



Hungary adopts new sectoral data protection laws

Before the changes in eastern European political systems in 1989, little or no attention was paid to data protection in former socialist countries, including Hungary. The political and legislative practices in place at the time made no reference to data protection, nor did the citizens have any knowledge of the existence of the concept of data protection. Dr. Kinga Szurday, Data Protection Expert at Hungary's Ministry of the Interior, explains the legislative changes which have occurred and those which are being prepared.

The Hungarian Constitution was almost completely reformulated in 1989. An important part of the constituent work which laid the foundation for changing the Hungarian legal system was the integration of a guarantee of basic human rights into the Constitution. As a result, the protection of personal data as a fundamental right is now guaranteed to all individuals. Regulations which detail the exact requirements of this guarantee are set out in Hungary's Data Protection Act (PL&B, Sep 1995, p.3)

Decision number 15 of the Constitution Court in 1991 (PL&B, Dec 1991, p.20) provided an impetus for legislation on data protection. This decision first examined the constitutionality of the personal identification number (PIN) assigned to individuals. PINs were being very widely used without restrictions, and provided legislators with a concrete example of data collection which did not meet the standards of fair information practices. PINs became the basis on which legislators framed an act on data protection.

The data protection framework law

The result was that Act No. 63 of 1992 on the Protection of Personal Data and Freedom of Information (the *Data Protection Act*) was passed by Parliament in 1992. This Act contains two sometimes conflicting constitutional fundamental rights - the right to protection of personal data, and the right to freedom of information.

In common with the European Union Data Protection Directive, the Hungarian *Data Protection Act* starts from the principle that personal data should be collected directly from,

and with the consent of, the individual to whom it pertains. The individual has the right to know what information is being held about him or her, and has the right to request correction and deletion of personal data. Last but not least, the personal data must be used only for specifically determined purposes.

The Act allows for the compulsory disclosure of personal data contained in administrative registries only where specifically authorised under an Act. Furthermore, the Act sets out instances when the rights of the individual may be restricted, but again, only by statutory provisions. Examples of such instances are where there is a risk to the internal or external safety of the state, national defence, national security, prevention of crime, law enforcement, financial interests of the state or local governments, or the protection of other individuals.

Civil and criminal sanctions

Prevailing Hungarian law contains many civil and criminal sanctions for cases where an individual's right to personal data protection has been violated. The *Data Protection Act* enables an individual to bring an action for loss of data protection and to sue for damages. Sanctions are also possible if personal data is being maintained in some unauthorised manner. These sanctions vary with the severity of the unauthorised activity.

Hungary has a Data Protection Commissioner, Dr. Laszlo Majtenyi, who was elected in July 1995, whose role is to ensure that the *Data Protection Act* is being complied with, and also to examine whether or not the Act provides adequate data protection. The Commissioner's legal status is identical to that of an ombudsman. He or she has independent constitutional status and is elected by Parliament. Responsibilities of the Data Protection Commissioner include: general supervision of the Act, examination of individual complaints concerning the way that personal data is handled, and the keeping of records pertaining to data protection. This last responsibility is administrative in nature, and has no legal effect.

New sectoral statutes for state records

Hungary's *Data Protection Act* identifies compulsory data maintenance as a subject requiring statutory regulation. However, deciding just what data should be maintained has been a



difficult task. Previously, there was no statutory requirement to maintain data, and the result was that there were several systems of records management that were established by secret internal orders. After the *Data Protection Act* entered into force, the Hungarian government had to review all state administration and jurisdictional records maintained for compulsory data dissemination purposes, and had to enact legislation to provide the required statutory basis for this dissemination.

In the past four years, significant progress has been made in this area. Hungary's government is fulfilling the responsibilities set out in the legislation in two ways. Rules are being laid down concerning the basic administration of records, with regulations being assigned to specific activities in separate Acts.

Population records: One of the first steps in this direction, based on the above mentioned decision of the Constitutional Court, was the adoption of an Act which regulates the system of population records and sets out exactly to whom, for what purposes and under which conditions data may be disseminated. This Act allowed the use of PINs until December 31, 1995, and clearly spells out which organisations may use them and for which purposes they may be used.

Personal Identification Numbers (PINS): Since the previously mentioned decision of the Constitutional Court, there has been a continuing dispute surrounding the question of the constitutionality of the PIN and the further fate of the system of population records. The administrative system governing population records that is currently in operation was developed in 1972 based on a Swedish model. However, due to lack of technical facilities resulting from the ban of some computer system exports to former communist countries, as information was added over the years, it was not carried out in keeping with the original model. The result is that the population records are now administered under a system which is out-of-date from the standpoint of informatics, and there is no way to ensure that data is updated and current. At the same time, the circle in which this data can be disseminated is much smaller and more restricted than in Sweden.

Before 1991, the use of the PIN was very widespread, especially in banking and insurance. At the same time, it was not used - presumably because of lack of confidence in the system's western origin - in state record systems which belonged expressly to the oppressive structure of the communist system, such as records concerning party members and records dealing with the activities of the internal informant network.

On this basis, it is possible to dispute the commonly held view that the PIN is a symbol of the old oppressive communist system and should therefore be abolished. While the old regime may not have had any system of record keeping and may not have made use of PINs, it is a regrettable historical fact, not only in Hungary but elsewhere, that dictatorial systems violated privacy rights. In the most extreme manifestation of privacy invasion, these regimes took away peoples' lives. Today, it is indisputable, that guarantees and restrictions should be established relating to the use of PINs.

Recently, the Constitutional Court took a position once again on the question of PINs. In the Court's view, privacy rights can be adequately protected by introducing separate systems and different identifying symbols for different branches of government. The Hungarian government is now preparing an Act which makes it possible to separate the three big independent systems currently in existence as well as the identifying symbols assigned to them. The three systems are a system of tax records, a system of social insurance records, and a system of population records. Data files of the latter could serve as a model in the future when applying separate identifying symbols. It is important that managers of the three systems do not know each other's identifying codes. When data dissemination and exchange is required between the systems, it will be regulated by the Act, based on the content of the data and the purposes for which it is required. This draft Act is currently only an outline concept which will be discussed by Parliament in the coming months, and cannot yet be considered final.

Research and marketing data: The Hungarian government has prepared a separate draft Act dealing with the use and maintenance of personal data for scientific research, public opinion polls, market research and direct marketing. This Act,



number 119 adopted in late 1995, entered into force in January 1996.

Statistics: Special mention should be made of the *Act on Statistics* which was adopted by Parliament in 1992. It regulates data protection in the field of statistics in harmony with the recommendations of the Council of Europe.

There are two additional fields where data maintenance will be regulated by separate Acts: health data, and data on criminal proceedings and the regulation of criminal statistics.

Health and criminal data: A draft regulation on the protection and keeping of health data is now ready and Hungary's Parliament is expected to adopt it this year. Regarding criminal data, partial regulation is still required in areas such as criminal statistics. Other areas are dealt with by the *Criminal Code* and the *Police Act*.

Police data: It is important that lawyers dealing in data regulation make a serious attempt to incorporate fair information practices into sectoral Acts. The maintenance of police data has already been regulated in this way based again on the Recommendation of the Council of Europe in the *Act on the Police* adopted in 1993.

National defence: The *Act on National Defence* contains important data protection provisions which specify the personal data the defence authorities may collect and process about soldiers and to which institutions or persons this data may be transferred.

Passports: There is also an Act dealing with passports and records related to them. Border guards are currently being prepared with significant data protection responsibilities. In preparing the Act on border guards, Hungary should take into account the Schengen Information System (PL&B, Apr 1996, p.10) on police records relating to people travelling across borders, since it is no secret that Hungary intends to join the Schengen Agreement as soon as possible.

Council of Europe and the EU

Internationally, Hungary's Secretary of State has signed the Council of Europe Data Protection Convention No. 108 which Hungary plans to ratify after adopting the above legislation.

Moreover, Hungary is paying special attention to the regulatory activities of the European Union in this field. The White Book published by the

European Commission - which contains the harmonisation tasks in the field of legislation to be carried out by countries before joining - deals with data protection in a separate chapter. Therefore, it is very important for Hungary to analyse and process the European Union's Data Protection Directive as early as possible. (In this endeavour, the publications of *Privacy Laws & Business* have been of great assistance).

Reorganisation of state records needed

Besides legislative responsibilities, the Hungarian government has several additional tasks to undertake. The outdated systems of records must be reorganised in order to satisfy data security requirements, which will require significant financial resources. In the public administration, this task will be exceedingly difficult as only a small part of the anticipated costs can be met by the budget.

In the private sector, there are not as many obstacles to updating records systems, because private companies can maintain their market position only by keeping up-to-date records. However, public awareness that could force organisations, such as banks and insurance companies, to take data protection rules into account is not yet evident. The state does not plan to interfere with regulation in the private sector, but would like to see self-regulating mechanisms in operation. However, these have not yet taken shape in Hungary.

Need to raise public awareness

Finally, our most important task is to transform the consciousness of our citizens, to enrich their knowledge of their own privacy interests, and to encourage them to protect those interests by taking appropriate steps, such as appealing to a court, where necessary. Active legal protection like this was not practised during the period of socialism. The Data Protection Commissioner has a significant role to help familiarise the public with their rights to have their personal data protected and in raising awareness of their privacy rights.

This report was written by Dr. Kinga Szurday, Data Protection Expert, Interior Ministry, Budapest, Hungary and edited by Shauna Van Dongen, a Privacy Laws & Business consultant.