information laws of individual member states. At the same time, it recognizes a number of exceptions and allows the member states to tighten restrictions on data controllers, in two senses: by allowing member states to broaden the scope of stipulations for re-use, and by allowing them to enact more stringent regulations for the data controllers than those of the Directive itself. ("*Member States' policies can go beyond the minimum standards established in this Directive, thus allowing for more extensive re-use.*" – Preamble, paragraph 8).

4.2 The notion of public information

Not unlike the legal custom followed by privacy advocates in other European countries, the Hungarian Data Protection Commissioners have given a rather broad interpretation to the concept of personal data. However, certain views in opposition to this interpretation make it quite fortunate that a new provision of the DP&FOIA, effective as of January 1, 2004, has altered the concept of "data processing" to the effect of vindicating its interpretation as it has been crystallized in the Commissioner's application and legal practice.

The picture is less clear-cut when it comes to the notion of "data of public interest" (superseded by the term "public information" in the English translation of the latest version of the Act). § 2, clause 4 defines "public information" as "*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 the public duties specified by law (including those data pertaining to the activities of the given authority, agency or body).*"

From the examples cited in the foregoing, it can be concluded that the Commissioner has construed the concept of "data" rather extensively–and in tandem with his broad interpretation of "personal data"–applying it to images as well as video and audio recordings, also in the context of public information.

When it comes to electronic freedom of information, however, the question of what could conceivably constitute "data" or "information," and to what degree, arises with more urgency than ever before. The fact that digitalization can be applied to individual numerical data, databases, image and audio files, videos, software etc., makes it doubtful whether it is really necessary to fine-tune and further specify the concept as it is used in the DP&FOIA, or whether we should continue to rely on the interpretation evolved through legal practice.

At this point, let us pause and examine the definition of "document" under Article 2, paragraph 3 of the Directive:

> *"(a) any content whatever its medium (written on paper or stored in electronic form or as a sound, visual or audiovisual recording);*
> *(b) any part of such content."*

According to paragraph 11 of the Preamble, "*a generic definition of the term 'document' […] covers any representation of acts, facts or information — and any compilation of such acts, facts or information — whatever its medium (written on paper, or stored in electronic form or as a sound, visual or audiovisual recording).*" Furthermore, "*The definition of 'document' is not intended to cover computer programmes*" (paragraph 9).

It is important to note that it is not in the least mandatory to adopt the Directive's definition to the Hungarian legal context. (As we have pointed out, the Directive admittedly builds on the member states' sovereign regulation of freedom of information, merely stipulating requirements for the *manner* in which public information can be re-used.) This lack of constraint notwithstanding, we should do well to consider introducing in the language of the DP&FOIA a definition that could be applied unequivocally and uniformly to the many types of data mentioned, irrespective of any interpretation by practitioners of the law.

There are a number of ways to attempt such a definition. First of all, a rigorous distinction must be made between data and carrier in order to differentiate content from form or medium. One starting point would be to set down the definition of "data," applicable to both public and personal information, for instance as "any information or content, regardless of its form of appearance, carrier, or medium, including photographs, audio and video recordings." This path has been followed by several European countries, including Luxembourg and Portugal. If such a definition is embraced, it will be necessary to modify the DP&FOIA's notion of "data processing," along with striking the phrase "It also includes" from the relevant section of the text. This solution would appear to be the most consistent from a dogmatic point of view.

For practical reasons–and to focus on the central subject of this Concept–it is even more pressing to adequately define the notion of "public information." We propose the following definition:

> *"Public information" means any data or set of data not falling under the definition of "personal data" that are managed by or pertaining to the activities of a body, agency or person fulfilling state or local government functions or other public duties as may be defined by law, including provisions of law or regulation, information about operations, and the official positions of the body or person in question, irrespective of the method of storage and transfer.*

The above minimal correction of language would make it unambiguously clear that freedom of information is relevant and applicable to a very broad range of data, while the phrase "set of data" would make room for data organized into databases and multimedia applications. Finally, the amendment of the notion of "public information" seems justified in light of the very clear interpretation given to "personal data," both in Hungarian legal practice and in Directive 95/46/EC.

4.4 Enabling "re-use"

Pursuant to Article 3 of the Directive, "Member States shall ensure that, where the re-use of documents held by public sector bodies is allowed, these documents shall be re-usable for commercial or non-commercial purposes in accordance with the conditions set out in Chapters III and IV. Where possible, documents shall be made available through electronic means." This general principle essentially asserts that it is allowed to re-use data obtained through the disclosure of public information, even for commercial purposes, subject to certain conditions stipulated elsewhere in the Directive (which obviously include the respect of privacy and intellectual property).

It is therefore necessary to expressly spell out the option of re-use in the Act, as follows:

> *Agencies are liable to keep on file all public information they may possess for purposes of access and re-use, subject to the rules of archiving and discarding documents.*
>
> *Public information can be disseminated freely, unless provided otherwise by law.*[1]

Interestingly, this provision essentially reiterates a right enshrined in § 61 of the Constitution. Causing a serious difficulty of legal application, the current version of the DP&FOIA does not expressly provide for the right to disseminate data of public interest subject to disclosure. The reiteration of this principle in the Act is in harmony with the Directive, not to mention that its enactment constitutes a vital guarantee for citizens.

Chapter II of the Directive deals with requests for re-using data. These requests can be regulated for concurrently with applications for simply accessing information. One solution here would be to allow the applicant to indicate his intent to re-use the information–possibly his desire to enter into contract for its re-use–when applying for the disclosure of public information under § 20 of the DP&FOIA. The alternative is to regulate the two types of application separately.

In our opinion, the former solution would be easier to incorporate in the structure of the existing Act. In fact, once access is secured, it should not be necessary to identify re-use as the motivation behind the request.

The Directive requires public agencies to make documents available for re-use "*within the reasonable time that is consistent with the timeframes laid down for the processing of*

[1] The phrase "Unless provided otherwise by law" must be inserted because in Hungarian law state secrets and office secrets theoretically fall under the definition of data of public interest (the term now superseded by "public information").

requests for access to documents." Barring provisions otherwise, the Directive stipulates a processing deadline of 20 working days for making documents available for re-use and for making a license offer to the applicant. "*This timeframe may be extended by another 20 working days for extensive or complex requests. In such cases the applicant shall be notified within three weeks after the initial request that more time is needed to process it.*" (Article 4, paragraph 2).

Hungary is under no obligation to adopt the deadlines set by the Directive. At present, the DP&FOIA allows public agencies 15 days to satisfy requests, and eight days for denying applications with an explanation [§ 20 (1)-(2)]. Obviously, these stipulations more than meet those of the Directive.

Article 4, paragraph (1) of the Directive establishes the requirement for agencies to use "electronic means where possible and appropriate." We recommend the adoption of this provision as an option rather than a requirement–possibly as part of regulating petitions, but preferably articulated as a general principle, followed by a detailed elaboration of the entitlements.

4.5 The issue of "disproportionate effort"

§ 5 of the Directive permits public sector bodies to deny applications for data in certain cases, for instance when satisfying the request would "involve disproportionate effort." The phrase "disproportionate effort" raises the question of non-existent information, which has caused an interpretive impasse for many years. The point is that if the non-existent public information existed and its production imposed no undue stress of effort or resources, then the request for it should not be denied.

> *The agency shall enable general access to public information held by it, unless satisfying the request for disclosure would imply disproportionate effort (for instance, due to the difficulty of producing the document sought).*

4.6 Documents for internal use and preparatory documents

4.6.1 A legislative exigency

In its Resolution No 12/2004 (IV. 7.), which concluded an *ex officio* procedure, the Constitutional Court determined a negligent violation of the constitution on the part of "the legislature that failed to enact sufficient guarantees that may be rightly expected in a constitutional democracy for accessing public information regulated under § 19 (5) of Act LXIII of 1992 on the Protection of Personal Data and the Disclosure of Data of Public Interest."

The Constitutional Court called on the National Assembly to remedy this legislative shortcoming by December 31, 2004.

Pursuant to the effective version of the DP&FOIA, "*Unless otherwise prescribed by law, any data that is for internal use or that is related to a decision-making process shall not be available to the public for twenty years from the date on which they are processed. Upon*

request, the head of the respective agency may authorize access to such data within that timeframe" [§ 19 (5)].

This text was incorporated through the latest, recent amendment of the Act, which did not bring any meaningful change beyond merely reducing the "buffer time." The Constitutional Court declared the provision unconstitutional.

The disputed notions could be legitimately incorporated in the DP&FOIA if given the following definitions:

> *"Information for internal use" means any information pertaining to the operations of a public agency or person and recorded by it or him in any manner that contains no decision relevant to the official duties and powers of the agency or person, provided that the disclosure of the information or its availability to an unauthorized entity would interfere with the exercise of those duties and powers without undue influence, and further provided that the agency/person has made the necessary steps to keep the information confidential.*
>
> *"Information related to decision-making" (or preparatory documents) means any information recorded in any medium and in any manner in preparation for a decision to be made by the agency within the scope of its duties and powers, which serves to provide the proper grounds for the decision and whose disclosure or availability to an unauthorized entity would interfere with the exercise of those duties and powers without undue influence, and further provided that the agency has made the necessary steps to keep the information confidential.*

The following text should be inserted among the provisions assigning limits to freedom of information:

> *Unless provided otherwise by law, information for internal use and information related to decision-making shall not be made public for ten years of its creation. However, if justified by an overriding public interest in open debate–including the case when this is required in the interest of transparency of operation and the assessment of its decisions–information for internal use and information related to decision-making shall be subject to disclosure to the public.*

Agencies whose core function is to pave the way for official decisions form a different category altogether, warranting the insertion of the following passage:

> *If the function of the public agency as defined by law or regulation is to perform monitoring or groundwork for decisions to be made by a senior agency to which it reports, the information related to decision-making that is generated by the agency may be handled confidentially even if it has been or will be forwarded to the agency with discretionary power.*

4.7 The price of public information: costs and fees charged for disclosure

The law to be drafted must make it clear that public information in and of itself is available free of charge, irrespective of the carrier or the means of its storage and processing. However,

in individual cases a fee may be charged for the disclosure, but only to the extent of the costs actually incurred in direct connection with making the information available to the petitoner.

In certain cases, the possibility of charging fee for disclosure may be ruled out altogether.

On the other hand, for the disclosure of certain types of data qualified as public information– such as sets of data or databases–it is acceptable to charge market prices with a margin over the actual cost of the disclosure, provided that this category of information is clearly differentiated from data barred from such commercial use as follows:

> *In return for making available public information in its possession, the agency may charge a fee up to the actual cost of the disclosure.*
>
> *For other public information embodying added value, including data that are processed, edited, annotated, supplemented with services to facilitate use, or subject to authorship rights as a publication, the agency may charge a fee in excess of the actual cost of disclosure.*
>
> *The agency shall notify the applicant of such costs and charges in advance.*

The above provisions can be actually derived from Article 8 of the Directive, drafted with a view to the crown copyright concept, which permits licensing public information on contract.

The method of pricing public information itself constitutes public information, and as such is subject to mandatory disclosure.

4.8 The Commissioner for Informational Rights

4.8.1 Title

Despite being named “Commissioner for Data Protection” in Hungary, this public official is equally responsible for safeguarding freedom of information. In countries where the law– sometimes in emulation of the Hungarian regulation–entrusts both informational rights to one and the same custodian, the name of the post has usually been changed to reflect its dual role. It stands to reason to effect the same change in Hungarian:

We recommend substituting the phrase “Commissioner for Informational Rights” for each occurrence of “Commissioner for Data Protection” in the language of the law.

4.9 Legal disputes over freedom of information

4.9.1 The enforcement of disclosure

The rules of enforcement form a vital part of any freedom of information legislation. A revision of these rules in the Act will be inevitable. Below are two versions of the proposed amendment to § 26 (4), of which we favor the second.

If the Commissioner for Informational Rights determines that the classification of certain information–except those classified under an international agreement–has been unjustified, he shall instruct the classifier to alter or abolish the classification. If the Commissioner for Informational Rights believes that a decision brought by the controller of public information violates the principles of disclosure, he shall likewise instruct the data controller to alter the decision in question. The classifier and/or data controller may contest such instruction within 30 days at the Capital Municipal Court of Budapest, which shall hear the case in camera.

4.9.2 Initiating disciplinary action

This Concept recommends that a further sanction beyond the one under § 21 be enacted for disclosure violations as follows:

> *If a court of law or the Commissioner for Informational Rights has determined that public information has been covered up or withheld from disclosure in violation of the law, the petitioner may request the supervisor of the agency to bring disciplinary action. The supervisor shall notify the petitioner of having instated or declined to instate the action, explaining the reasons for and results of the procedure.*

4.9.3 Fines

It is hardly conceivable to confer administrative powers on the Commissioner for Informational Rights without at the same time vesting him with the power to impose fines for disclosure violations. Such fines could be imposed on the authority of the following provision, to be inserted in the law:

> *Fines for violating an informational obligation*
>
> *Violations of a provision of law, a final court verdict or judgment, or a resolution of the authority concerning the disclosure of public information, are subject to a fine, in proportion to the gravity of the violation, its repetition, and the magnitude of the injury caused.*
>
> *The fine is regarded as a public liability subject to collection as taxes, and payable by bank transfer to the National Civic Fund.*
>
> *Payment of the fine does not waive or prejudice the offender's liability under criminal, penal, and misdemeanor provisions or his liability for damages, nor may it be construed as an exemption from performing the obligation determined by the Commissioner for Informational Rights.*

The rules of imposing and collecting fines must be laid down as part of the procedural rules of the DP&FOIA.

4.9.4 Avoidance of judgment without knowledge of the facts

One of the most remarkable cases reviewed by the Commissioner during the history of the office was initiated by a presiding judge of the Capital Municipal Court, who turned to the Commissioner for help. The Commissioner could not help but to withhold assistance because the laws did not provide (and have not provided since) a solution for the legal dilemma involved in the case (No. 800/K/1997). According to the judge, the plaintiff had applied to the defendant, the Office of Information (an intelligence agency), to allow him to inspect files kept on his person, to discontinue the illegitimate processing of his data, and to delete the data from the agency's records. The Office of Information refused to satisfy these requests, citing the protection of the external and internal security of the Hungarian state. The petitioner was simply given to understand that the Office had "not engaged in any illegitimate processing" of his personal data. Citing § 44 (2) and (3) of Act CXXV of 1995 on National Security, the Office even declined to supply meaningful information to the court.

Under these circumstances, a judge is expected to reach a judgment without being able to inspect documents of the National Security Service classified as state or office secrets or, in a civil lawsuit, the documents withheld from the petitioner as "documents for internal use." As a result, the judge is barred from knowing some or all of the facts at issue. In the particular case at hand, the judge only had the defendant's testimony on the facts of the case to rely on in ruling that no violation had been committed.

Related to this dilemma–albeit short of providing a solution–is the notorious telephone tapping case of Klass vs. Germany, in which the European Court of Human Rights ruled that covert surveillance by the police was inadmissible except on exceedingly stringent conditions. According to the Court, the secret surveillance of citizens is typically used as a tool by police states. Recourse to such measures is prohibited under the Convention, except when positively justified by the interests of protecting democratic institutions, and then not beyond the extent that is strictly necessary to accomplish that protection. At the same time, the Court recognized the threat of espionage and terrorism, ruling that the state was entitled to place "subversive elements" engaging in such activities under surveillance, but also that keeping such surveillance in check by judicial and other means was both desirable and necessary. In the case at hand, German law ruled out a court review, although it allowed the establishment of two bodies to perform the investigation. The Bundestag created a five-member committee and a three-member subcommittee, with proportional representation of parliamentary factions, to monitor compliance with the law. Ultimately, the Court ruled that no violation of Article 8 of the Convention was committed, and also threw out the claim that the German state breached Article 13 of the Convention on the right to effective remedy, on the grounds that legal redress cannot be effective beyond the narrow confines allowed by the system of checks and balances.

In short, there are cases when not only the plaintiff but the court itself is prevented from accessing internal documents or documents related to the decision-making process. In Hungary, a possible solution to this quandary would lead through the amendment of the Rules of Civil Procedure (RCP), to the effect of enabling the court to inspect the document sought by the plaintiff, without the same document being released to the plaintiff before a judgment is reached. This stipulation could seem to be in conflict with the principle of equal treatment of clients before the court, but this is not the case. The legal objective of the plaintiff is to gain access to a withheld document, and under this amendment he or she may not accomplish that objective unless and until he has won the litigation. The current regulations also err by

requiring such actions to be conducted according to rules other than those of public administration lawsuits (RCP, Chapter XX).

4.10 The internal officer of informational rights

Considering the unified protection of the two informational rights in Hungary, as reflected both by the regulations and the institutional structure, it stands to reason to broaden the function of internal privacy officers to include the custody of both informational rights, particularly if the organization in question handles a large quantity of public information. This would imply an extension of purview without any special claims on costs or resources. The viability of this idea has been borne out by foreign examples and a number of Hungarian experiments, pioneered by the emulation of the "Canadian Model" by the office of public administration of Bács-Kiskun County.

In order to extend the benefits of this successful experiment to the entire country, we propose the enactment of the following provisions:

The title preceding § 31/A should be superseded by the following title:

> *The internal data protection officer, the data protection policy, and the internal officer for informational rights*

Clause b) of § 31/A (2) should be superseded by the following provision:

> *The internal data protection officer shall draft the internal data protection and data security policy, except for organizations that have appointed an internal officer for informational rights.*

§ 31/A should be supplemented by § 31/B as follows:

> *Organizations liable to maintain a web site shall appoint or hire an officer for informational rights, who shall have a university of college degree in law, public administration, computer science, or comparable disciple, and shall report directly to the executive of the organization. The creation of the post shall remain optional for other organizations exercising public functions.*
>
> *The internal officer for informational rights shall*
> *a) assume the duties of the internal data protection officer;*
> *b) participate in making decisions with disclosure implications and in safeguarding the rights of subjects;*
> *c) monitors compliance with this Act and other provisions, as well as the organization's internal policy of processing public information;*
> *d) investigate complaints in connection with the processing of public information;*
> *e) draft the organization's internal policy on informational rights.*