ANNEX 1

Act LXIII of 1992

on the Protection of Personal Data and the Disclosure of Information of Public Interest

Having regard to the protection of personal data and to access to information of public interest, the Parliament has adopted the following Act in accordance with the Constitution of the Republic of Hungary:

Chapter I

GENERAL PROVISIONS

Purpose of this Act

Section 1.

(1) The purpose of this Act is to ensure the right to privacy regarding personal data and free access to information of public interest, notwithstanding any exemptions provided by legal regulation specified in this Act.

(2) No derogation from the provisions of this Act shall be permitted, unless it is expressly provided for in this Act.

(3) Any exemption granted in this Act must apply to specific data and specific data manager together.

Scope

Section 1/A.

(1) This Act shall apply to all data management and data processing operations performed in the territory of the Republic of Hungary that pertain to the data of natural persons or to public information or information of public interest.

(2) This Act shall apply to data management and data processing operations whether performed in full or in part by an automated process or by manual processing.

(3) This Act shall not apply where data is processed by a natural person exclusively for his own purposes.

Definitions

Section 2.

For the purposes of this Act:

1) 'personal data' shall mean any information relating to an identified or identifiable natural person (hereinafter referred to as "data subject') and any reference drawn, whether directly or indirectly, from such information. In the course of data processing, such information shall be treated as personal data as long as the data subject remains identifiable through it. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

2) 'special data' shall mean

a) personal data revealing racial, national or ethnic origin, political opinions and any affiliation with political parties, religious or philosophical beliefs, trade-union membership,

b) personal data concerning health, addictions, sex life, or criminal record;

3) 'personal data relating to criminal offenses' shall mean personal data that might be related to the data subject or that pertain to any prior criminal offense committed by the data subject and that is obtained by organizations authorized to conduct criminal proceedings or investigations or by penal institutions during or prior to criminal proceedings in connection with a crime or criminal proceedings;

4) 'public information' shall mean 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);

5) 'public information subject to disclosure' shall mean any data managed by or pertaining to a natural or legal person or an unincorporated organization, other than public information that is not subject to disclosure, that are prescribed by law to be published or disclosed for the benefit of the general public;

6) 'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed without limitation or with regard to specific operations;

7) 'the data subject's objection' shall mean an indication of his wishes by which the data subject objects to the processing of his data and requests that the processing of data relating to him be terminated and/or the processed data be deleted;

8) 'controller' shall mean a natural or legal person or unincorporated organization that determines the purpose of the processing of personal data, makes decisions regarding data management (including the means) and implements such decisions itself or engages a processor to implement them;

9) 'data management' shall mean any operation or set of operations that is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, deletion or destruction, and blocking them from further use. Photographing, sound and video recording, and the recording of physical attributes for identification purposes (such as fingerprints and palm prints, DNA samples and retinal images;

10) 'disclosure by transmission' shall mean making data available to a specific third party;

11) 'public disclosure' shall mean making data available to the general public;

12) 'deletion of data' shall mean the destruction or elimination of data sufficient to make them irretrievable;

13) 'blocking of data' shall mean preventing - permanently or for a predetermined period - the transmission, access to, disclosure, adaptation or alteration, destruction, deletion, alignment or combination, and the use of data;

14) 'destruction of data' shall mean the complete physical destruction of data or the medium containing the data;

15) 'data processing' shall mean the technical operations involved in data management, irrespective of the method and instruments employed for such operations and the venue where it takes place;

16) 'processor' shall mean a natural or legal person or unincorporated organization that is engaged in the processing of personal data on behalf of a controller - including when ordered by virtue of legal regulation;

17) 'personal data filing system' (filing system) shall mean any structured set of personal data that are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

18) 'set of data' shall mean all data contained in a filing system;

19) 'third person' shall mean any natural or legal person or unincorporated organization other than the data subject, the controller or the processor;

20) 'third country' shall mean any country that is not a member of the European Union.

Chapter II

PROTECTION OF PERSONAL DATA

Data Processing

Section 3.

(1) Personal data may be processed if

a) the data subject has given his consent, or

b) decreed by law or by a local authority based on authorization conferred by law concerning specific data defined therein.

(2) Special data may be processed if

a) the data subject has given his explicit consent in writing, or

b) prescribed by treaty concerning the personal data specified in Point 2. a) of Section 2, or if ordered by law in connection with the enforcement of some constitutional right or for national security or law enforcement purposes,

c) ordered by law in other cases.

(3) Where data management is mandatory, the purpose and the conditions of management, the type of data and access to such data, the duration of the proposed processing operation, and the controller shall be specified by the statute or local government decree in which it is ordered.

(4) Where it serves the interest of the public, free access to particular personal data may be ordered by law as defined therein. In all other cases, free access to personal data may be provided only upon the consent of the data subject that is to be made in writing with regard to special data. If there is any doubt, it is to be presumed that the data subject did not consent to allow free access.

(5) The consent of the data subject shall be considered granted in connection with any data he has conveyed to the public or has supplied for publication.

(6) In connection with any proceeding requested by the data subject, his consent for processing his data to the extent necessary shall be considered granted, of which the data subject must be advised.

(7) The data subject may grant consent in a written agreement concluded with the controller for the performance of the contract. In this case, the contract shall contain all information that is to be made available to the data subject under this Act in connection with the processing of personal data, such as the description of the data involved, the duration of the proposed processing operation, the purpose of processing, the transmission of data and the use of a processor. The contract must clearly indicate the data subject's signature and explicit consent for having his data processed as stipulated in the contract.

(8) If the data subject is physically or legally incapable of giving his consent for processing his personal data, the processing of his personal data - which includes his special data - is allowed to the extent necessary to protect the vital interests of the data subject or of another person or in order to prevent or avert a catastrophe or emergency.

Section 4.

The right for the protection of personal data and the fundamental right to privacy of individuals must not be breached by any other interest, including free access to information of public interest (Section 19) for data processing, unless an exemption is granted by law.

Data Processing

Section 4/A.

(1) The rights and obligations of data processors arising in connection with the processing of personal data shall be determined by the data manager within the scope specified by the this Act and other legislation on data management. The data manager shall be held liable for the legitimacy of instructions pertaining to data management operations.

(2) The data processor shall be held liable within his sphere of competence and within the scope specified by the data manager for the processing, alteration, erasure and disclosure by transmission of personal data. The data processor shall not be permitted to subcontract any part of his operations to another data processor.

(3) A processor may not make any decision on the merits of data management and shall process any and all data entrusted to him solely as instructed by the controller; the processor shall not engage in data processing for his own purposes and shall store and safeguard personal data according to the instructions of the controller.

(4) Contracts for the processing of data must be made in writing. Any company that is interested in the business activity for which personal data is used may not be contracted for the processing of such data.

(5) Contracts for the processing of data to be concluded with third-country processors shall be drafted in compliance with the Decision of the Commission of the European Communities, which has been published by the data protection commissioner in *Magyar Közlöny* [Official Hungarian Gazette].

(6) This Act shall apply if a third-country controller that is involved in the processing of personal data employs a processor whose registered address or place of business (branch) or habitual residence (place of abode) is situated in the territory of the Republic of Hungary or if it makes use of equipment situated on the territory of the Republic of Hungary, unless such equipment is used solely for the purpose of transit through the territory of the European Union. Such controllers shall have a representative installed in the territory of the Republic of Hungary.

Legitimacy of Data Processing

Section 5.

(1) Personal data may be processed only for specified and explicit purposes, where it is necessary for carrying out certain rights or obligations. This purpose must be satisfied in all stages of operations of data processing.

(2) 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.

(3) The processing of data prescribed to be disclosed may be ordered in the public interest.

(4) Personal data may - with the data subject's consent or by virtue of legal regulation - be processed for the performance of a task carried out in the public interest or in the exercise of official authority, in the fulfillment of the official tasks of the controller or the recipient third party, for the protection of the data subject's vital interest, for the performance of a contract between the data subject and the controller, in the legitimate interests of the controller or a third party, or in the legitimate operation of a charitable organization.

(5) Personal data that concern criminal offenses and are being processed for the purposes of preventing, investigating, detecting and prosecuting criminal offences and data files containing information pertaining to misdemeanor cases, civil lawsuits and non-litigious cases may only be processed by central or local government authorities.

Section 6.

(1) Prior to the collection of data the data subject shall be informed whether disclosure is voluntary or compulsory. If compulsory, the legal regulation on which it is based shall also be indicated.

(2) The data subject shall be clearly and elaborately informed of all aspects concerning the processing of his personal data, such as the purpose for which his data is required and the legal grounds, the person entitled to carry out the processing, the duration of the proposed processing operation and the persons to whom his data may be disclosed. Information shall also be provided on the data subject's rights and remedies.

(3) Notification of data management is considered granted where disclosure by transmission from existing data processing operations or by alignment or combination for further processing is prescribed by legal regulation.

(4) If individual notification is impossible or likely to result in unreasonable expense, notification of data management - particularly if it is for statistical or scientific purposes (including historical research) - may occur by way of publishing the fact of data collection, the data subjects involved, the purpose and duration of the proposed processing operation and the availability of data.

Data Quality

Section 7.

(1) Personal data collected for processing must be

a) processed fairly and lawfully;

b) accurate, complete and, where necessary, kept up to date;

c) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected.

(2) The use of personal identification codes or any other identifier of general application shall not be permitted.

Transfer of Data, Set of Transfer Operations

Section 8.

(1) Data may be transferred, whether in a single or in a set of operations, if the data subject has given his consent or if the transfer is legally permitted, and if the safeguards for data processing are satisfied with regard to each and every personal data.

(2) Subsection (1) shall also apply where data is structured between various filing systems of the same processor, or between those of government and local authorities.

Transfer of Data to Foreign Countries

Section 9.

(1) Personal data (including special data) may be transferred - irrespective of the medium and the manner in which it is transferred - to a third-country controller or processor if the data subject has given his consent, if the transfer is permitted by law or if it is prescribed by treaty or international convention, provided the laws of the third country in

question afford an adequate level of protection within the meaning of Community standards with respect to the processing of the data transferred.

(2) Transmission of data to Member States of the European Union shall be treated as transmission within the territory of the Republic of Hungary.

Automated Individual Decisions

Section 9/A.

(1) Evaluation of certain personal aspects of any person by automated (computerized) processing of data may only be carried out if the data subject explicitly gives his consent or if such evaluation is permitted by law. The data subject must be given the opportunity to express his opinion.

(2) Where personal data is processed by automated means, the data subject must, at his request, be informed of the mathematical method that is used and its essence.

Security of Processing

Section 10.

(1) Data managers, and within their sphere of competence, data processors must implement adequate safeguards and appropriate technical and organizational measures to protect personal data, as well as adequate procedural rules to enforce the provisions of this Act and other regulations concerning confidentiality and security of data processing.

(2) Data must be protected against unauthorized access, alteration, transfer, disclosure by transmission or deletion as well as damage and accidental destruction. For the technical protection of personal data, the controller, the processor or the operator of the telecommunications or information technology equipment shall implement security measures in particular if the processing involves the transmission of data over a network or any other means of information technology.

The Rights of Data Subjects and their Enforcement

Section 11.

(1) Any data subject may request

a) confirmation as to whether or not data relating to him are being processed (Sections 12 and 13), and

b) the rectification or erasure of his personal data, with the exception of those processed by order of legal regulation (Sections 14-16).

(2) The register of processing operations [Subsection (1) of Section 28] may be inspected (including the taking of notes) by any person. An extract of the data contained therein may be requested upon payment of a fee.

Section 12.

(1) Upon the data subject's request the data manager must provide information concerning the data relating to him, including those processed by a data processor on its behalf, the purpose, grounds and duration of processing, the name and address (corporate address) of the data processor and on its activities relating to data management, and the recipients of his data and the purpose for which they are or had been transferred. The duration for which records must be kept on the data transferred, and in consequence the obligation of information may be limited by legal regulation on data processing. The period of restriction shall not be less than five years in respect of personal data, and twenty years in respect of special data.

(2) Data processor must comply with requests for information without any delay, and provide the information requested in an intelligible form within no more than 30 days.

(3) The information specified in Subsection (2) shall be provided free of charge for any category of data once a year. Additional information concerning the same category of data may be subject to a charge. Where any payment is made in connection with data that was processed unlawfully, or the request led to rectification, it shall be refunded.

Section 13.

(1) A data processor may refuse to provide information to the data subject where it is permitted by law in the cases defined under Section 16.

(2) The data processor must notify the data subject of the reasons for refusal.

(3) Data processors shall notify the data protection commissioner once a year on refused requests.

Section 14.

(1) Data processors must correct the data if it is false.

(2) Personal data must be erased if

a) processed unlawfully;

b) so requested by the data subject in accordance with Paragraph b) of Subsection (1) of Section 11;

c) it is deficient or inaccurate and it cannot be legitimately corrected, provided that deletion is not disallowed by statutory provision;

d) the purpose of processing no longer exists or the legal time limit for storage has expired;

e) so instructed by court order or by the data protection commissioner.

(3) With the exception of illicit data processing, the requirement of erasure shall not apply to the personal data recorded on a medium that is to be deposited in archive under the legal regulation on archive materials.

Section 15.

When a data is corrected or erased, the data subject to whom it pertains and all recipients to whom it was transferred for processing must be notified. This notification shall not be required if it does not violate the rightful interest of the data subject in view of the purpose of processing.

Section 16.

The rights of data subjects (Sections 11-15) may be restricted by this Act in order to safeguard the external and internal security of the State (e.g., defense, national security, the prevention, investigation, detection and prosecution of criminal offences), protect the economic and financial interests of central and local government, safeguard the important economic and financial interests of the European Union, guard against disciplinary and ethical breaches in the regulated professions, prevent and detect breaches of obligation related to labor law and job safety - including in all cases control and supervision - and to protect data subjects or the rights and freedoms of others.

The Data Subject's Right to Object

Section 16/A.

(1) The data subject shall have the right to object to the processing of data relating to him

a) if processing (disclosure) is carried out solely for the purpose of enforcing the rights and legitimate interests of the controller or the recipient, unless processing is prescribed by law;

b) if personal data is used or transferred for the purposes of direct marketing, public opinion polling or scientific research;

c) if the right to object is ensured by law.

(2) In the event of objection, the controller shall discontinue processing operations and investigate the cause of objection within the shortest possible time, not to exceed 15 days, and shall notify the data subject in writing of the findings of the investigation. If the objection is justified, the controller shall terminate all processing operations (including data collection and transmission), block the data involved and notify all recipients to whom any of these data had been previously transferred concerning the objection and the ensuing measures; these recipients shall also take measures regarding the objection.

(3) If the data subject disagrees with the decision taken by the controller under Subsection (2), the data subject shall have the right under this Act to seek legal remedy within 30 days of the date the decision was conveyed.

(4) If data that are necessary to assert the data recipient's lawful rights are withheld owing to the data subject's objection, the data recipient shall have the right under this Act to file charges against the controller within 15 days from the date the decision is conveyed under Subsection (2) in order to obtain the data. The controller may implicate the data subject in such lawsuit.

(5) If the court rejects the petition filed by the data recipient, the controller shall be required to delete the data subject's personal data within three days of the court ruling. The controller shall delete the data even if the data recipient does not file for court action within the time limit referred to in Subsection (4).

(6) The controller shall not delete the data of the data subject if processing has been prescribed by law. However, data may not be disclosed to the data recipient if the controller agrees with the objection or if the court has found the objection justified.

Judicial Remedy

Section 17.

(1) The data subject and the person referred to in Subsection (4) of Section 16/A may file for court action against the controller for any violation of their rights. The court shall hear such cases immediately.

(2) The burden of proof of compliance with the law lies with the data processor.

(3) Such lawsuits are heard by the court in whose jurisdiction the controller's registered address (residence) is located or, if so requested by the data subject, by the court in whose jurisdiction the data subject's residence (place of abode) is located. Even persons lacking legal capacity to sue may be a party in such lawsuits.

(4) When the decision is in favor of the plaintiff, the court shall order the controller to provide the information, to correct or delete the data in question, to void the automated individual decision, to honor the data subject's objection, or to disclose the data requested by the person referred to in Subsection (4) of Section 16/A.

(5) The court may also order publication of its decision, by way of publishing the identification data of the controller, if it is necessitated for data protection in general or in connection with the rights of large numbers of data subjects under protection by this Act.

Liability

Section 18.

(1) Data managers shall be liable for any damage caused to a data subject as a result of unlawful processing or by breaching the technical requirements of data protection. The data manager shall also be liable for any damage caused by a data processor acting on its behalf. The data manager may be exempted from liability if he proves that the damage was caused by reasons beyond his control.

(2) No compensation shall be paid where the damage was caused by intentional or negligent conduct on the part of the data subject.

Chapter III

ACCESS TO INFORMATION OF PUBLIC INTEREST

Section 19.

(1) State or local public authorities and agencies and other bodies attending to the public duties specified by law (hereinafter jointly referred to as "agency') shall provide the general public with accurate and speedy information concerning the matters under their competence, such as the budgets of the central government and local governments and the implementation thereof, the management of assets controlled by the central government and by local governments, the appropriation of public funds, and special and exclusive rights conferred upon market actors, private organizations or individuals.

(2) The agencies referred to in Subsection (1) shall regularly publish or otherwise make available all information of import concerning their competence, jurisdiction, organizational structure, professional activities, the evaluation of such activities (including their effectiveness), the categories of data they process, the legal regulations that pertain to their operations, and their financial management. The names and positions of persons acting in the name and on behalf of the above-specified agencies shall be treated as public information, unless otherwise prescribed by law. The manner of disclosure and the data to be disclosed may be prescribed by legal regulation.

(3) The agencies defined in Subsection (1) shall allow free access to the public information they have on files to any person, excluding those labelled state or service secret by an agency vested with proper authorization, or if classified by virtue of commitment under treaty or convention, or if access to specific information of public interest is restricted by law in connection with

a) defense;

b) national security;

c) prevention, investigation, detection and prosecution of criminal offences;
d) central financial or foreign exchange policy;
e) external relations, relations with international organizations;
f) court proceeding.

(4) The personal data of a person acting in the name and on behalf of the agencies specified in Subsection (1), to the extent that it relates to his duties, shall not restrict access to specific information of public interest.

(5) 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.

(6) Access to business secrets in connection with access to and publication of information of public interest shall be governed by the relevant provisions of the Civil Code.

(7) The availability of public information may also be limited by European Union legislation with a view to any important economic or financial interests of the European Union, including monetary, budgetary and tax policies.

Section 20.

(1) The agencies processing information of public interest must comply with requests for information without any delay, and shall provide it in an intelligible form within no more than 15 days. The applicant may also request for a fee, a copy of the document or part of a document containing the data in question, regardless of the form of storage.

(2) When a request for information is refused, the applicant must be notified within 8 days in writing and must be given the reasons for refusal.

(3) The head of agency processing information of public interest may charge a fee for any supply of information, not exceeding the costs of service. If requested by the applicant, the amount of charges must be specified in advance.

(4) The agencies specified in Subsection (1) of Section 19 shall notify the data protection commissioner once a year on refused requests, including the reasons of refusal.

Section 21.

(1) When a person's request for public information is refused, he may file for court action.

(2) The burden of proof of compliance with the law lies with the data processor agency.

(3) The lawsuit shall be initiated within 30 days from the date of refusal against the agency that has refused the information.

(4) Any person who cannot sue or be sued may also be involved in such lawsuits.

(5) Lawsuits against agencies of nationwide jurisdiction shall be filed at the competent county (Budapest) court. Lawsuits against local agencies shall be filed at the central county court, or at the Central Pest District Court in Budapest. The competency of the court is determined based on the location of the agency that refused to provide information.

(6) The court shall hear such cases under priority.

(7) When the decision is in favor of the plaintiff, the court shall order the data processor agency to provide the information.

Section 22.

This Chapter shall not apply to the supply of information from official records that is subject to the provisions of specific other legislation.

Chapter IV

DATA PROTECTION COMMISSIONER, REGISTER OF PROCESSING OPERATIONS

Data Protection Commissioner

Section 23.

(1) To protect the rights and freedoms afforded by the Constitution for the protection of personal data and access to information of public interest, the Parliament shall appoint a data protection commissioner from candidates of high

repute satisfying the following criteria: must be a Hungarian citizen holding a diploma, have no prior criminal record, must have outstanding theoretical knowledge or 10 years of professional experience in the field of data protection, including all phases of administration and control.

(2) The provisions of the Act on the Ombudsman of Civil Rights shall apply to the data protection commissioner with the exceptions set forth in this Act.

Section 24.

The data protection commissioner

a) shall oversee compliance with the regulations of this Act and other legislation related to data protection;

b) shall investigate the reports he receives;

c) shall provide for the register of processing operations.

d) shall facilitate the uniform enforcement of the statutory provisions on the processing of personal data and on the availability of public information;

e) shall exercise and perform the tasks and duties conferred under this Act.

Section 25.

(1) The data protection commissioner shall monitor compliance with the requirements for the protection of personal data and for free access to information of public interest. He/she shall have authority to make recommendations for new regulations and for the amendment of legislation pertaining to data processing and information of public interest, and shall express his opinion on bills covering the same subject. As to the scope of data to be treated as state or service secrets, the data protection commissioner shall have authority to recommend specific data to be removed or added.

(2) Upon noticing any unlawful data processing operation, the data protection commissioner shall advise the data processor to cease such operation. The data processor must comply within 30 days and shall report to the data protection commissioner in writing concerning the measures taken.

(3) If the controller or processor fails to comply and cease the above-specified unlawful data processing operation, the data protection commissioner may order that unlawfully processed data be blocked, deleted or destroyed, or the data protection commissioner may prohibit the unauthorized data management and/or processing operations and suspend any operation aimed at transferring data abroad. The data protection commissioner shall announce these illegitimate data management and/or processing operations to the public and identify the controller (processor) and the measures proposed by it.

(4) The controller, the processor or the data subject may seek judicial remedy against the data protection commissioner's actions. The data involved in such litigated data processing operations may not be deleted or destroyed until the court has made a definitive ruling; however, processing operations must be discontinued and data must be blocked.

Section 26.

(1) The data protection commissioner in his official capacity shall have powers to request information from data processors and to inspect any document and processing operations that may involve personal data or information of public interest.

(2) The data protection commissioner shall be authorized to enter any premises where data processing takes place.

(3) The data protection commissioner shall also have access to state and service secrets in connection with his official duties defined in this Section, however, the rules of confidentiality must be observed by the data protection commissioner as well. The data protection commissioner must act in person when investigating any case of data processing that involves state or service secrets, or may have members of his staff acting on his behalf, if they have volunteered and have been checked for national security reasons.

(4) When the data protection commissioner concludes in his official capacity that any restricted-access data has been classified without proper justification, other than those classified by virtue of treaty or convention, the commissioner shall instruct the person by whom it was classified to lift or revise the restriction. The classifying person may contest such instruction within 30 days at the Municipal Court of Budapest where it will be heard in a closed session under priority.

Section 27.

(1) In the case of any violation of the rights of a person in connection with his personal data or free access to public information, or if there is imminent danger of such violation, it shall be reported to the data protection commissioner, unless a court action is already pending concerning the case in question.

(2) The person making a report to the data protection commissioner must not suffer any detriment for making such report. Any person filing such report shall be entitled to the same protection afforded to persons filing reports in the public interest.

Register of Processing Operations

Section 28.

(1) Prior to commencing operations, data processors must notify for the purpose of registration the data protection commissioner of the following:

a) the purpose of processing;

b) the category of data and the grounds for processing;

c) the data subjects involved;

d) the source;

e) the categories of data transferred, the recipients and the grounds for transfer;

f) the deadline of erasure of specific categories;

g) name and address (corporate address) of the data manager and the data processor, the place where records are kept and/or where processing is carried out, and the data processor's activities in connection with data management operations.

h) the name of and contact information for the internal data protection officer.

(2) When the processing of certain data is prescribed by legal regulation, it shall be announced by the competent minister, the director of the agency of national jurisdiction, or by the mayor or the person presiding over the county assembly concerned within 15 days from the date when the legal regulation in question enters into force.

(3) National security agencies shall announce the purpose and the grounds for data processing.

Section 29.

(1) Upon registration, each data processor shall be issued a registration number. This registration number shall be used for all operations with data, such as when data is transferred or published, or when provided to the data subject.

(2) Any changes in the data specified Subsection (1) of Section 28 shall be reported to the data protection commissioner within 8 days, and the records shall be revised accordingly.

Section 30.

Data processing shall not be notified to the register of processing operations

a) when it concerns the data of the data processor's employees, members, students or customers;

b) when carried out in accordance with the internal rules of the church or other religious organization;

c) if it concerns the personal data of a person undergoing medical treatment, for the purposes of health care and preventive measures or for settling claims for benefits and services in the social insurance system;

d) where it contains information concerning the provision of social and other benefits to the data subject;

e) where it contains the personal data of persons implicated in an official regulatory, public prosecutor or court proceeding to the extent required for such proceeding;

f) if it contains personal data for official statistical purposes, provided there are adequate guarantees that the data is rendered anonymous in such a way that the data subject is no longer identifiable;

g) where it contains data of organizations and bodies falling under the scope of the Media Act, if they are used solely for their own information;

h) if it serves the purposes of scientific research, and if the data are not made available to the public;

i) if the data is transferred to a public archive;

j) if it serves the own purposes of a natural person.

Preliminary Inspection

Section 31.

(1) The data protection commissioner shall have powers to conduct preliminary inspections prior to registration.

(2) Prior to the processing of any new data files or the use of new data processing technologies, the data protection commissioner may conduct preliminary inspections at controllers processing the following data:

a) data files concerning authorities of nationwide jurisdiction, data files concerning employment and criminal records;

b) data files from the customer records of financial institutions and public utility companies;

c) data files from the customer records of telecommunications service providers;

d) data files containing the individual statistical data defined in specific other legislation.

(3) Controllers shall be required to notify the data protection commissioner 30 days prior to the commencement of the processing of any new data files or the use of new data processing technologies. The data protection commissioner shall notify a controller of his intention to conduct a preliminary inspection within eight days of receiving the above-specified notification and shall carry out the inspection within 30 days. Processing operations may commence only upon completion of the inspection conducted by the data protection commissioner.

(4) On the basis of the findings of the inspection, the data protection commissioner may prohibit the processing of specific data or may instruct the controller to change the processing technology. If the data protection commissioner disagrees with the legal regulation prescribing data processing, he may submit a proposal to amend the legal regulation in question.

Internal Data Protection Officer, Data Protection Regulations

Section 31/A.

(1) The following controllers and processors shall appoint or commission an internal data protection officer - who shall hold a law degree, a degree in economics or computer sciences or an equivalent degree in higher education - who is to report directly to the head of the organization:

a) authorities of nationwide jurisdiction, and controllers and processors engaged in processing data files of employment and criminal records;

b) financial institutions;

c) telecommunications service providers and public utility companies.

(2) The internal data protection officer shall:

a) participate and assist in the decision-making process with regard to data processing and in enforcing the rights of data subjects;

b) monitor compliance with the provisions of this Act and other legal regulations on data processing as well as with the provisions of internal data protection and data security regulations and the data security requirements;

c) investigate complaints conveyed to him and, if he detects any unauthorized data processing operations, request the controller or processor in question to cease such operations;

d) prepare the internal data protection and data security regulations;

e) maintain the internal data protection register;

f) arrange training sessions on the subject of data protection.

(3) The controllers referred to in Subsection (1) and central and local government controllers - other than controllers not required to report to the data protection register - shall be required to adopt data protection and data security regulations in accordance with this Act.

Chapter V

SPECIAL PROVISIONS

Processing and Use of Personal Data by Research Institutions

Section 32.

(1) Personal data collected and stored for scientific reasons must be used only for scientific research projects.

(2) Any personal data that no longer serves research purposes must be rendered anonymous. Any data relating to an identified or identifiable natural person must be stored separately. Such data may be related to other data if it is necessary for the purposes of research.

(3) An agency or person performing scientific research shall be allowed to publish personal data only if

a) the data subject has given his consent, or
b) it is necessary to demonstrate the findings of research in connection with historical events.

Use of Personal Data for Statistical Purposes

Section 32/A.

(1) Personal data recorded, received or processed for statistical purposes may only be used for statistical purposes. The individual statistical data defined in specific other legislation, including personal data, may not be transferred, received or processed in any way or form or under any circumstances, and they may not be published.
(2) The detailed regulations governing processing operations involving personal data are contained in another act.

Chapter VI

CLOSING PROVISIONS

Amendments

Section 33.

The following provision shall replace Subsection (1) of Section 83 of Act IV of 1959 on the Civil Code of the Republic of Hungary:
(1) Data management and data processing by computer or other means may not violate inherent rights."

Entry into Force

Section 34.

(1) This Act, with the exceptions set forth in Subsections (2) and (3), shall enter into force on the first day of the sixth mouth following its promulgation.
(2) Chapter III (Sections 19-22) of this Act shall enter into force on the 15th day following promulgation.
(3) Chapter IV (Sections 23-31) of this Act shall enter into force simultaneously with the Act on the Ombudsman for Civil Rights.

Section 35.

(1) Where this Act prescribes legislation in the form of an act, it shall be drafted by 31 December 1992, with the exception of Subsection (3), Section 4, and Subsection (1) of Section 13.
(2) Legal directives in connection with data processing cannot be used after the promulgation of this Act.

Section 36.

(1)
(2) Data processors shall notify all processing operations already existing at the time of this Act entering into force within three months from the appointment of the data protection commissioner for registration in the register of processing operations.

Section 37.

The Minister of Finance is hereby authorized to decree the amount of fees payable under Subsection (2) of Section 11 and the detailed regulations for the administration of such fees.

Act LXIII of 1992

on the Protection of Personal Data and the Disclosure of Information of Public Interest

Having regard to the protection of personal data and to access to information of public interest, the Parliament has adopted the following Act in accordance with the Constitution of the Republic of Hungary:

Chapter I

GENERAL PROVISIONS

Purpose of this Act

Section 1.

(1) The purpose of this Act is to ensure the right to privacy regarding personal data and free access to information of public interest, notwithstanding any exemptions provided by legal regulation specified in this Act.

(2) No derogation from the provisions of this Act shall be permitted, unless it is expressly provided for in this Act.

(3) Any exemption granted in this Act must apply to specific data and specific data manager together.

Scope

Section 1/A.

(1) This Act shall apply to all data management and data processing operations performed in the territory of the Republic of Hungary that pertain to the data of natural persons or to public information or information of public interest.

(2) This Act shall apply to data management and data processing operations whether performed in full or in part by an automated process or by manual processing.

(3) This Act shall not apply where data is processed by a natural person exclusively for his own purposes.

Definitions

Section 2.

For the purposes of this Act:

1) 'personal data' shall mean any information relating to an identified or identifiable natural person (hereinafter referred to as "data subject') and any reference drawn, whether directly or indirectly, from such information. In the course of data processing, such information shall be treated as personal data as long as the data subject remains identifiable through it. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

2) 'special data' shall mean

a) personal data revealing racial, national or ethnic origin, political opinions and any affiliation with political parties, religious or philosophical beliefs, trade-union membership,

b) personal data concerning health, addictions, sex life, or criminal record;

3) 'personal data relating to criminal offenses' shall mean personal data that might be related to the data subject or that pertain to any prior criminal offense committed by the data subject and that is obtained by organizations authorized to conduct criminal proceedings or investigations or by penal institutions during or prior to criminal proceedings in connection with a crime or criminal proceedings;

4) 'public information' shall mean 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);

5) 'public information subject to disclosure' shall mean any data managed by or pertaining to a natural or legal person or an unincorporated organization, other than public information that is not subject to disclosure, that are prescribed by law to be published or disclosed for the benefit of the general public;

6) 'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed without limitation or with regard to specific operations;

7) 'the data subject's objection' shall mean an indication of his wishes by which the data subject objects to the processing of his data and requests that the processing of data relating to him be terminated and/or the processed data be deleted;

8) 'controller' shall mean a natural or legal person or unincorporated organization that determines the purpose of the processing of personal data, makes decisions regarding data management (including the means) and implements such decisions itself or engages a processor to implement them;

9) 'data management' shall mean any operation or set of operations that is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, deletion or destruction, and blocking them from further use. Photographing, sound and video recording, and the recording of physical attributes for identification purposes (such as fingerprints and palm prints, DNA samples and retinal images;

10) 'disclosure by transmission' shall mean making data available to a specific third party;

11) 'public disclosure' shall mean making data available to the general public;

12) 'deletion of data' shall mean the destruction or elimination of data sufficient to make them irretrievable;

13) 'blocking of data' shall mean preventing - permanently or for a predetermined period - the transmission, access to, disclosure, adaptation or alteration, destruction, deletion, alignment or combination, and the use of data;

14) 'destruction of data' shall mean the complete physical destruction of data or the medium containing the data;

15) 'data processing' shall mean the technical operations involved in data management, irrespective of the method and instruments employed for such operations and the venue where it takes place;

16) 'processor' shall mean a natural or legal person or unincorporated organization that is engaged in the processing of personal data on behalf of a controller - including when ordered by virtue of legal regulation;

17) 'personal data filing system' (filing system) shall mean any structured set of personal data that are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

18) 'set of data' shall mean all data contained in a filing system;

19) 'third person' shall mean any natural or legal person or unincorporated organization other than the data subject, the controller or the processor;

20) 'third country' shall mean any country that is not a member of the European Union.

Chapter II

PROTECTION OF PERSONAL DATA

Data Processing

Section 3.

(1) Personal data may be processed if

a) the data subject has given his consent, or

b) decreed by law or by a local authority based on authorization conferred by law concerning specific data defined therein.

(2) Special data may be processed if

a) the data subject has given his explicit consent in writing, or

b) prescribed by treaty concerning the personal data specified in Point 2. a) of Section 2, or if ordered by law in connection with the enforcement of some constitutional right or for national security or law enforcement purposes,

c) ordered by law in other cases.

(3) Where data management is mandatory, the purpose and the conditions of management, the type of data and access to such data, the duration of the proposed processing operation, and the controller shall be specified by the statute or local government decree in which it is ordered.

(4) Where it serves the interest of the public, free access to particular personal data may be ordered by law as defined therein. In all other cases, free access to personal data may be provided only upon the consent of the data subject that is to be made in writing with regard to special data. If there is any doubt, it is to be presumed that the data subject did not consent to allow free access.

(5) The consent of the data subject shall be considered granted in connection with any data he has conveyed to the public or has supplied for publication.

(6) In connection with any proceeding requested by the data subject, his consent for processing his data to the extent necessary shall be considered granted, of which the data subject must be advised.

(7) The data subject may grant consent in a written agreement concluded with the controller for the performance of the contract. In this case, the contract shall contain all information that is to be made available to the data subject under this Act in connection with the processing of personal data, such as the description of the data involved, the duration of the proposed processing operation, the purpose of processing, the transmission of data and the use of a processor. The contract must clearly indicate the data subject's signature and explicit consent for having his data processed as stipulated in the contract.

(8) If the data subject is physically or legally incapable of giving his consent for processing his personal data, the processing of his personal data - which includes his special data - is allowed to the extent necessary to protect the vital interests of the data subject or of another person or in order to prevent or avert a catastrophe or emergency.

Section 4.

The right for the protection of personal data and the fundamental right to privacy of individuals must not be breached by any other interest, including free access to information of public interest (Section 19) for data processing, unless an exemption is granted by law.

Data Processing

Section 4/A.

(1) The rights and obligations of data processors arising in connection with the processing of personal data shall be determined by the data manager within the scope specified by the this Act and other legislation on data management. The data manager shall be held liable for the legitimacy of instructions pertaining to data management operations.

(2) The data processor shall be held liable within his sphere of competence and within the scope specified by the data manager for the processing, alteration, erasure and disclosure by transmission of personal data. The data processor shall not be permitted to subcontract any part of his operations to another data processor.

(3) A processor may not make any decision on the merits of data management and shall process any and all data entrusted to him solely as instructed by the controller; the processor shall not engage in data processing for his own purposes and shall store and safeguard personal data according to the instructions of the controller.

(4) Contracts for the processing of data must be made in writing. Any company that is interested in the business activity for which personal data is used may not be contracted for the processing of such data.

(5) Contracts for the processing of data to be concluded with third-country processors shall be drafted in compliance with the Decision of the Commission of the European Communities, which has been published by the data protection commissioner in *Magyar Közlöny* [Official Hungarian Gazette].

(6) This Act shall apply if a third-country controller that is involved in the processing of personal data employs a processor whose registered address or place of business (branch) or habitual residence (place of abode) is situated in the territory of the Republic of Hungary or if it makes use of equipment situated on the territory of the Republic of Hungary, unless such equipment is used solely for the purpose of transit through the territory of the European Union. Such controllers shall have a representative installed in the territory of the Republic of Hungary.

Legitimacy of Data Processing

Section 5.

(1) Personal data may be processed only for specified and explicit purposes, where it is necessary for carrying out certain rights or obligations. This purpose must be satisfied in all stages of operations of data processing.

(2) 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.

(3) The processing of data prescribed to be disclosed may be ordered in the public interest.

(4) Personal data may - with the data subject's consent or by virtue of legal regulation - be processed for the performance of a task carried out in the public interest or in the exercise of official authority, in the fulfillment of the official tasks of the controller or the recipient third party, for the protection of the data subject's vital interest, for the performance of a contract between the data subject and the controller, in the legitimate interests of the controller or a third party, or in the legitimate operation of a charitable organization.

(5) Personal data that concern criminal offenses and are being processed for the purposes of preventing, investigating, detecting and prosecuting criminal offences and data files containing information pertaining to misdemeanor cases, civil lawsuits and non-litigious cases may only be processed by central or local government authorities.

Section 6.

(1) Prior to the collection of data the data subject shall be informed whether disclosure is voluntary or compulsory. If compulsory, the legal regulation on which it is based shall also be indicated.

(2) The data subject shall be clearly and elaborately informed of all aspects concerning the processing of his personal data, such as the purpose for which his data is required and the legal grounds, the person entitled to carry out the processing, the duration of the proposed processing operation and the persons to whom his data may be disclosed. Information shall also be provided on the data subject's rights and remedies.

(3) Notification of data management is considered granted where disclosure by transmission from existing data processing operations or by alignment or combination for further processing is prescribed by legal regulation.

(4) If individual notification is impossible or likely to result in unreasonable expense, notification of data management - particularly if it is for statistical or scientific purposes (including historical research) - may occur by way of publishing the fact of data collection, the data subjects involved, the purpose and duration of the proposed processing operation and the availability of data.

Data Quality

Section 7.

(1) Personal data collected for processing must be

a) processed fairly and lawfully;

b) accurate, complete and, where necessary, kept up to date;

c) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected.

(2) The use of personal identification codes or any other identifier of general application shall not be permitted.

Transfer of Data, Set of Transfer Operations

Section 8.

(1) Data may be transferred, whether in a single or in a set of operations, if the data subject has given his consent or if the transfer is legally permitted, and if the safeguards for data processing are satisfied with regard to each and every personal data.

(2) Subsection (1) shall also apply where data is structured between various filing systems of the same processor, or between those of government and local authorities.

Transfer of Data to Foreign Countries

Section 9.

(1) Personal data (including special data) may be transferred - irrespective of the medium and the manner in which it is transferred - to a third-country controller or processor if the data subject has given his consent, if the transfer is permitted by law or if it is prescribed by treaty or international convention, provided the laws of the third country in question afford an adequate level of protection within the meaning of Community standards with respect to the processing of the data transferred.

(2) Transmission of data to Member States of the European Union shall be treated as transmission within the territory of the Republic of Hungary.

Automated Individual Decisions

Section 9/A.

(1) Evaluation of certain personal aspects of any person by automated (computerized) processing of data may only be carried out if the data subject explicitly gives his consent or if such evaluation is permitted by law. The data subject must be given the opportunity to express his opinion.

(2) Where personal data is processed by automated means, the data subject must, at his request, be informed of the mathematical method that is used and its essence.

Security of Processing

Section 10.

(1) Data managers, and within their sphere of competence, data processors must implement adequate safeguards and appropriate technical and organizational measures to protect personal data, as well as adequate procedural rules to enforce the provisions of this Act and other regulations concerning confidentiality and security of data processing.

(2) Data must be protected against unauthorized access, alteration, transfer, disclosure by transmission or deletion as well as damage and accidental destruction. For the technical protection of personal data, the controller, the processor or the operator of the telecommunications or information technology equipment shall implement security measures in particular if the processing involves the transmission of data over a network or any other means of information technology.

The Rights of Data Subjects and their Enforcement

Section 11.

(1) Any data subject may request

a) confirmation as to whether or not data relating to him are being processed (Sections 12 and 13), and

b) the rectification or erasure of his personal data, with the exception of those processed by order of legal regulation (Sections 14-16).

(2) The register of processing operations [Subsection (1) of Section 28] may be inspected (including the taking of notes) by any person. An extract of the data contained therein may be requested upon payment of a fee.

Section 12.

(1) Upon the data subject's request the data manager must provide information concerning the data relating to him, including those processed by a data processor on its behalf, the purpose, grounds and duration of processing, the name and address (corporate address) of the data processor and on its activities relating to data management, and the recipients of his data and the purpose for which they are or had been transferred. The duration for which records must be kept on the data transferred, and in consequence the obligation of information may be limited by legal regulation on data processing. The period of restriction shall not be less than five years in respect of personal data, and twenty years in respect of special data.

(2) Data processor must comply with requests for information without any delay, and provide the information requested in an intelligible form within no more than 30 days.

(3) The information specified in Subsection (2) shall be provided free of charge for any category of data once a year. Additional information concerning the same category of data may be subject to a charge. Where any payment is made in connection with data that was processed unlawfully, or the request led to rectification, it shall be refunded.

Section 13.

(1) A data processor may refuse to provide information to the data subject where it is permitted by law in the cases defined under Section 16.

(2) The data processor must notify the data subject of the reasons for refusal.

(3) Data processors shall notify the data protection commissioner once a year on refused requests.

Section 14.

(1) Data processors must correct the data if it is false.

(2) Personal data must be erased if

a) processed unlawfully;

b) so requested by the data subject in accordance with Paragraph b) of Subsection (1) of Section 11;

c) it is deficient or inaccurate and it cannot be legitimately corrected, provided that deletion is not disallowed by statutory provision;

d) the purpose of processing no longer exists or the legal time limit for storage has expired;

e) so instructed by court order or by the data protection commissioner.

(3) With the exception of illicit data processing, the requirement of erasure shall not apply to the personal data recorded on a medium that is to be deposited in archive under the legal regulation on archive materials.

Section 15.

When a data is corrected or erased, the data subject to whom it pertains and all recipients to whom it was transferred for processing must be notified. This notification shall not be required if it does not violate the rightful interest of the data subject in view of the purpose of processing.

Section 16.

The rights of data subjects (Sections 11-15) may be restricted by this Act in order to safeguard the external and internal security of the State (e.g., defense, national security, the prevention, investigation, detection and prosecution of criminal offences), protect the economic and financial interests of central and local government, safeguard the important economic and financial interests of the European Union, guard against disciplinary and ethical breaches in the regulated professions, prevent and detect breaches of obligation related to labor law and job safety - including in all cases control and supervision - and to protect data subjects or the rights and freedoms of others.

The Data Subject's Right to Object

Section 16/A.

(1) The data subject shall have the right to object to the processing of data relating to him

a) if processing (disclosure) is carried out solely for the purpose of enforcing the rights and legitimate interests of the controller or the recipient, unless processing is prescribed by law;

b) if personal data is used or transferred for the purposes of direct marketing, public opinion polling or scientific research;

c) if the right to object is ensured by law.

(2) In the event of objection, the controller shall discontinue processing operations and investigate the cause of objection within the shortest possible time, not to exceed 15 days, and shall notify the data subject in writing of the findings of the investigation. If the objection is justified, the controller shall terminate all processing operations (including data collection and transmission), block the data involved and notify all recipients to whom any of these data had been previously transferred concerning the objection and the ensuing measures; these recipients shall also take measures regarding the objection.

(3) If the data subject disagrees with the decision taken by the controller under Subsection (2), the data subject shall have the right under this Act to seek legal remedy within 30 days of the date the decision was conveyed.

(4) If data that are necessary to assert the data recipient's lawful rights are withheld owing to the data subject's objection, the data recipient shall have the right under this Act to file charges against the controller within 15 days from the date the decision is conveyed under Subsection (2) in order to obtain the data. The controller may implicate the data subject in such lawsuit.

(5) If the court rejects the petition filed by the data recipient, the controller shall be required to delete the data subject's personal data within three days of the court ruling. The controller shall delete the data even if the data recipient does not file for court action within the time limit referred to in Subsection (4).

(6) The controller shall not delete the data of the data subject if processing has been prescribed by law. However, data may not be disclosed to the data recipient if the controller agrees with the objection or if the court has found the objection justified.

Judicial Remedy

Section 17.

(1) The data subject and the person referred to in Subsection (4) of Section 16/A may file for court action against the controller for any violation of their rights. The court shall hear such cases immediately.

(2) The burden of proof of compliance with the law lies with the data processor.

(3) Such lawsuits are heard by the court in whose jurisdiction the controller's registered address (residence) is located or, if so requested by the data subject, by the court in whose jurisdiction the data subject's residence (place of abode) is located. Even persons lacking legal capacity to sue may be a party in such lawsuits.

(4) When the decision is in favor of the plaintiff, the court shall order the controller to provide the information, to correct or delete the data in question, to void the automated individual decision, to honor the data subject's objection, or to disclose the data requested by the person referred to in Subsection (4) of Section 16/A.

(5) The court may also order publication of its decision, by way of publishing the identification data of the controller, if it is necessitated for data protection in general or in connection with the rights of large numbers of data subjects under protection by this Act.

Liability

Section 18.

(1) Data managers shall be liable for any damage caused to a data subject as a result of unlawful processing or by breaching the technical requirements of data protection. The data manager shall also be liable for any damage caused by a data processor acting on its behalf. The data manager may be exempted from liability if he proves that the damage was caused by reasons beyond his control.

(2) No compensation shall be paid where the damage was caused by intentional or negligent conduct on the part of the data subject.

Chapter III

ACCESS TO INFORMATION OF PUBLIC INTEREST

Section 19.

(1) State or local public authorities and agencies and other bodies attending to the public duties specified by law (hereinafter jointly referred to as "agency') shall provide the general public with accurate and speedy information concerning the matters under their competence, such as the budgets of the central government and local governments and the implementation thereof, the management of assets controlled by the central government and by local governments, the appropriation of public funds, and special and exclusive rights conferred upon market actors, private organizations or individuals.

(2) The agencies referred to in Subsection (1) shall regularly publish or otherwise make available all information of import concerning their competence, jurisdiction, organizational structure, professional activities, the evaluation of such activities (including their effectiveness), the categories of data they process, the legal regulations that pertain to their operations, and their financial management. The names and positions of persons acting in the name and on behalf of the above-specified agencies shall be treated as public information, unless otherwise prescribed by law. The manner of disclosure and the data to be disclosed may be prescribed by legal regulation.

(3) The agencies defined in Subsection (1) shall allow free access to the public information they have on files to any person, excluding those labelled state or service secret by an agency vested with proper authorization, or if classified by virtue of commitment under treaty or convention, or if access to specific information of public interest is restricted by law in connection with

a) defense;

b) national security;

c) prevention, investigation, detection and prosecution of criminal offences;

d) central financial or foreign exchange policy;

e) external relations, relations with international organizations;

f) court proceeding.

(4) The personal data of a person acting in the name and on behalf of the agencies specified in Subsection (1), to the extent that it relates to his duties, shall not restrict access to specific information of public interest.

(5) 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.

(6) Access to business secrets in connection with access to and publication of information of public interest shall be governed by the relevant provisions of the Civil Code.

(7) The availability of public information may also be limited by European Union legislation with a view to any important economic or financial interests of the European Union, including monetary, budgetary and tax policies.

Section 20.

(1) The agencies processing information of public interest must comply with requests for information without any delay, and shall provide it in an intelligible form within no more than 15 days. The applicant may also request for a fee, a copy of the document or part of a document containing the data in question, regardless of the form of storage.

(2) When a request for information is refused, the applicant must be notified within 8 days in writing and must be given the reasons for refusal.

(3) The head of agency processing information of public interest may charge a fee for any supply of information, not exceeding the costs of service. If requested by the applicant, the amount of charges must be specified in advance.

(4) The agencies specified in Subsection (1) of Section 19 shall notify the data protection commissioner once a year on refused requests, including the reasons of refusal.

Section 21.

(1) When a person's request for public information is refused, he may file for court action.

(2) The burden of proof of compliance with the law lies with the data processor agency.

(3) The lawsuit shall be initiated within 30 days from the date of refusal against the agency that has refused the information.

(4) Any person who cannot sue or be sued may also be involved in such lawsuits.

(5) Lawsuits against agencies of nationwide jurisdiction shall be filed at the competent county (Budapest) court. Lawsuits against local agencies shall be filed at the central county court, or at the Central Pest District Court in Budapest. The competency of the court is determined based on the location of the agency that refused to provide information.

(6) The court shall hear such cases under priority.

(7) When the decision is in favor of the plaintiff, the court shall order the data processor agency to provide the information.

Section 22.

This Chapter shall not apply to the supply of information from official records that is subject to the provisions of specific other legislation.

Chapter IV

DATA PROTECTION COMMISSIONER, REGISTER OF PROCESSING OPERATIONS

Data Protection Commissioner

Section 23.

(1) To protect the rights and freedoms afforded by the Constitution for the protection of personal data and access to information of public interest, the Parliament shall appoint a data protection commissioner from candidates of high repute satisfying the following criteria: must be a Hungarian citizen holding a diploma, have no prior criminal record, must have outstanding theoretical knowledge or 10 years of professional experience in the field of data protection, including all phases of administration and control.

(2) The provisions of the Act on the Ombudsman of Civil Rights shall apply to the data protection commissioner with the exceptions set forth in this Act.

Section 24.

The data protection commissioner

a) shall oversee compliance with the regulations of this Act and other legislation related to data protection;

b) shall investigate the reports he receives;

c) shall provide for the register of processing operations.

d) shall facilitate the uniform enforcement of the statutory provisions on the processing of personal data and on the availability of public information;

e) shall exercise and perform the tasks and duties conferred under this Act.

Section 25.

(1) The data protection commissioner shall monitor compliance with the requirements for the protection of personal data and for free access to information of public interest. He/she shall have authority to make recommendations for new regulations and for the amendment of legislation pertaining to data processing and information of public interest, and shall express his opinion on bills covering the same subject. As to the scope of data to be treated as state or service secrets, the data protection commissioner shall have authority to recommend specific data to be removed or added.

(2) Upon noticing any unlawful data processing operation, the data protection commissioner shall advise the data processor to cease such operation. The data processor must comply within 30 days and shall report to the data protection commissioner in writing concerning the measures taken.

(3) If the controller or processor fails to comply and cease the above-specified unlawful data processing operation, the data protection commissioner may order that unlawfully processed data be blocked, deleted or destroyed, or the data protection commissioner may prohibit the unauthorized data management and/or processing operations and suspend any operation aimed at transferring data abroad. The data protection commissioner shall announce these illegitimate data management and/or processing operations to the public and identify the controller (processor) and the measures proposed by it.

(4) The controller, the processor or the data subject may seek judicial remedy against the data protection commissioner's actions. The data involved in such litigated data processing operations may not be deleted or destroyed until the court has made a definitive ruling; however, processing operations must be discontinued and data must be blocked.

Section 26.

(1) The data protection commissioner in his official capacity shall have powers to request information from data processors and to inspect any document and processing operations that may involve personal data or information of public interest.

(2) The data protection commissioner shall be authorized to enter any premises where data processing takes place.

(3) The data protection commissioner shall also have access to state and service secrets in connection with his official duties defined in this Section, however, the rules of confidentiality must be observed by the data protection commissioner as well. The data protection commissioner must act in person when investigating any case of data processing that involves state or service secrets, or may have members of his staff acting on his behalf, if they have volunteered and have been checked for national security reasons.

(4) When the data protection commissioner concludes in his official capacity that any restricted-access data has been classified without proper justification, other than those classified by virtue of treaty or convention, the commissioner shall instruct the person by whom it was classified to lift or revise the restriction. The classifying person may contest such instruction within 30 days at the Municipal Court of Budapest where it will be heard in a closed session under priority.

Section 27.

(1) In the case of any violation of the rights of a person in connection with his personal data or free access to public information, or if there is imminent danger of such violation, it shall be reported to the data protection commissioner, unless a court action is already pending concerning the case in question.

(2) The person making a report to the data protection commissioner must not suffer any detriment for making such report. Any person filing such report shall be entitled to the same protection afforded to persons filing reports in the public interest.

Register of Processing Operations

Section 28.

(1) Prior to commencing operations, data processors must notify for the purpose of registration the data protection commissioner of the following:

a) the purpose of processing;

b) the category of data and the grounds for processing;

c) the data subjects involved;

d) the source;

e) the categories of data transferred, the recipients and the grounds for transfer;

f) the deadline of erasure of specific categories;

g) name and address (corporate address) of the data manager and the data processor, the place where records are kept and/or where processing is carried out, and the data processor's activities in connection with data management operations.

h) the name of and contact information for the internal data protection officer.

(2) When the processing of certain data is prescribed by legal regulation, it shall be announced by the competent minister, the director of the agency of national jurisdiction, or by the mayor or the person presiding over the county assembly concerned within 15 days from the date when the legal regulation in question enters into force.

(3) National security agencies shall announce the purpose and the grounds for data processing.

Section 29.

(1) Upon registration, each data processor shall be issued a registration number. This registration number shall be used for all operations with data, such as when data is transferred or published, or when provided to the data subject.

(2) Any changes in the data specified Subsection (1) of Section 28 shall be reported to the data protection commissioner within 8 days, and the records shall be revised accordingly.

Section 30.

Data processing shall not be notified to the register of processing operations

a) when it concerns the data of the data processor's employees, members, students or customers;

b) when carried out in accordance with the internal rules of the church or other religious organization;

c) if it concerns the personal data of a person undergoing medical treatment, for the purposes of health care and preventive measures or for settling claims for benefits and services in the social insurance system;

d) where it contains information concerning the provision of social and other benefits to the data subject;

e) where it contains the personal data of persons implicated in an official regulatory, public prosecutor or court proceeding to the extent required for such proceeding;

f) if it contains personal data for official statistical purposes, provided there are adequate guarantees that the data is rendered anonymous in such a way that the data subject is no longer identifiable;

g) where it contains data of organizations and bodies falling under the scope of the Media Act, if they are used solely for their own information;

h) if it serves the purposes of scientific research, and if the data are not made available to the public;

i) if the data is transferred to a public archive;

j) if it serves the own purposes of a natural person.

Preliminary Inspection

Section 31.

(1) The data protection commissioner shall have powers to conduct preliminary inspections prior to registration.

(2) Prior to the processing of any new data files or the use of new data processing technologies, the data protection commissioner may conduct preliminary inspections at controllers processing the following data:

a) data files concerning authorities of nationwide jurisdiction, data files concerning employment and criminal records;

b) data files from the customer records of financial institutions and public utility companies;

c) data files from the customer records of telecommunications service providers;

d) data files containing the individual statistical data defined in specific other legislation.

(3) Controllers shall be required to notify the data protection commissioner 30 days prior to the commencement of the processing of any new data files or the use of new data processing technologies. The data protection

commissioner shall notify a controller of his intention to conduct a preliminary inspection within eight days of receiving the above-specified notification and shall carry out the inspection within 30 days. Processing operations may commence only upon completion of the inspection conducted by the data protection commissioner.

(4) On the basis of the findings of the inspection, the data protection commissioner may prohibit the processing of specific data or may instruct the controller to change the processing technology. If the data protection commissioner disagrees with the legal regulation prescribing data processing, he may submit a proposal to amend the legal regulation in question.

Internal Data Protection Officer, Data Protection Regulations

Section 31/A.

(1) The following controllers and processors shall appoint or commission an internal data protection officer - who shall hold a law degree, a degree in economics or computer sciences or an equivalent degree in higher education - who is to report directly to the head of the organization:

a) authorities of nationwide jurisdiction, and controllers and processors engaged in processing data files of employment and criminal records;

b) financial institutions;

c) telecommunications service providers and public utility companies.

(2) The internal data protection officer shall:

a) participate and assist in the decision-making process with regard to data processing and in enforcing the rights of data subjects;

b) monitor compliance with the provisions of this Act and other legal regulations on data processing as well as with the provisions of internal data protection and data security regulations and the data security requirements;

c) investigate complaints conveyed to him and, if he detects any unauthorized data processing operations, request the controller or processor in question to cease such operations;

d) prepare the internal data protection and data security regulations;

e) maintain the internal data protection register;

f) arrange training sessions on the subject of data protection.

(3) The controllers referred to in Subsection (1) and central and local government controllers - other than controllers not required to report to the data protection register - shall be required to adopt data protection and data security regulations in accordance with this Act.

Chapter V

SPECIAL PROVISIONS

Processing and Use of Personal Data by Research Institutions

Section 32.

(1) Personal data collected and stored for scientific reasons must be used only for scientific research projects.

(2) Any personal data that no longer serves research purposes must be rendered anonymous. Any data relating to an identified or identifiable natural person must be stored separately. Such data may be related to other data if it is necessary for the purposes of research.

(3) An agency or person performing scientific research shall be allowed to publish personal data only if

a) the data subject has given his consent, or

b) it is necessary to demonstrate the findings of research in connection with historical events.

Use of Personal Data for Statistical Purposes

Section 32/A.

(1) Personal data recorded, received or processed for statistical purposes may only be used for statistical purposes. The individual statistical data defined in specific other legislation, including personal data, may not be transferred, received or processed in any way or form or under any circumstances, and they may not be published.

(2) The detailed regulations governing processing operations involving personal data are contained in another act.

Chapter VI

CLOSING PROVISIONS

Amendments

Section 33.

The following provision shall replace Subsection (1) of Section 83 of Act IV of 1959 on the Civil Code of the Republic of Hungary:

(1) Data management and data processing by computer or other means may not violate inherent rights."

Entry into Force

Section 34.

(1) This Act, with the exceptions set forth in Subsections (2) and (3), shall enter into force on the first day of the sixth mouth following its promulgation.

(2) Chapter III (Sections 19-22) of this Act shall enter into force on the 15th day following promulgation.

(3) Chapter IV (Sections 23-31) of this Act shall enter into force simultaneously with the Act on the Ombudsman for Civil Rights.

Section 35.

(1) Where this Act prescribes legislation in the form of an act, it shall be drafted by 31 December 1992, with the exception of Subsection (3), Section 4, and Subsection (1) of Section 13.

(2) Legal directives in connection with data processing cannot be used after the promulgation of this Act.

Section 36.

(1)

(2) Data processors shall notify all processing operations already existing at the time of this Act entering into force within three months from the appointment of the data protection commissioner for registration in the register of processing operations.

Section 37.

The Minister of Finance is hereby authorized to decree the amount of fees payable under Subsection (2) of Section 11 and the detailed regulations for the administration of such fees.

Act LXIII of 1992

on the Protection of Personal Data and the Disclosure of Information of Public Interest

Having regard to the protection of personal data and to access to information of public interest, the Parliament has adopted the following Act in accordance with the Constitution of the Republic of Hungary:

Chapter I

GENERAL PROVISIONS

Purpose of this Act

Section 1.

(1) The purpose of this Act is to ensure the right to privacy regarding personal data and free access to information of public interest, notwithstanding any exemptions provided by legal regulation specified in this Act.

(2) No derogation from the provisions of this Act shall be permitted, unless it is expressly provided for in this Act.

(3) Any exemption granted in this Act must apply to specific data and specific data manager together.

Scope

Section 1/A.

(1) This Act shall apply to all data management and data processing operations performed in the territory of the Republic of Hungary that pertain to the data of natural persons or to public information or information of public interest.

(2) This Act shall apply to data management and data processing operations whether performed in full or in part by an automated process or by manual processing.

(3) This Act shall not apply where data is processed by a natural person exclusively for his own purposes.

Definitions

Section 2.

For the purposes of this Act:

1) 'personal data' shall mean any information relating to an identified or identifiable natural person (hereinafter referred to as "data subject') and any reference drawn, whether directly or indirectly, from such information. In the course of data processing, such information shall be treated as personal data as long as the data subject remains identifiable through it. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

2) 'special data' shall mean

a) personal data revealing racial, national or ethnic origin, political opinions and any affiliation with political parties, religious or philosophical beliefs, trade-union membership,

b) personal data concerning health, addictions, sex life, or criminal record;

3) 'personal data relating to criminal offenses' shall mean personal data that might be related to the data subject or that pertain to any prior criminal offense committed by the data subject and that is obtained by organizations authorized to conduct criminal proceedings or investigations or by penal institutions during or prior to criminal proceedings in connection with a crime or criminal proceedings;

4) 'public information' shall mean 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);

5) 'public information subject to disclosure' shall mean any data managed by or pertaining to a natural or legal person or an unincorporated organization, other than public information that is not subject to disclosure, that are prescribed by law to be published or disclosed for the benefit of the general public;

6) 'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed without limitation or with regard to specific operations;

7) 'the data subject's objection' shall mean an indication of his wishes by which the data subject objects to the processing of his data and requests that the processing of data relating to him be terminated and/or the processed data be deleted;

8) 'controller' shall mean a natural or legal person or unincorporated organization that determines the purpose of the processing of personal data, makes decisions regarding data management (including the means) and implements such decisions itself or engages a processor to implement them;

9) 'data management' shall mean any operation or set of operations that is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, deletion or destruction, and blocking them from further use. Photographing, sound and video recording, and the recording of physical attributes for identification purposes (such as fingerprints and palm prints, DNA samples and retinal images;

10) 'disclosure by transmission' shall mean making data available to a specific third party;

11) 'public disclosure' shall mean making data available to the general public;

12) 'deletion of data' shall mean the destruction or elimination of data sufficient to make them irretrievable;

13) 'blocking of data' shall mean preventing - permanently or for a predetermined period - the transmission, access to, disclosure, adaptation or alteration, destruction, deletion, alignment or combination, and the use of data;

14) 'destruction of data' shall mean the complete physical destruction of data or the medium containing the data;

15) 'data processing' shall mean the technical operations involved in data management, irrespective of the method and instruments employed for such operations and the venue where it takes place;

16) 'processor' shall mean a natural or legal person or unincorporated organization that is engaged in the processing of personal data on behalf of a controller - including when ordered by virtue of legal regulation;

17) 'personal data filing system' (filing system) shall mean any structured set of personal data that are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

18) 'set of data' shall mean all data contained in a filing system;

19) 'third person' shall mean any natural or legal person or unincorporated organization other than the data subject, the controller or the processor;

20) 'third country' shall mean any country that is not a member of the European Union.

Chapter II

PROTECTION OF PERSONAL DATA

Data Processing

Section 3.

(1) Personal data may be processed if

a) the data subject has given his consent, or

b) decreed by law or by a local authority based on authorization conferred by law concerning specific data defined therein.

(2) Special data may be processed if

a) the data subject has given his explicit consent in writing, or

b) prescribed by treaty concerning the personal data specified in Point 2. a) of Section 2, or if ordered by law in connection with the enforcement of some constitutional right or for national security or law enforcement purposes,

c) ordered by law in other cases.

(3) Where data management is mandatory, the purpose and the conditions of management, the type of data and access to such data, the duration of the proposed processing operation, and the controller shall be specified by the statute or local government decree in which it is ordered.

(4) Where it serves the interest of the public, free access to particular personal data may be ordered by law as defined therein. In all other cases, free access to personal data may be provided only upon the consent of the data subject that is to be made in writing with regard to special data. If there is any doubt, it is to be presumed that the data subject did not consent to allow free access.

(5) The consent of the data subject shall be considered granted in connection with any data he has conveyed to the public or has supplied for publication.

(6) In connection with any proceeding requested by the data subject, his consent for processing his data to the extent necessary shall be considered granted, of which the data subject must be advised.

(7) The data subject may grant consent in a written agreement concluded with the controller for the performance of the contract. In this case, the contract shall contain all information that is to be made available to the data subject under this Act in connection with the processing of personal data, such as the description of the data involved, the duration of the proposed processing operation, the purpose of processing, the transmission of data and the use of a processor. The contract must clearly indicate the data subject's signature and explicit consent for having his data processed as stipulated in the contract.

(8) If the data subject is physically or legally incapable of giving his consent for processing his personal data, the processing of his personal data - which includes his special data - is allowed to the extent necessary to protect the vital interests of the data subject or of another person or in order to prevent or avert a catastrophe or emergency.

Section 4.

The right for the protection of personal data and the fundamental right to privacy of individuals must not be breached by any other interest, including free access to information of public interest (Section 19) for data processing, unless an exemption is granted by law.

Data Processing

Section 4/A.

(1) The rights and obligations of data processors arising in connection with the processing of personal data shall be determined by the data manager within the scope specified by the this Act and other legislation on data management. The data manager shall be held liable for the legitimacy of instructions pertaining to data management operations.

(2) The data processor shall be held liable within his sphere of competence and within the scope specified by the data manager for the processing, alteration, erasure and disclosure by transmission of personal data. The data processor shall not be permitted to subcontract any part of his operations to another data processor.

(3) A processor may not make any decision on the merits of data management and shall process any and all data entrusted to him solely as instructed by the controller; the processor shall not engage in data processing for his own purposes and shall store and safeguard personal data according to the instructions of the controller.

(4) Contracts for the processing of data must be made in writing. Any company that is interested in the business activity for which personal data is used may not be contracted for the processing of such data.

(5) Contracts for the processing of data to be concluded with third-country processors shall be drafted in compliance with the Decision of the Commission of the European Communities, which has been published by the data protection commissioner in *Magyar Közlöny* [Official Hungarian Gazette].

(6) This Act shall apply if a third-country controller that is involved in the processing of personal data employs a processor whose registered address or place of business (branch) or habitual residence (place of abode) is situated in the territory of the Republic of Hungary or if it makes use of equipment situated on the territory of the Republic of Hungary, unless such equipment is used solely for the purpose of transit through the territory of the European Union. Such controllers shall have a representative installed in the territory of the Republic of Hungary.

Legitimacy of Data Processing

Section 5.

(1) Personal data may be processed only for specified and explicit purposes, where it is necessary for carrying out certain rights or obligations. This purpose must be satisfied in all stages of operations of data processing.

(2) 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.

(3) The processing of data prescribed to be disclosed may be ordered in the public interest.

(4) Personal data may - with the data subject's consent or by virtue of legal regulation - be processed for the performance of a task carried out in the public interest or in the exercise of official authority, in the fulfillment of the official tasks of the controller or the recipient third party, for the protection of the data subject's vital interest, for the performance of a contract between the data subject and the controller, in the legitimate interests of the controller or a third party, or in the legitimate operation of a charitable organization.

(5) Personal data that concern criminal offenses and are being processed for the purposes of preventing, investigating, detecting and prosecuting criminal offences and data files containing information pertaining to

misdemeanor cases, civil lawsuits and non-litigious cases may only be processed by central or local government authorities.

Section 6.

(1) Prior to the collection of data the data subject shall be informed whether disclosure is voluntary or compulsory. If compulsory, the legal regulation on which it is based shall also be indicated.

(2) The data subject shall be clearly and elaborately informed of all aspects concerning the processing of his personal data, such as the purpose for which his data is required and the legal grounds, the person entitled to carry out the processing, the duration of the proposed processing operation and the persons to whom his data may be disclosed. Information shall also be provided on the data subject's rights and remedies.

(3) Notification of data management is considered granted where disclosure by transmission from existing data processing operations or by alignment or combination for further processing is prescribed by legal regulation.

(4) If individual notification is impossible or likely to result in unreasonable expense, notification of data management - particularly if it is for statistical or scientific purposes (including historical research) - may occur by way of publishing the fact of data collection, the data subjects involved, the purpose and duration of the proposed processing operation and the availability of data.

Data Quality

Section 7.

(1) Personal data collected for processing must be

a) processed fairly and lawfully;

b) accurate, complete and, where necessary, kept up to date;

c) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected.

(2) The use of personal identification codes or any other identifier of general application shall not be permitted.

Transfer of Data, Set of Transfer Operations

Section 8.

(1) Data may be transferred, whether in a single or in a set of operations, if the data subject has given his consent or if the transfer is legally permitted, and if the safeguards for data processing are satisfied with regard to each and every personal data.

(2) Subsection (1) shall also apply where data is structured between various filing systems of the same processor, or between those of government and local authorities.

Transfer of Data to Foreign Countries

Section 9.

(1) Personal data (including special data) may be transferred - irrespective of the medium and the manner in which it is transferred - to a third-country controller or processor if the data subject has given his consent, if the transfer is permitted by law or if it is prescribed by treaty or international convention, provided the laws of the third country in question afford an adequate level of protection within the meaning of Community standards with respect to the processing of the data transferred.

(2) Transmission of data to Member States of the European Union shall be treated as transmission within the territory of the Republic of Hungary.

Automated Individual Decisions

Section 9/A.

(1) Evaluation of certain personal aspects of any person by automated (computerized) processing of data may only be carried out if the data subject explicitly gives his consent or if such evaluation is permitted by law. The data subject must be given the opportunity to express his opinion.

(2) Where personal data is processed by automated means, the data subject must, at his request, be informed of the mathematical method that is used and its essence.

Security of Processing

Section 10.

(1) Data managers, and within their sphere of competence, data processors must implement adequate safeguards and appropriate technical and organizational measures to protect personal data, as well as adequate procedural rules to enforce the provisions of this Act and other regulations concerning confidentiality and security of data processing.

(2) Data must be protected against unauthorized access, alteration, transfer, disclosure by transmission or deletion as well as damage and accidental destruction. For the technical protection of personal data, the controller, the processor or the operator of the telecommunications or information technology equipment shall implement security measures in particular if the processing involves the transmission of data over a network or any other means of information technology.

The Rights of Data Subjects and their Enforcement

Section 11.

(1) Any data subject may request

a) confirmation as to whether or not data relating to him are being processed (Sections 12 and 13), and

b) the rectification or erasure of his personal data, with the exception of those processed by order of legal regulation (Sections 14-16).

(2) The register of processing operations [Subsection (1) of Section 28] may be inspected (including the taking of notes) by any person. An extract of the data contained therein may be requested upon payment of a fee.

Section 12.

(1) Upon the data subject's request the data manager must provide information concerning the data relating to him, including those processed by a data processor on its behalf, the purpose, grounds and duration of processing, the name and address (corporate address) of the data processor and on its activities relating to data management, and the recipients of his data and the purpose for which they are or had been transferred. The duration for which records must be kept on the data transferred, and in consequence the obligation of information may be limited by legal regulation on data processing. The period of restriction shall not be less than five years in respect of personal data, and twenty years in respect of special data.

(2) Data processor must comply with requests for information without any delay, and provide the information requested in an intelligible form within no more than 30 days.

(3) The information specified in Subsection (2) shall be provided free of charge for any category of data once a year. Additional information concerning the same category of data may be subject to a charge. Where any payment is made in connection with data that was processed unlawfully, or the request led to rectification, it shall be refunded.

Section 13.

(1) A data processor may refuse to provide information to the data subject where it is permitted by law in the cases defined under Section 16.

(2) The data processor must notify the data subject of the reasons for refusal.

(3) Data processors shall notify the data protection commissioner once a year on refused requests.

Section 14.

(1) Data processors must correct the data if it is false.

(2) Personal data must be erased if

a) processed unlawfully;

b) so requested by the data subject in accordance with Paragraph b) of Subsection (1) of Section 11;

c) it is deficient or inaccurate and it cannot be legitimately corrected, provided that deletion is not disallowed by statutory provision;

d) the purpose of processing no longer exists or the legal time limit for storage has expired;

e) so instructed by court order or by the data protection commissioner.

(3) With the exception of illicit data processing, the requirement of erasure shall not apply to the personal data recorded on a medium that is to be deposited in archive under the legal regulation on archive materials.

Section 15.

When a data is corrected or erased, the data subject to whom it pertains and all recipients to whom it was transferred for processing must be notified. This notification shall not be required if it does not violate the rightful interest of the data subject in view of the purpose of processing.

Section 16.

The rights of data subjects (Sections 11-15) may be restricted by this Act in order to safeguard the external and internal security of the State (e.g., defense, national security, the prevention, investigation, detection and prosecution of criminal offences), protect the economic and financial interests of central and local government, safeguard the important economic and financial interests of the European Union, guard against disciplinary and ethical breaches in the regulated professions, prevent and detect breaches of obligation related to labor law and job safety - including in all cases control and supervision - and to protect data subjects or the rights and freedoms of others.

The Data Subject's Right to Object

Section 16/A.

(1) The data subject shall have the right to object to the processing of data relating to him

a) if processing (disclosure) is carried out solely for the purpose of enforcing the rights and legitimate interests of the controller or the recipient, unless processing is prescribed by law;

b) if personal data is used or transferred for the purposes of direct marketing, public opinion polling or scientific research;

c) if the right to object is ensured by law.

(2) In the event of objection, the controller shall discontinue processing operations and investigate the cause of objection within the shortest possible time, not to exceed 15 days, and shall notify the data subject in writing of the findings of the investigation. If the objection is justified, the controller shall terminate all processing operations (including data collection and transmission), block the data involved and notify all recipients to whom any of these data had been previously transferred concerning the objection and the ensuing measures; these recipients shall also take measures regarding the objection.

(3) If the data subject disagrees with the decision taken by the controller under Subsection (2), the data subject shall have the right under this Act to seek legal remedy within 30 days of the date the decision was conveyed.

(4) If data that are necessary to assert the data recipient's lawful rights are withheld owing to the data subject's objection, the data recipient shall have the right under this Act to file charges against the controller within 15 days from the date the decision is conveyed under Subsection (2) in order to obtain the data. The controller may implicate the data subject in such lawsuit.

(5) If the court rejects the petition filed by the data recipient, the controller shall be required to delete the data subject's personal data within three days of the court ruling. The controller shall delete the data even if the data recipient does not file for court action within the time limit referred to in Subsection (4).

(6) The controller shall not delete the data of the data subject if processing has been prescribed by law. However, data may not be disclosed to the data recipient if the controller agrees with the objection or if the court has found the objection justified.

Judicial Remedy

Section 17.

(1) The data subject and the person referred to in Subsection (4) of Section 16/A may file for court action against the controller for any violation of their rights. The court shall hear such cases immediately.

(2) The burden of proof of compliance with the law lies with the data processor.

(3) Such lawsuits are heard by the court in whose jurisdiction the controller's registered address (residence) is located or, if so requested by the data subject, by the court in whose jurisdiction the data subject's residence (place of abode) is located. Even persons lacking legal capacity to sue may be a party in such lawsuits.

(4) When the decision is in favor of the plaintiff, the court shall order the controller to provide the information, to correct or delete the data in question, to void the automated individual decision, to honor the data subject's objection, or to disclose the data requested by the person referred to in Subsection (4) of Section 16/A.

(5) The court may also order publication of its decision, by way of publishing the identification data of the controller, if it is necessitated for data protection in general or in connection with the rights of large numbers of data subjects under protection by this Act.

Liability

Section 18.

(1) Data managers shall be liable for any damage caused to a data subject as a result of unlawful processing or by breaching the technical requirements of data protection. The data manager shall also be liable for any damage caused by a data processor acting on its behalf. The data manager may be exempted from liability if he proves that the damage was caused by reasons beyond his control.

(2) No compensation shall be paid where the damage was caused by intentional or negligent conduct on the part of the data subject.

Chapter III

ACCESS TO INFORMATION OF PUBLIC INTEREST

Section 19.

(1) State or local public authorities and agencies and other bodies attending to the public duties specified by law (hereinafter jointly referred to as "agency') shall provide the general public with accurate and speedy information concerning the matters under their competence, such as the budgets of the central government and local governments and the implementation thereof, the management of assets controlled by the central government and by local governments, the appropriation of public funds, and special and exclusive rights conferred upon market actors, private organizations or individuals.

(2) The agencies referred to in Subsection (1) shall regularly publish or otherwise make available all information of import concerning their competence, jurisdiction, organizational structure, professional activities, the evaluation of such activities (including their effectiveness), the categories of data they process, the legal regulations that pertain to their operations, and their financial management. The names and positions of persons acting in the name and on behalf of the above-specified agencies shall be treated as public information, unless otherwise prescribed by law. The manner of disclosure and the data to be disclosed may be prescribed by legal regulation.

(3) The agencies defined in Subsection (1) shall allow free access to the public information they have on files to any person, excluding those labelled state or service secret by an agency vested with proper authorization, or if classified by virtue of commitment under treaty or convention, or if access to specific information of public interest is restricted by law in connection with

a) defense;

b) national security;

c) prevention, investigation, detection and prosecution of criminal offences;

d) central financial or foreign exchange policy;

e) external relations, relations with international organizations;

f) court proceeding.

(4) The personal data of a person acting in the name and on behalf of the agencies specified in Subsection (1), to the extent that it relates to his duties, shall not restrict access to specific information of public interest.

(5) 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.

(6) Access to business secrets in connection with access to and publication of information of public interest shall be governed by the relevant provisions of the Civil Code.

(7) The availability of public information may also be limited by European Union legislation with a view to any important economic or financial interests of the European Union, including monetary, budgetary and tax policies.

Section 20.

(1) The agencies processing information of public interest must comply with requests for information without any delay, and shall provide it in an intelligible form within no more than 15 days. The applicant may also request for a fee, a copy of the document or part of a document containing the data in question, regardless of the form of storage.

(2) When a request for information is refused, the applicant must be notified within 8 days in writing and must be given the reasons for refusal.

(3) The head of agency processing information of public interest may charge a fee for any supply of information, not exceeding the costs of service. If requested by the applicant, the amount of charges must be specified in advance.

(4) The agencies specified in Subsection (1) of Section 19 shall notify the data protection commissioner once a year on refused requests, including the reasons of refusal.

Section 21.

(1) When a person's request for public information is refused, he may file for court action.

(2) The burden of proof of compliance with the law lies with the data processor agency.

(3) The lawsuit shall be initiated within 30 days from the date of refusal against the agency that has refused the information.

(4) Any person who cannot sue or be sued may also be involved in such lawsuits.

(5) Lawsuits against agencies of nationwide jurisdiction shall be filed at the competent county (Budapest) court. Lawsuits against local agencies shall be filed at the central county court, or at the Central Pest District Court in Budapest. The competency of the court is determined based on the location of the agency that refused to provide information.

(6) The court shall hear such cases under priority.

(7) When the decision is in favor of the plaintiff, the court shall order the data processor agency to provide the information.

Section 22.

This Chapter shall not apply to the supply of information from official records that is subject to the provisions of specific other legislation.

Chapter IV

DATA PROTECTION COMMISSIONER, REGISTER OF PROCESSING OPERATIONS

Data Protection Commissioner

Section 23.

(1) To protect the rights and freedoms afforded by the Constitution for the protection of personal data and access to information of public interest, the Parliament shall appoint a data protection commissioner from candidates of high repute satisfying the following criteria: must be a Hungarian citizen holding a diploma, have no prior criminal record, must have outstanding theoretical knowledge or 10 years of professional experience in the field of data protection, including all phases of administration and control.

(2) The provisions of the Act on the Ombudsman of Civil Rights shall apply to the data protection commissioner with the exceptions set forth in this Act.

Section 24.

The data protection commissioner

a) shall oversee compliance with the regulations of this Act and other legislation related to data protection;

b) shall investigate the reports he receives;

c) shall provide for the register of processing operations.

d) shall facilitate the uniform enforcement of the statutory provisions on the processing of personal data and on the availability of public information;

e) shall exercise and perform the tasks and duties conferred under this Act.

Section 25.

(1) The data protection commissioner shall monitor compliance with the requirements for the protection of personal data and for free access to information of public interest. He/she shall have authority to make recommendations for new regulations and for the amendment of legislation pertaining to data processing and information of public interest, and shall express his opinion on bills covering the same subject. As to the scope of data to be treated as state or service secrets, the data protection commissioner shall have authority to recommend specific data to be removed or added.

(2) Upon noticing any unlawful data processing operation, the data protection commissioner shall advise the data processor to cease such operation. The data processor must comply within 30 days and shall report to the data protection commissioner in writing concerning the measures taken.

(3) If the controller or processor fails to comply and cease the above-specified unlawful data processing operation, the data protection commissioner may order that unlawfully processed data be blocked, deleted or destroyed, or the data protection commissioner may prohibit the unauthorized data management and/or processing operations and suspend any operation aimed at transferring data abroad. The data protection commissioner shall announce these illegitimate data management and/or processing operations to the public and identify the controller (processor) and the measures proposed by it.

(4) The controller, the processor or the data subject may seek judicial remedy against the data protection commissioner's actions. The data involved in such litigated data processing operations may not be deleted or destroyed until the court has made a definitive ruling; however, processing operations must be discontinued and data must be blocked.

Section 26.

(1) The data protection commissioner in his official capacity shall have powers to request information from data processors and to inspect any document and processing operations that may involve personal data or information of public interest.

(2) The data protection commissioner shall be authorized to enter any premises where data processing takes place.

(3) The data protection commissioner shall also have access to state and service secrets in connection with his official duties defined in this Section, however, the rules of confidentiality must be observed by the data protection commissioner as well. The data protection commissioner must act in person when investigating any case of data processing that involves state or service secrets, or may have members of his staff acting on his behalf, if they have volunteered and have been checked for national security reasons.

(4) When the data protection commissioner concludes in his official capacity that any restricted-access data has been classified without proper justification, other than those classified by virtue of treaty or convention, the commissioner shall instruct the person by whom it was classified to lift or revise the restriction. The classifying person may contest such instruction within 30 days at the Municipal Court of Budapest where it will be heard in a closed session under priority.

Section 27.

(1) In the case of any violation of the rights of a person in connection with his personal data or free access to public information, or if there is imminent danger of such violation, it shall be reported to the data protection commissioner, unless a court action is already pending concerning the case in question.

(2) The person making a report to the data protection commissioner must not suffer any detriment for making such report. Any person filing such report shall be entitled to the same protection afforded to persons filing reports in the public interest.

Register of Processing Operations

Section 28.

(1) Prior to commencing operations, data processors must notify for the purpose of registration the data protection commissioner of the following:

a) the purpose of processing;

b) the category of data and the grounds for processing;

c) the data subjects involved;

d) the source;

e) the categories of data transferred, the recipients and the grounds for transfer;

f) the deadline of erasure of specific categories;

g) name and address (corporate address) of the data manager and the data processor, the place where records are kept and/or where processing is carried out, and the data processor's activities in connection with data management operations.

h) the name of and contact information for the internal data protection officer.

(2) When the processing of certain data is prescribed by legal regulation, it shall be announced by the competent minister, the director of the agency of national jurisdiction, or by the mayor or the person presiding over the county assembly concerned within 15 days from the date when the legal regulation in question enters into force.

(3) National security agencies shall announce the purpose and the grounds for data processing.

Section 29.

(1) Upon registration, each data processor shall be issued a registration number. This registration number shall be used for all operations with data, such as when data is transferred or published, or when provided to the data subject.

(2) Any changes in the data specified Subsection (1) of Section 28 shall be reported to the data protection commissioner within 8 days, and the records shall be revised accordingly.

Section 30.

Data processing shall not be notified to the register of processing operations

a) when it concerns the data of the data processor's employees, members, students or customers;

b) when carried out in accordance with the internal rules of the church or other religious organization;

c) if it concerns the personal data of a person undergoing medical treatment, for the purposes of health care and preventive measures or for settling claims for benefits and services in the social insurance system;

d) where it contains information concerning the provision of social and other benefits to the data subject;

e) where it contains the personal data of persons implicated in an official regulatory, public prosecutor or court proceeding to the extent required for such proceeding;

f) if it contains personal data for official statistical purposes, provided there are adequate guarantees that the data is rendered anonymous in such a way that the data subject is no longer identifiable;

g) where it contains data of organizations and bodies falling under the scope of the Media Act, if they are used solely for their own information;

h) if it serves the purposes of scientific research, and if the data are not made available to the public;

i) if the data is transferred to a public archive;

j) if it serves the own purposes of a natural person.

Preliminary Inspection

Section 31.

(1) The data protection commissioner shall have powers to conduct preliminary inspections prior to registration.

(2) Prior to the processing of any new data files or the use of new data processing technologies, the data protection commissioner may conduct preliminary inspections at controllers processing the following data:

a) data files concerning authorities of nationwide jurisdiction, data files concerning employment and criminal records;

b) data files from the customer records of financial institutions and public utility companies;

c) data files from the customer records of telecommunications service providers;

d) data files containing the individual statistical data defined in specific other legislation.

(3) Controllers shall be required to notify the data protection commissioner 30 days prior to the commencement of the processing of any new data files or the use of new data processing technologies. The data protection commissioner shall notify a controller of his intention to conduct a preliminary inspection within eight days of

receiving the above-specified notification and shall carry out the inspection within 30 days. Processing operations may commence only upon completion of the inspection conducted by the data protection commissioner.

(4) On the basis of the findings of the inspection, the data protection commissioner may prohibit the processing of specific data or may instruct the controller to change the processing technology. If the data protection commissioner disagrees with the legal regulation prescribing data processing, he may submit a proposal to amend the legal regulation in question.

Internal Data Protection Officer, Data Protection Regulations

Section 31/A.

(1) The following controllers and processors shall appoint or commission an internal data protection officer - who shall hold a law degree, a degree in economics or computer sciences or an equivalent degree in higher education - who is to report directly to the head of the organization:

a) authorities of nationwide jurisdiction, and controllers and processors engaged in processing data files of employment and criminal records;

b) financial institutions;

c) telecommunications service providers and public utility companies.

(2) The internal data protection officer shall:

a) participate and assist in the decision-making process with regard to data processing and in enforcing the rights of data subjects;

b) monitor compliance with the provisions of this Act and other legal regulations on data processing as well as with the provisions of internal data protection and data security regulations and the data security requirements;

c) investigate complaints conveyed to him and, if he detects any unauthorized data processing operations, request the controller or processor in question to cease such operations;

d) prepare the internal data protection and data security regulations;

e) maintain the internal data protection register;

f) arrange training sessions on the subject of data protection.

(3) The controllers referred to in Subsection (1) and central and local government controllers - other than controllers not required to report to the data protection register - shall be required to adopt data protection and data security regulations in accordance with this Act.

Chapter V

SPECIAL PROVISIONS

Processing and Use of Personal Data by Research Institutions

Section 32.

(1) Personal data collected and stored for scientific reasons must be used only for scientific research projects.

(2) Any personal data that no longer serves research purposes must be rendered anonymous. Any data relating to an identified or identifiable natural person must be stored separately. Such data may be related to other data if it is necessary for the purposes of research.

(3) An agency or person performing scientific research shall be allowed to publish personal data only if

a) the data subject has given his consent, or

b) it is necessary to demonstrate the findings of research in connection with historical events.

Use of Personal Data for Statistical Purposes

Section 32/A.

(1) Personal data recorded, received or processed for statistical purposes may only be used for statistical purposes. The individual statistical data defined in specific other legislation, including personal data, may not be transferred, received or processed in any way or form or under any circumstances, and they may not be published.

(2) The detailed regulations governing processing operations involving personal data are contained in another act.

Chapter VI

CLOSING PROVISIONS

Amendments

Section 33.

The following provision shall replace Subsection (1) of Section 83 of Act IV of 1959 on the Civil Code of the Republic of Hungary:

(1) Data management and data processing by computer or other means may not violate inherent rights."

Entry into Force

Section 34.

(1) This Act, with the exceptions set forth in Subsections (2) and (3), shall enter into force on the first day of the sixth mouth following its promulgation.

(2) Chapter III (Sections 19-22) of this Act shall enter into force on the 15th day following promulgation.

(3) Chapter IV (Sections 23-31) of this Act shall enter into force simultaneously with the Act on the Ombudsman for Civil Rights.

Section 35.

(1) Where this Act prescribes legislation in the form of an act, it shall be drafted by 31 December 1992, with the exception of Subsection (3), Section 4, and Subsection (1) of Section 13.

(2) Legal directives in connection with data processing cannot be used after the promulgation of this Act.

Section 36.

(1)

(2) Data processors shall notify all processing operations already existing at the time of this Act entering into force within three months from the appointment of the data protection commissioner for registration in the register of processing operations.

Section 37.

The Minister of Finance is hereby authorized to decree the amount of fees payable under Subsection (2) of Section 11 and the detailed regulations for the administration of such fees.

Act LXIII of 1992

on the Protection of Personal Data and the Disclosure of Information of Public Interest

Having regard to the protection of personal data and to access to information of public interest, the Parliament has adopted the following Act in accordance with the Constitution of the Republic of Hungary:

Chapter I

GENERAL PROVISIONS

Purpose of this Act

Section 1.

(1) The purpose of this Act is to ensure the right to privacy regarding personal data and free access to information of public interest, notwithstanding any exemptions provided by legal regulation specified in this Act.

(2) No derogation from the provisions of this Act shall be permitted, unless it is expressly provided for in this Act.

(3) Any exemption granted in this Act must apply to specific data and specific data manager together.

Scope

Section 1/A.

(1) This Act shall apply to all data management and data processing operations performed in the territory of the Republic of Hungary that pertain to the data of natural persons or to public information or information of public interest.

(2) This Act shall apply to data management and data processing operations whether performed in full or in part by an automated process or by manual processing.

(3) This Act shall not apply where data is processed by a natural person exclusively for his own purposes.

Definitions

Section 2.

For the purposes of this Act:

1) 'personal data' shall mean any information relating to an identified or identifiable natural person (hereinafter referred to as "data subject') and any reference drawn, whether directly or indirectly, from such information. In the course of data processing, such information shall be treated as personal data as long as the data subject remains identifiable through it. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

2) 'special data' shall mean

a) personal data revealing racial, national or ethnic origin, political opinions and any affiliation with political parties, religious or philosophical beliefs, trade-union membership,

b) personal data concerning health, addictions, sex life, or criminal record;

3) 'personal data relating to criminal offenses' shall mean personal data that might be related to the data subject or that pertain to any prior criminal offense committed by the data subject and that is obtained by organizations authorized to conduct criminal proceedings or investigations or by penal institutions during or prior to criminal proceedings in connection with a crime or criminal proceedings;

4) 'public information' shall mean 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);

5) 'public information subject to disclosure' shall mean any data managed by or pertaining to a natural or legal person or an unincorporated organization, other than public information that is not subject to disclosure, that are prescribed by law to be published or disclosed for the benefit of the general public;

6) 'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed without limitation or with regard to specific operations;

7) 'the data subject's objection' shall mean an indication of his wishes by which the data subject objects to the processing of his data and requests that the processing of data relating to him be terminated and/or the processed data be deleted;

8) 'controller' shall mean a natural or legal person or unincorporated organization that determines the purpose of the processing of personal data, makes decisions regarding data management (including the means) and implements such decisions itself or engages a processor to implement them;

9) 'data management' shall mean any operation or set of operations that is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, deletion or destruction, and blocking them from further use. Photographing, sound and video recording, and the recording of physical attributes for identification purposes (such as fingerprints and palm prints, DNA samples and retinal images;

10) 'disclosure by transmission' shall mean making data available to a specific third party;

11) 'public disclosure' shall mean making data available to the general public;

12) 'deletion of data' shall mean the destruction or elimination of data sufficient to make them irretrievable;

13) 'blocking of data' shall mean preventing - permanently or for a predetermined period - the transmission, access to, disclosure, adaptation or alteration, destruction, deletion, alignment or combination, and the use of data;

14) 'destruction of data' shall mean the complete physical destruction of data or the medium containing the data;

15) 'data processing' shall mean the technical operations involved in data management, irrespective of the method and instruments employed for such operations and the venue where it takes place;

16) 'processor' shall mean a natural or legal person or unincorporated organization that is engaged in the processing of personal data on behalf of a controller - including when ordered by virtue of legal regulation;

17) 'personal data filing system' (filing system) shall mean any structured set of personal data that are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

18) 'set of data' shall mean all data contained in a filing system;

19) 'third person' shall mean any natural or legal person or unincorporated organization other than the data subject, the controller or the processor;

20) 'third country' shall mean any country that is not a member of the European Union.

Chapter II

PROTECTION OF PERSONAL DATA

Data Processing

Section 3.

(1) Personal data may be processed if

a) the data subject has given his consent, or

b) decreed by law or by a local authority based on authorization conferred by law concerning specific data defined therein.

(2) Special data may be processed if

a) the data subject has given his explicit consent in writing, or

b) prescribed by treaty concerning the personal data specified in Point 2. a) of Section 2, or if ordered by law in connection with the enforcement of some constitutional right or for national security or law enforcement purposes,

c) ordered by law in other cases.

(3) Where data management is mandatory, the purpose and the conditions of management, the type of data and access to such data, the duration of the proposed processing operation, and the controller shall be specified by the statute or local government decree in which it is ordered.

(4) Where it serves the interest of the public, free access to particular personal data may be ordered by law as defined therein. In all other cases, free access to personal data may be provided only upon the consent of the data subject that is to be made in writing with regard to special data. If there is any doubt, it is to be presumed that the data subject did not consent to allow free access.

(5) The consent of the data subject shall be considered granted in connection with any data he has conveyed to the public or has supplied for publication.

(6) In connection with any proceeding requested by the data subject, his consent for processing his data to the extent necessary shall be considered granted, of which the data subject must be advised.

(7) The data subject may grant consent in a written agreement concluded with the controller for the performance of the contract. In this case, the contract shall contain all information that is to be made available to the data subject under this Act in connection with the processing of personal data, such as the description of the data involved, the duration of the proposed processing operation, the purpose of processing, the transmission of data and the use of a processor. The contract must clearly indicate the data subject's signature and explicit consent for having his data processed as stipulated in the contract.

(8) If the data subject is physically or legally incapable of giving his consent for processing his personal data, the processing of his personal data - which includes his special data - is allowed to the extent necessary to protect the vital interests of the data subject or of another person or in order to prevent or avert a catastrophe or emergency.

Section 4.

The right for the protection of personal data and the fundamental right to privacy of individuals must not be breached by any other interest, including free access to information of public interest (Section 19) for data processing, unless an exemption is granted by law.

Data Processing

Section 4/A.

(1) The rights and obligations of data processors arising in connection with the processing of personal data shall be determined by the data manager within the scope specified by the this Act and other legislation on data management. The data manager shall be held liable for the legitimacy of instructions pertaining to data management operations.

(2) The data processor shall be held liable within his sphere of competence and within the scope specified by the data manager for the processing, alteration, erasure and disclosure by transmission of personal data. The data processor shall not be permitted to subcontract any part of his operations to another data processor.

(3) A processor may not make any decision on the merits of data management and shall process any and all data entrusted to him solely as instructed by the controller; the processor shall not engage in data processing for his own purposes and shall store and safeguard personal data according to the instructions of the controller.

(4) Contracts for the processing of data must be made in writing. Any company that is interested in the business activity for which personal data is used may not be contracted for the processing of such data.

(5) Contracts for the processing of data to be concluded with third-country processors shall be drafted in compliance with the Decision of the Commission of the European Communities, which has been published by the data protection commissioner in *Magyar Közlöny* [Official Hungarian Gazette].

(6) This Act shall apply if a third-country controller that is involved in the processing of personal data employs a processor whose registered address or place of business (branch) or habitual residence (place of abode) is situated in the territory of the Republic of Hungary or if it makes use of equipment situated on the territory of the Republic of Hungary, unless such equipment is used solely for the purpose of transit through the territory of the European Union. Such controllers shall have a representative installed in the territory of the Republic of Hungary.

Legitimacy of Data Processing

Section 5.

(1) Personal data may be processed only for specified and explicit purposes, where it is necessary for carrying out certain rights or obligations. This purpose must be satisfied in all stages of operations of data processing.

(2) 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.

(3) The processing of data prescribed to be disclosed may be ordered in the public interest.

(4) Personal data may - with the data subject's consent or by virtue of legal regulation - be processed for the performance of a task carried out in the public interest or in the exercise of official authority, in the fulfillment of the official tasks of the controller or the recipient third party, for the protection of the data subject's vital interest, for the performance of a contract between the data subject and the controller, in the legitimate interests of the controller or a third party, or in the legitimate operation of a charitable organization.

(5) Personal data that concern criminal offenses and are being processed for the purposes of preventing, investigating, detecting and prosecuting criminal offences and data files containing information pertaining to

misdemeanor cases, civil lawsuits and non-litigious cases may only be processed by central or local government authorities.

Section 6.

(1) Prior to the collection of data the data subject shall be informed whether disclosure is voluntary or compulsory. If compulsory, the legal regulation on which it is based shall also be indicated.

(2) The data subject shall be clearly and elaborately informed of all aspects concerning the processing of his personal data, such as the purpose for which his data is required and the legal grounds, the person entitled to carry out the processing, the duration of the proposed processing operation and the persons to whom his data may be disclosed. Information shall also be provided on the data subject's rights and remedies.

(3) Notification of data management is considered granted where disclosure by transmission from existing data processing operations or by alignment or combination for further processing is prescribed by legal regulation.

(4) If individual notification is impossible or likely to result in unreasonable expense, notification of data management - particularly if it is for statistical or scientific purposes (including historical research) - may occur by way of publishing the fact of data collection, the data subjects involved, the purpose and duration of the proposed processing operation and the availability of data.

Data Quality

Section 7.

(1) Personal data collected for processing must be

a) processed fairly and lawfully;

b) accurate, complete and, where necessary, kept up to date;

c) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected.

(2) The use of personal identification codes or any other identifier of general application shall not be permitted.

Transfer of Data, Set of Transfer Operations

Section 8.

(1) Data may be transferred, whether in a single or in a set of operations, if the data subject has given his consent or if the transfer is legally permitted, and if the safeguards for data processing are satisfied with regard to each and every personal data.

(2) Subsection (1) shall also apply where data is structured between various filing systems of the same processor, or between those of government and local authorities.

Transfer of Data to Foreign Countries

Section 9.

(1) Personal data (including special data) may be transferred - irrespective of the medium and the manner in which it is transferred - to a third-country controller or processor if the data subject has given his consent, if the transfer is permitted by law or if it is prescribed by treaty or international convention, provided the laws of the third country in question afford an adequate level of protection within the meaning of Community standards with respect to the processing of the data transferred.

(2) Transmission of data to Member States of the European Union shall be treated as transmission within the territory of the Republic of Hungary.

Automated Individual Decisions

Section 9/A.

(1) Evaluation of certain personal aspects of any person by automated (computerized) processing of data may only be carried out if the data subject explicitly gives his consent or if such evaluation is permitted by law. The data subject must be given the opportunity to express his opinion.

(2) Where personal data is processed by automated means, the data subject must, at his request, be informed of the mathematical method that is used and its essence.

Security of Processing

Section 10.

(1) Data managers, and within their sphere of competence, data processors must implement adequate safeguards and appropriate technical and organizational measures to protect personal data, as well as adequate procedural rules to enforce the provisions of this Act and other regulations concerning confidentiality and security of data processing.

(2) Data must be protected against unauthorized access, alteration, transfer, disclosure by transmission or deletion as well as damage and accidental destruction. For the technical protection of personal data, the controller, the processor or the operator of the telecommunications or information technology equipment shall implement security measures in particular if the processing involves the transmission of data over a network or any other means of information technology.

The Rights of Data Subjects and their Enforcement

Section 11.

(1) Any data subject may request

a) confirmation as to whether or not data relating to him are being processed (Sections 12 and 13), and

b) the rectification or erasure of his personal data, with the exception of those processed by order of legal regulation (Sections 14-16).

(2) The register of processing operations [Subsection (1) of Section 28] may be inspected (including the taking of notes) by any person. An extract of the data contained therein may be requested upon payment of a fee.

Section 12.

(1) Upon the data subject's request the data manager must provide information concerning the data relating to him, including those processed by a data processor on its behalf, the purpose, grounds and duration of processing, the name and address (corporate address) of the data processor and on its activities relating to data management, and the recipients of his data and the purpose for which they are or had been transferred. The duration for which records must be kept on the data transferred, and in consequence the obligation of information may be limited by legal regulation on data processing. The period of restriction shall not be less than five years in respect of personal data, and twenty years in respect of special data.

(2) Data processor must comply with requests for information without any delay, and provide the information requested in an intelligible form within no more than 30 days.

(3) The information specified in Subsection (2) shall be provided free of charge for any category of data once a year. Additional information concerning the same category of data may be subject to a charge. Where any payment is made in connection with data that was processed unlawfully, or the request led to rectification, it shall be refunded.

Section 13.

(1) A data processor may refuse to provide information to the data subject where it is permitted by law in the cases defined under Section 16.

(2) The data processor must notify the data subject of the reasons for refusal.

(3) Data processors shall notify the data protection commissioner once a year on refused requests.

Section 14.

(1) Data processors must correct the data if it is false.

(2) Personal data must be erased if

a) processed unlawfully;

b) so requested by the data subject in accordance with Paragraph b) of Subsection (1) of Section 11;

c) it is deficient or inaccurate and it cannot be legitimately corrected, provided that deletion is not disallowed by statutory provision;

d) the purpose of processing no longer exists or the legal time limit for storage has expired;

e) so instructed by court order or by the data protection commissioner.

(3) With the exception of illicit data processing, the requirement of erasure shall not apply to the personal data recorded on a medium that is to be deposited in archive under the legal regulation on archive materials.

Section 15.

When a data is corrected or erased, the data subject to whom it pertains and all recipients to whom it was transferred for processing must be notified. This notification shall not be required if it does not violate the rightful interest of the data subject in view of the purpose of processing.

Section 16.

The rights of data subjects (Sections 11-15) may be restricted by this Act in order to safeguard the external and internal security of the State (e.g., defense, national security, the prevention, investigation, detection and prosecution of criminal offences), protect the economic and financial interests of central and local government, safeguard the important economic and financial interests of the European Union, guard against disciplinary and ethical breaches in the regulated professions, prevent and detect breaches of obligation related to labor law and job safety - including in all cases control and supervision - and to protect data subjects or the rights and freedoms of others.

The Data Subject's Right to Object

Section 16/A.

(1) The data subject shall have the right to object to the processing of data relating to him

a) if processing (disclosure) is carried out solely for the purpose of enforcing the rights and legitimate interests of the controller or the recipient, unless processing is prescribed by law;

b) if personal data is used or transferred for the purposes of direct marketing, public opinion polling or scientific research;

c) if the right to object is ensured by law.

(2) In the event of objection, the controller shall discontinue processing operations and investigate the cause of objection within the shortest possible time, not to exceed 15 days, and shall notify the data subject in writing of the findings of the investigation. If the objection is justified, the controller shall terminate all processing operations (including data collection and transmission), block the data involved and notify all recipients to whom any of these data had been previously transferred concerning the objection and the ensuing measures; these recipients shall also take measures regarding the objection.

(3) If the data subject disagrees with the decision taken by the controller under Subsection (2), the data subject shall have the right under this Act to seek legal remedy within 30 days of the date the decision was conveyed.

(4) If data that are necessary to assert the data recipient's lawful rights are withheld owing to the data subject's objection, the data recipient shall have the right under this Act to file charges against the controller within 15 days from the date the decision is conveyed under Subsection (2) in order to obtain the data. The controller may implicate the data subject in such lawsuit.

(5) If the court rejects the petition filed by the data recipient, the controller shall be required to delete the data subject's personal data within three days of the court ruling. The controller shall delete the data even if the data recipient does not file for court action within the time limit referred to in Subsection (4).

(6) The controller shall not delete the data of the data subject if processing has been prescribed by law. However, data may not be disclosed to the data recipient if the controller agrees with the objection or if the court has found the objection justified.

Judicial Remedy

Section 17.

(1) The data subject and the person referred to in Subsection (4) of Section 16/A may file for court action against the controller for any violation of their rights. The court shall hear such cases immediately.

(2) The burden of proof of compliance with the law lies with the data processor.

(3) Such lawsuits are heard by the court in whose jurisdiction the controller's registered address (residence) is located or, if so requested by the data subject, by the court in whose jurisdiction the data subject's residence (place of abode) is located. Even persons lacking legal capacity to sue may be a party in such lawsuits.

(4) When the decision is in favor of the plaintiff, the court shall order the controller to provide the information, to correct or delete the data in question, to void the automated individual decision, to honor the data subject's objection, or to disclose the data requested by the person referred to in Subsection (4) of Section 16/A.

(5) The court may also order publication of its decision, by way of publishing the identification data of the controller, if it is necessitated for data protection in general or in connection with the rights of large numbers of data subjects under protection by this Act.

Liability

Section 18.

(1) Data managers shall be liable for any damage caused to a data subject as a result of unlawful processing or by breaching the technical requirements of data protection. The data manager shall also be liable for any damage caused by a data processor acting on its behalf. The data manager may be exempted from liability if he proves that the damage was caused by reasons beyond his control.

(2) No compensation shall be paid where the damage was caused by intentional or negligent conduct on the part of the data subject.

Chapter III

ACCESS TO INFORMATION OF PUBLIC INTEREST

Section 19.

(1) State or local public authorities and agencies and other bodies attending to the public duties specified by law (hereinafter jointly referred to as "agency') shall provide the general public with accurate and speedy information concerning the matters under their competence, such as the budgets of the central government and local governments and the implementation thereof, the management of assets controlled by the central government and by local governments, the appropriation of public funds, and special and exclusive rights conferred upon market actors, private organizations or individuals.

(2) The agencies referred to in Subsection (1) shall regularly publish or otherwise make available all information of import concerning their competence, jurisdiction, organizational structure, professional activities, the evaluation of such activities (including their effectiveness), the categories of data they process, the legal regulations that pertain to their operations, and their financial management. The names and positions of persons acting in the name and on behalf of the above-specified agencies shall be treated as public information, unless otherwise prescribed by law. The manner of disclosure and the data to be disclosed may be prescribed by legal regulation.

(3) The agencies defined in Subsection (1) shall allow free access to the public information they have on files to any person, excluding those labelled state or service secret by an agency vested with proper authorization, or if classified by virtue of commitment under treaty or convention, or if access to specific information of public interest is restricted by law in connection with

a) defense;

b) national security;

c) prevention, investigation, detection and prosecution of criminal offences;

d) central financial or foreign exchange policy;

e) external relations, relations with international organizations;

f) court proceeding.

(4) The personal data of a person acting in the name and on behalf of the agencies specified in Subsection (1), to the extent that it relates to his duties, shall not restrict access to specific information of public interest.

(5) 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.

(6) Access to business secrets in connection with access to and publication of information of public interest shall be governed by the relevant provisions of the Civil Code.

(7) The availability of public information may also be limited by European Union legislation with a view to any important economic or financial interests of the European Union, including monetary, budgetary and tax policies.

Section 20.

(1) The agencies processing information of public interest must comply with requests for information without any delay, and shall provide it in an intelligible form within no more than 15 days. The applicant may also request for a fee, a copy of the document or part of a document containing the data in question, regardless of the form of storage.

(2) When a request for information is refused, the applicant must be notified within 8 days in writing and must be given the reasons for refusal.

(3) The head of agency processing information of public interest may charge a fee for any supply of information, not exceeding the costs of service. If requested by the applicant, the amount of charges must be specified in advance.

(4) The agencies specified in Subsection (1) of Section 19 shall notify the data protection commissioner once a year on refused requests, including the reasons of refusal.

Section 21.

(1) When a person's request for public information is refused, he may file for court action.

(2) The burden of proof of compliance with the law lies with the data processor agency.

(3) The lawsuit shall be initiated within 30 days from the date of refusal against the agency that has refused the information.

(4) Any person who cannot sue or be sued may also be involved in such lawsuits.

(5) Lawsuits against agencies of nationwide jurisdiction shall be filed at the competent county (Budapest) court. Lawsuits against local agencies shall be filed at the central county court, or at the Central Pest District Court in Budapest. The competency of the court is determined based on the location of the agency that refused to provide information.

(6) The court shall hear such cases under priority.

(7) When the decision is in favor of the plaintiff, the court shall order the data processor agency to provide the information.

Section 22.

This Chapter shall not apply to the supply of information from official records that is subject to the provisions of specific other legislation.

Chapter IV

DATA PROTECTION COMMISSIONER, REGISTER OF PROCESSING OPERATIONS

Data Protection Commissioner

Section 23.

(1) To protect the rights and freedoms afforded by the Constitution for the protection of personal data and access to information of public interest, the Parliament shall appoint a data protection commissioner from candidates of high repute satisfying the following criteria: must be a Hungarian citizen holding a diploma, have no prior criminal record, must have outstanding theoretical knowledge or 10 years of professional experience in the field of data protection, including all phases of administration and control.

(2) The provisions of the Act on the Ombudsman of Civil Rights shall apply to the data protection commissioner with the exceptions set forth in this Act.

Section 24.

The data protection commissioner

a) shall oversee compliance with the regulations of this Act and other legislation related to data protection;

b) shall investigate the reports he receives;

c) shall provide for the register of processing operations.

d) shall facilitate the uniform enforcement of the statutory provisions on the processing of personal data and on the availability of public information;

e) shall exercise and perform the tasks and duties conferred under this Act.

Section 25.

(1) The data protection commissioner shall monitor compliance with the requirements for the protection of personal data and for free access to information of public interest. He/she shall have authority to make recommendations for new regulations and for the amendment of legislation pertaining to data processing and information of public interest, and shall express his opinion on bills covering the same subject. As to the scope of data to be treated as state or service secrets, the data protection commissioner shall have authority to recommend specific data to be removed or added.

(2) Upon noticing any unlawful data processing operation, the data protection commissioner shall advise the data processor to cease such operation. The data processor must comply within 30 days and shall report to the data protection commissioner in writing concerning the measures taken.

(3) If the controller or processor fails to comply and cease the above-specified unlawful data processing operation, the data protection commissioner may order that unlawfully processed data be blocked, deleted or destroyed, or the data protection commissioner may prohibit the unauthorized data management and/or processing operations and suspend any operation aimed at transferring data abroad. The data protection commissioner shall announce these illegitimate data management and/or processing operations to the public and identify the controller (processor) and the measures proposed by it.

(4) The controller, the processor or the data subject may seek judicial remedy against the data protection commissioner's actions. The data involved in such litigated data processing operations may not be deleted or destroyed until the court has made a definitive ruling; however, processing operations must be discontinued and data must be blocked.

Section 26.

(1) The data protection commissioner in his official capacity shall have powers to request information from data processors and to inspect any document and processing operations that may involve personal data or information of public interest.

(2) The data protection commissioner shall be authorized to enter any premises where data processing takes place.

(3) The data protection commissioner shall also have access to state and service secrets in connection with his official duties defined in this Section, however, the rules of confidentiality must be observed by the data protection commissioner as well. The data protection commissioner must act in person when investigating any case of data processing that involves state or service secrets, or may have members of his staff acting on his behalf, if they have volunteered and have been checked for national security reasons.

(4) When the data protection commissioner concludes in his official capacity that any restricted-access data has been classified without proper justification, other than those classified by virtue of treaty or convention, the commissioner shall instruct the person by whom it was classified to lift or revise the restriction. The classifying person may contest such instruction within 30 days at the Municipal Court of Budapest where it will be heard in a closed session under priority.

Section 27.

(1) In the case of any violation of the rights of a person in connection with his personal data or free access to public information, or if there is imminent danger of such violation, it shall be reported to the data protection commissioner, unless a court action is already pending concerning the case in question.

(2) The person making a report to the data protection commissioner must not suffer any detriment for making such report. Any person filing such report shall be entitled to the same protection afforded to persons filing reports in the public interest.

Register of Processing Operations

Section 28.

(1) Prior to commencing operations, data processors must notify for the purpose of registration the data protection commissioner of the following:

a) the purpose of processing;

b) the category of data and the grounds for processing;

c) the data subjects involved;

d) the source;

e) the categories of data transferred, the recipients and the grounds for transfer;

f) the deadline of erasure of specific categories;

g) name and address (corporate address) of the data manager and the data processor, the place where records are kept and/or where processing is carried out, and the data processor's activities in connection with data management operations.

h) the name of and contact information for the internal data protection officer.

(2) When the processing of certain data is prescribed by legal regulation, it shall be announced by the competent minister, the director of the agency of national jurisdiction, or by the mayor or the person presiding over the county assembly concerned within 15 days from the date when the legal regulation in question enters into force.

(3) National security agencies shall announce the purpose and the grounds for data processing.

Section 29.

(1) Upon registration, each data processor shall be issued a registration number. This registration number shall be used for all operations with data, such as when data is transferred or published, or when provided to the data subject.

(2) Any changes in the data specified Subsection (1) of Section 28 shall be reported to the data protection commissioner within 8 days, and the records shall be revised accordingly.

Section 30.

Data processing shall not be notified to the register of processing operations

a) when it concerns the data of the data processor's employees, members, students or customers;

b) when carried out in accordance with the internal rules of the church or other religious organization;

c) if it concerns the personal data of a person undergoing medical treatment, for the purposes of health care and preventive measures or for settling claims for benefits and services in the social insurance system;

d) where it contains information concerning the provision of social and other benefits to the data subject;

e) where it contains the personal data of persons implicated in an official regulatory, public prosecutor or court proceeding to the extent required for such proceeding;

f) if it contains personal data for official statistical purposes, provided there are adequate guarantees that the data is rendered anonymous in such a way that the data subject is no longer identifiable;

g) where it contains data of organizations and bodies falling under the scope of the Media Act, if they are used solely for their own information;

h) if it serves the purposes of scientific research, and if the data are not made available to the public;

i) if the data is transferred to a public archive;

j) if it serves the own purposes of a natural person.

Preliminary Inspection

Section 31.

(1) The data protection commissioner shall have powers to conduct preliminary inspections prior to registration.

(2) Prior to the processing of any new data files or the use of new data processing technologies, the data protection commissioner may conduct preliminary inspections at controllers processing the following data:

a) data files concerning authorities of nationwide jurisdiction, data files concerning employment and criminal records;

b) data files from the customer records of financial institutions and public utility companies;

c) data files from the customer records of telecommunications service providers;

d) data files containing the individual statistical data defined in specific other legislation.

(3) Controllers shall be required to notify the data protection commissioner 30 days prior to the commencement of the processing of any new data files or the use of new data processing technologies. The data protection commissioner shall notify a controller of his intention to conduct a preliminary inspection within eight days of

receiving the above-specified notification and shall carry out the inspection within 30 days. Processing operations may commence only upon completion of the inspection conducted by the data protection commissioner.

(4) On the basis of the findings of the inspection, the data protection commissioner may prohibit the processing of specific data or may instruct the controller to change the processing technology. If the data protection commissioner disagrees with the legal regulation prescribing data processing, he may submit a proposal to amend the legal regulation in question.

Internal Data Protection Officer, Data Protection Regulations

Section 31/A.

(1) The following controllers and processors shall appoint or commission an internal data protection officer - who shall hold a law degree, a degree in economics or computer sciences or an equivalent degree in higher education - who is to report directly to the head of the organization:

a) authorities of nationwide jurisdiction, and controllers and processors engaged in processing data files of employment and criminal records;

b) financial institutions;

c) telecommunications service providers and public utility companies.

(2) The internal data protection officer shall:

a) participate and assist in the decision-making process with regard to data processing and in enforcing the rights of data subjects;

b) monitor compliance with the provisions of this Act and other legal regulations on data processing as well as with the provisions of internal data protection and data security regulations and the data security requirements;

c) investigate complaints conveyed to him and, if he detects any unauthorized data processing operations, request the controller or processor in question to cease such operations;

d) prepare the internal data protection and data security regulations;

e) maintain the internal data protection register;

f) arrange training sessions on the subject of data protection.

(3) The controllers referred to in Subsection (1) and central and local government controllers - other than controllers not required to report to the data protection register - shall be required to adopt data protection and data security regulations in accordance with this Act.

Chapter V

SPECIAL PROVISIONS

Processing and Use of Personal Data by Research Institutions

Section 32.

(1) Personal data collected and stored for scientific reasons must be used only for scientific research projects.

(2) Any personal data that no longer serves research purposes must be rendered anonymous. Any data relating to an identified or identifiable natural person must be stored separately. Such data may be related to other data if it is necessary for the purposes of research.

(3) An agency or person performing scientific research shall be allowed to publish personal data only if

a) the data subject has given his consent, or

b) it is necessary to demonstrate the findings of research in connection with historical events.

Use of Personal Data for Statistical Purposes

Section 32/A.

(1) Personal data recorded, received or processed for statistical purposes may only be used for statistical purposes. The individual statistical data defined in specific other legislation, including personal data, may not be transferred, received or processed in any way or form or under any circumstances, and they may not be published.

(2) The detailed regulations governing processing operations involving personal data are contained in another act.

Chapter VI

CLOSING PROVISIONS

Amendments

Section 33.

The following provision shall replace Subsection (1) of Section 83 of Act IV of 1959 on the Civil Code of the Republic of Hungary:

(1) Data management and data processing by computer or other means may not violate inherent rights."

Entry into Force

Section 34.

(1) This Act, with the exceptions set forth in Subsections (2) and (3), shall enter into force on the first day of the sixth mouth following its promulgation.

(2) Chapter III (Sections 19-22) of this Act shall enter into force on the 15th day following promulgation.

(3) Chapter IV (Sections 23-31) of this Act shall enter into force simultaneously with the Act on the Ombudsman for Civil Rights.

Section 35.

(1) Where this Act prescribes legislation in the form of an act, it shall be drafted by 31 December 1992, with the exception of Subsection (3), Section 4, and Subsection (1) of Section 13.

(2) Legal directives in connection with data processing cannot be used after the promulgation of this Act.

Section 36.

(1)

(2) Data processors shall notify all processing operations already existing at the time of this Act entering into force within three months from the appointment of the data protection commissioner for registration in the register of processing operations.

Section 37.

The Minister of Finance is hereby authorized to decree the amount of fees payable under Subsection (2) of Section 11 and the detailed regulations for the administration of such fees.

Act LXIII of 1992

on the Protection of Personal Data and the Disclosure of Information of Public Interest

Having regard to the protection of personal data and to access to information of public interest, the Parliament has adopted the following Act in accordance with the Constitution of the Republic of Hungary:

Chapter I

GENERAL PROVISIONS

Purpose of this Act

Section 1.

(1) The purpose of this Act is to ensure the right to privacy regarding personal data and free access to information of public interest, notwithstanding any exemptions provided by legal regulation specified in this Act.

(2) No derogation from the provisions of this Act shall be permitted, unless it is expressly provided for in this Act.

(3) Any exemption granted in this Act must apply to specific data and specific data manager together.

Scope

Section 1/A.

(1) This Act shall apply to all data management and data processing operations performed in the territory of the Republic of Hungary that pertain to the data of natural persons or to public information or information of public interest.

(2) This Act shall apply to data management and data processing operations whether performed in full or in part by an automated process or by manual processing.

(3) This Act shall not apply where data is processed by a natural person exclusively for his own purposes.

Definitions

Section 2.

For the purposes of this Act:

1) 'personal data' shall mean any information relating to an identified or identifiable natural person (hereinafter referred to as "data subject') and any reference drawn, whether directly or indirectly, from such information. In the course of data processing, such information shall be treated as personal data as long as the data subject remains identifiable through it. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

2) 'special data' shall mean

a) personal data revealing racial, national or ethnic origin, political opinions and any affiliation with political parties, religious or philosophical beliefs, trade-union membership,

b) personal data concerning health, addictions, sex life, or criminal record;

3) 'personal data relating to criminal offenses' shall mean personal data that might be related to the data subject or that pertain to any prior criminal offense committed by the data subject and that is obtained by organizations authorized to conduct criminal proceedings or investigations or by penal institutions during or prior to criminal proceedings in connection with a crime or criminal proceedings;

4) 'public information' shall mean 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);

5) 'public information subject to disclosure' shall mean any data managed by or pertaining to a natural or legal person or an unincorporated organization, other than public information that is not subject to disclosure, that are prescribed by law to be published or disclosed for the benefit of the general public;

6) 'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed without limitation or with regard to specific operations;

7) 'the data subject's objection' shall mean an indication of his wishes by which the data subject objects to the processing of his data and requests that the processing of data relating to him be terminated and/or the processed data be deleted;

8) 'controller' shall mean a natural or legal person or unincorporated organization that determines the purpose of the processing of personal data, makes decisions regarding data management (including the means) and implements such decisions itself or engages a processor to implement them;

9) 'data management' shall mean any operation or set of operations that is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, deletion or destruction, and blocking them from further use. Photographing, sound and video recording, and the recording of physical attributes for identification purposes (such as fingerprints and palm prints, DNA samples and retinal images;

10) 'disclosure by transmission' shall mean making data available to a specific third party;

11) 'public disclosure' shall mean making data available to the general public;

12) 'deletion of data' shall mean the destruction or elimination of data sufficient to make them irretrievable;

13) 'blocking of data' shall mean preventing - permanently or for a predetermined period - the transmission, access to, disclosure, adaptation or alteration, destruction, deletion, alignment or combination, and the use of data;

14) 'destruction of data' shall mean the complete physical destruction of data or the medium containing the data;

15) 'data processing' shall mean the technical operations involved in data management, irrespective of the method and instruments employed for such operations and the venue where it takes place;

16) 'processor' shall mean a natural or legal person or unincorporated organization that is engaged in the processing of personal data on behalf of a controller - including when ordered by virtue of legal regulation;

17) 'personal data filing system' (filing system) shall mean any structured set of personal data that are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

18) 'set of data' shall mean all data contained in a filing system;

19) 'third person' shall mean any natural or legal person or unincorporated organization other than the data subject, the controller or the processor;

20) 'third country' shall mean any country that is not a member of the European Union.

Chapter II

PROTECTION OF PERSONAL DATA

Data Processing

Section 3.

(1) Personal data may be processed if

a) the data subject has given his consent, or

b) decreed by law or by a local authority based on authorization conferred by law concerning specific data defined therein.

(2) Special data may be processed if

a) the data subject has given his explicit consent in writing, or

b) prescribed by treaty concerning the personal data specified in Point 2. a) of Section 2, or if ordered by law in connection with the enforcement of some constitutional right or for national security or law enforcement purposes,

c) ordered by law in other cases.

(3) Where data management is mandatory, the purpose and the conditions of management, the type of data and access to such data, the duration of the proposed processing operation, and the controller shall be specified by the statute or local government decree in which it is ordered.

(4) Where it serves the interest of the public, free access to particular personal data may be ordered by law as defined therein. In all other cases, free access to personal data may be provided only upon the consent of the data subject that is to be made in writing with regard to special data. If there is any doubt, it is to be presumed that the data subject did not consent to allow free access.

(5) The consent of the data subject shall be considered granted in connection with any data he has conveyed to the public or has supplied for publication.

(6) In connection with any proceeding requested by the data subject, his consent for processing his data to the extent necessary shall be considered granted, of which the data subject must be advised.

(7) The data subject may grant consent in a written agreement concluded with the controller for the performance of the contract. In this case, the contract shall contain all information that is to be made available to the data subject under this Act in connection with the processing of personal data, such as the description of the data involved, the duration of the proposed processing operation, the purpose of processing, the transmission of data and the use of a processor. The contract must clearly indicate the data subject's signature and explicit consent for having his data processed as stipulated in the contract.

(8) If the data subject is physically or legally incapable of giving his consent for processing his personal data, the processing of his personal data - which includes his special data - is allowed to the extent necessary to protect the vital interests of the data subject or of another person or in order to prevent or avert a catastrophe or emergency.

Section 4.

The right for the protection of personal data and the fundamental right to privacy of individuals must not be breached by any other interest, including free access to information of public interest (Section 19) for data processing, unless an exemption is granted by law.

Data Processing

Section 4/A.

(1) The rights and obligations of data processors arising in connection with the processing of personal data shall be determined by the data manager within the scope specified by the this Act and other legislation on data management. The data manager shall be held liable for the legitimacy of instructions pertaining to data management operations.

(2) The data processor shall be held liable within his sphere of competence and within the scope specified by the data manager for the processing, alteration, erasure and disclosure by transmission of personal data. The data processor shall not be permitted to subcontract any part of his operations to another data processor.

(3) A processor may not make any decision on the merits of data management and shall process any and all data entrusted to him solely as instructed by the controller; the processor shall not engage in data processing for his own purposes and shall store and safeguard personal data according to the instructions of the controller.

(4) Contracts for the processing of data must be made in writing. Any company that is interested in the business activity for which personal data is used may not be contracted for the processing of such data.

(5) Contracts for the processing of data to be concluded with third-country processors shall be drafted in compliance with the Decision of the Commission of the European Communities, which has been published by the data protection commissioner in *Magyar Közlöny* [Official Hungarian Gazette].

(6) This Act shall apply if a third-country controller that is involved in the processing of personal data employs a processor whose registered address or place of business (branch) or habitual residence (place of abode) is situated in the territory of the Republic of Hungary or if it makes use of equipment situated on the territory of the Republic of Hungary, unless such equipment is used solely for the purpose of transit through the territory of the European Union. Such controllers shall have a representative installed in the territory of the Republic of Hungary.

Legitimacy of Data Processing

Section 5.

(1) Personal data may be processed only for specified and explicit purposes, where it is necessary for carrying out certain rights or obligations. This purpose must be satisfied in all stages of operations of data processing.

(2) 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.

(3) The processing of data prescribed to be disclosed may be ordered in the public interest.

(4) Personal data may - with the data subject's consent or by virtue of legal regulation - be processed for the performance of a task carried out in the public interest or in the exercise of official authority, in the fulfillment of the official tasks of the controller or the recipient third party, for the protection of the data subject's vital interest, for the performance of a contract between the data subject and the controller, in the legitimate interests of the controller or a third party, or in the legitimate operation of a charitable organization.

(5) Personal data that concern criminal offenses and are being processed for the purposes of preventing, investigating, detecting and prosecuting criminal offences and data files containing information pertaining to

misdemeanor cases, civil lawsuits and non-litigious cases may only be processed by central or local government authorities.

Section 6.

(1) Prior to the collection of data the data subject shall be informed whether disclosure is voluntary or compulsory. If compulsory, the legal regulation on which it is based shall also be indicated.

(2) The data subject shall be clearly and elaborately informed of all aspects concerning the processing of his personal data, such as the purpose for which his data is required and the legal grounds, the person entitled to carry out the processing, the duration of the proposed processing operation and the persons to whom his data may be disclosed. Information shall also be provided on the data subject's rights and remedies.

(3) Notification of data management is considered granted where disclosure by transmission from existing data processing operations or by alignment or combination for further processing is prescribed by legal regulation.

(4) If individual notification is impossible or likely to result in unreasonable expense, notification of data management - particularly if it is for statistical or scientific purposes (including historical research) - may occur by way of publishing the fact of data collection, the data subjects involved, the purpose and duration of the proposed processing operation and the availability of data.

Data Quality

Section 7.

(1) Personal data collected for processing must be

a) processed fairly and lawfully;

b) accurate, complete and, where necessary, kept up to date;

c) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected.

(2) The use of personal identification codes or any other identifier of general application shall not be permitted.

Transfer of Data, Set of Transfer Operations

Section 8.

(1) Data may be transferred, whether in a single or in a set of operations, if the data subject has given his consent or if the transfer is legally permitted, and if the safeguards for data processing are satisfied with regard to each and every personal data.

(2) Subsection (1) shall also apply where data is structured between various filing systems of the same processor, or between those of government and local authorities.

Transfer of Data to Foreign Countries

Section 9.

(1) Personal data (including special data) may be transferred - irrespective of the medium and the manner in which it is transferred - to a third-country controller or processor if the data subject has given his consent, if the transfer is permitted by law or if it is prescribed by treaty or international convention, provided the laws of the third country in question afford an adequate level of protection within the meaning of Community standards with respect to the processing of the data transferred.

(2) Transmission of data to Member States of the European Union shall be treated as transmission within the territory of the Republic of Hungary.

Automated Individual Decisions

Section 9/A.

(1) Evaluation of certain personal aspects of any person by automated (computerized) processing of data may only be carried out if the data subject explicitly gives his consent or if such evaluation is permitted by law. The data subject must be given the opportunity to express his opinion.

(2) Where personal data is processed by automated means, the data subject must, at his request, be informed of the mathematical method that is used and its essence.

Security of Processing

Section 10.

(1) Data managers, and within their sphere of competence, data processors must implement adequate safeguards and appropriate technical and organizational measures to protect personal data, as well as adequate procedural rules to enforce the provisions of this Act and other regulations concerning confidentiality and security of data processing.

(2) Data must be protected against unauthorized access, alteration, transfer, disclosure by transmission or deletion as well as damage and accidental destruction. For the technical protection of personal data, the controller, the processor or the operator of the telecommunications or information technology equipment shall implement security measures in particular if the processing involves the transmission of data over a network or any other means of information technology.

The Rights of Data Subjects and their Enforcement

Section 11.

(1) Any data subject may request

a) confirmation as to whether or not data relating to him are being processed (Sections 12 and 13), and

b) the rectification or erasure of his personal data, with the exception of those processed by order of legal regulation (Sections 14-16).

(2) The register of processing operations [Subsection (1) of Section 28] may be inspected (including the taking of notes) by any person. An extract of the data contained therein may be requested upon payment of a fee.

Section 12.

(1) Upon the data subject's request the data manager must provide information concerning the data relating to him, including those processed by a data processor on its behalf, the purpose, grounds and duration of processing, the name and address (corporate address) of the data processor and on its activities relating to data management, and the recipients of his data and the purpose for which they are or had been transferred. The duration for which records must be kept on the data transferred, and in consequence the obligation of information may be limited by legal regulation on data processing. The period of restriction shall not be less than five years in respect of personal data, and twenty years in respect of special data.

(2) Data processor must comply with requests for information without any delay, and provide the information requested in an intelligible form within no more than 30 days.

(3) The information specified in Subsection (2) shall be provided free of charge for any category of data once a year. Additional information concerning the same category of data may be subject to a charge. Where any payment is made in connection with data that was processed unlawfully, or the request led to rectification, it shall be refunded.

Section 13.

(1) A data processor may refuse to provide information to the data subject where it is permitted by law in the cases defined under Section 16.

(2) The data processor must notify the data subject of the reasons for refusal.

(3) Data processors shall notify the data protection commissioner once a year on refused requests.

Section 14.

(1) Data processors must correct the data if it is false.

(2) Personal data must be erased if

a) processed unlawfully;

b) so requested by the data subject in accordance with Paragraph b) of Subsection (1) of Section 11;

c) it is deficient or inaccurate and it cannot be legitimately corrected, provided that deletion is not disallowed by statutory provision;

d) the purpose of processing no longer exists or the legal time limit for storage has expired;

e) so instructed by court order or by the data protection commissioner.

(3) With the exception of illicit data processing, the requirement of erasure shall not apply to the personal data recorded on a medium that is to be deposited in archive under the legal regulation on archive materials.

Section 15.

When a data is corrected or erased, the data subject to whom it pertains and all recipients to whom it was transferred for processing must be notified. This notification shall not be required if it does not violate the rightful interest of the data subject in view of the purpose of processing.

Section 16.

The rights of data subjects (Sections 11-15) may be restricted by this Act in order to safeguard the external and internal security of the State (e.g., defense, national security, the prevention, investigation, detection and prosecution of criminal offences), protect the economic and financial interests of central and local government, safeguard the important economic and financial interests of the European Union, guard against disciplinary and ethical breaches in the regulated professions, prevent and detect breaches of obligation related to labor law and job safety - including in all cases control and supervision - and to protect data subjects or the rights and freedoms of others.

The Data Subject's Right to Object

Section 16/A.

(1) The data subject shall have the right to object to the processing of data relating to him

a) if processing (disclosure) is carried out solely for the purpose of enforcing the rights and legitimate interests of the controller or the recipient, unless processing is prescribed by law;

b) if personal data is used or transferred for the purposes of direct marketing, public opinion polling or scientific research;

c) if the right to object is ensured by law.

(2) In the event of objection, the controller shall discontinue processing operations and investigate the cause of objection within the shortest possible time, not to exceed 15 days, and shall notify the data subject in writing of the findings of the investigation. If the objection is justified, the controller shall terminate all processing operations (including data collection and transmission), block the data involved and notify all recipients to whom any of these data had been previously transferred concerning the objection and the ensuing measures; these recipients shall also take measures regarding the objection.

(3) If the data subject disagrees with the decision taken by the controller under Subsection (2), the data subject shall have the right under this Act to seek legal remedy within 30 days of the date the decision was conveyed.

(4) If data that are necessary to assert the data recipient's lawful rights are withheld owing to the data subject's objection, the data recipient shall have the right under this Act to file charges against the controller within 15 days from the date the decision is conveyed under Subsection (2) in order to obtain the data. The controller may implicate the data subject in such lawsuit.

(5) If the court rejects the petition filed by the data recipient, the controller shall be required to delete the data subject's personal data within three days of the court ruling. The controller shall delete the data even if the data recipient does not file for court action within the time limit referred to in Subsection (4).

(6) The controller shall not delete the data of the data subject if processing has been prescribed by law. However, data may not be disclosed to the data recipient if the controller agrees with the objection or if the court has found the objection justified.

Judicial Remedy

Section 17.

(1) The data subject and the person referred to in Subsection (4) of Section 16/A may file for court action against the controller for any violation of their rights. The court shall hear such cases immediately.

(2) The burden of proof of compliance with the law lies with the data processor.

(3) Such lawsuits are heard by the court in whose jurisdiction the controller's registered address (residence) is located or, if so requested by the data subject, by the court in whose jurisdiction the data subject's residence (place of abode) is located. Even persons lacking legal capacity to sue may be a party in such lawsuits.

(4) When the decision is in favor of the plaintiff, the court shall order the controller to provide the information, to correct or delete the data in question, to void the automated individual decision, to honor the data subject's objection, or to disclose the data requested by the person referred to in Subsection (4) of Section 16/A.

(5) The court may also order publication of its decision, by way of publishing the identification data of the controller, if it is necessitated for data protection in general or in connection with the rights of large numbers of data subjects under protection by this Act.

Liability

Section 18.

(1) Data managers shall be liable for any damage caused to a data subject as a result of unlawful processing or by breaching the technical requirements of data protection. The data manager shall also be liable for any damage caused by a data processor acting on its behalf. The data manager may be exempted from liability if he proves that the damage was caused by reasons beyond his control.

(2) No compensation shall be paid where the damage was caused by intentional or negligent conduct on the part of the data subject.

Chapter III

ACCESS TO INFORMATION OF PUBLIC INTEREST

Section 19.

(1) State or local public authorities and agencies and other bodies attending to the public duties specified by law (hereinafter jointly referred to as "agency') shall provide the general public with accurate and speedy information concerning the matters under their competence, such as the budgets of the central government and local governments and the implementation thereof, the management of assets controlled by the central government and by local governments, the appropriation of public funds, and special and exclusive rights conferred upon market actors, private organizations or individuals.

(2) The agencies referred to in Subsection (1) shall regularly publish or otherwise make available all information of import concerning their competence, jurisdiction, organizational structure, professional activities, the evaluation of such activities (including their effectiveness), the categories of data they process, the legal regulations that pertain to their operations, and their financial management. The names and positions of persons acting in the name and on behalf of the above-specified agencies shall be treated as public information, unless otherwise prescribed by law. The manner of disclosure and the data to be disclosed may be prescribed by legal regulation.

(3) The agencies defined in Subsection (1) shall allow free access to the public information they have on files to any person, excluding those labelled state or service secret by an agency vested with proper authorization, or if classified by virtue of commitment under treaty or convention, or if access to specific information of public interest is restricted by law in connection with

a) defense;

b) national security;

c) prevention, investigation, detection and prosecution of criminal offences;

d) central financial or foreign exchange policy;

e) external relations, relations with international organizations;

f) court proceeding.

(4) The personal data of a person acting in the name and on behalf of the agencies specified in Subsection (1), to the extent that it relates to his duties, shall not restrict access to specific information of public interest.

(5) 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.

(6) Access to business secrets in connection with access to and publication of information of public interest shall be governed by the relevant provisions of the Civil Code.

(7) The availability of public information may also be limited by European Union legislation with a view to any important economic or financial interests of the European Union, including monetary, budgetary and tax policies.

Section 20.

(1) The agencies processing information of public interest must comply with requests for information without any delay, and shall provide it in an intelligible form within no more than 15 days. The applicant may also request for a fee, a copy of the document or part of a document containing the data in question, regardless of the form of storage.

(2) When a request for information is refused, the applicant must be notified within 8 days in writing and must be given the reasons for refusal.

(3) The head of agency processing information of public interest may charge a fee for any supply of information, not exceeding the costs of service. If requested by the applicant, the amount of charges must be specified in advance.

(4) The agencies specified in Subsection (1) of Section 19 shall notify the data protection commissioner once a year on refused requests, including the reasons of refusal.

Section 21.

(1) When a person's request for public information is refused, he may file for court action.

(2) The burden of proof of compliance with the law lies with the data processor agency.

(3) The lawsuit shall be initiated within 30 days from the date of refusal against the agency that has refused the information.

(4) Any person who cannot sue or be sued may also be involved in such lawsuits.

(5) Lawsuits against agencies of nationwide jurisdiction shall be filed at the competent county (Budapest) court. Lawsuits against local agencies shall be filed at the central county court, or at the Central Pest District Court in Budapest. The competency of the court is determined based on the location of the agency that refused to provide information.

(6) The court shall hear such cases under priority.

(7) When the decision is in favor of the plaintiff, the court shall order the data processor agency to provide the information.

Section 22.

This Chapter shall not apply to the supply of information from official records that is subject to the provisions of specific other legislation.

Chapter IV

DATA PROTECTION COMMISSIONER, REGISTER OF PROCESSING OPERATIONS

Data Protection Commissioner

Section 23.

(1) To protect the rights and freedoms afforded by the Constitution for the protection of personal data and access to information of public interest, the Parliament shall appoint a data protection commissioner from candidates of high repute satisfying the following criteria: must be a Hungarian citizen holding a diploma, have no prior criminal record, must have outstanding theoretical knowledge or 10 years of professional experience in the field of data protection, including all phases of administration and control.

(2) The provisions of the Act on the Ombudsman of Civil Rights shall apply to the data protection commissioner with the exceptions set forth in this Act.

Section 24.

The data protection commissioner

a) shall oversee compliance with the regulations of this Act and other legislation related to data protection;

b) shall investigate the reports he receives;

c) shall provide for the register of processing operations.

d) shall facilitate the uniform enforcement of the statutory provisions on the processing of personal data and on the availability of public information;

e) shall exercise and perform the tasks and duties conferred under this Act.

Section 25.

(1) The data protection commissioner shall monitor compliance with the requirements for the protection of personal data and for free access to information of public interest. He/she shall have authority to make recommendations for new regulations and for the amendment of legislation pertaining to data processing and information of public interest, and shall express his opinion on bills covering the same subject. As to the scope of data to be treated as state or service secrets, the data protection commissioner shall have authority to recommend specific data to be removed or added.

(2) Upon noticing any unlawful data processing operation, the data protection commissioner shall advise the data processor to cease such operation. The data processor must comply within 30 days and shall report to the data protection commissioner in writing concerning the measures taken.

(3) If the controller or processor fails to comply and cease the above-specified unlawful data processing operation, the data protection commissioner may order that unlawfully processed data be blocked, deleted or destroyed, or the data protection commissioner may prohibit the unauthorized data management and/or processing operations and suspend any operation aimed at transferring data abroad. The data protection commissioner shall announce these illegitimate data management and/or processing operations to the public and identify the controller (processor) and the measures proposed by it.

(4) The controller, the processor or the data subject may seek judicial remedy against the data protection commissioner's actions. The data involved in such litigated data processing operations may not be deleted or destroyed until the court has made a definitive ruling; however, processing operations must be discontinued and data must be blocked.

Section 26.

(1) The data protection commissioner in his official capacity shall have powers to request information from data processors and to inspect any document and processing operations that may involve personal data or information of public interest.

(2) The data protection commissioner shall be authorized to enter any premises where data processing takes place.

(3) The data protection commissioner shall also have access to state and service secrets in connection with his official duties defined in this Section, however, the rules of confidentiality must be observed by the data protection commissioner as well. The data protection commissioner must act in person when investigating any case of data processing that involves state or service secrets, or may have members of his staff acting on his behalf, if they have volunteered and have been checked for national security reasons.

(4) When the data protection commissioner concludes in his official capacity that any restricted-access data has been classified without proper justification, other than those classified by virtue of treaty or convention, the commissioner shall instruct the person by whom it was classified to lift or revise the restriction. The classifying person may contest such instruction within 30 days at the Municipal Court of Budapest where it will be heard in a closed session under priority.

Section 27.

(1) In the case of any violation of the rights of a person in connection with his personal data or free access to public information, or if there is imminent danger of such violation, it shall be reported to the data protection commissioner, unless a court action is already pending concerning the case in question.

(2) The person making a report to the data protection commissioner must not suffer any detriment for making such report. Any person filing such report shall be entitled to the same protection afforded to persons filing reports in the public interest.

Register of Processing Operations

Section 28.

(1) Prior to commencing operations, data processors must notify for the purpose of registration the data protection commissioner of the following:

a) the purpose of processing;

b) the category of data and the grounds for processing;

c) the data subjects involved;

d) the source;

e) the categories of data transferred, the recipients and the grounds for transfer;

f) the deadline of erasure of specific categories;

g) name and address (corporate address) of the data manager and the data processor, the place where records are kept and/or where processing is carried out, and the data processor's activities in connection with data management operations.

h) the name of and contact information for the internal data protection officer.

(2) When the processing of certain data is prescribed by legal regulation, it shall be announced by the competent minister, the director of the agency of national jurisdiction, or by the mayor or the person presiding over the county assembly concerned within 15 days from the date when the legal regulation in question enters into force.

(3) National security agencies shall announce the purpose and the grounds for data processing.

Section 29.

(1) Upon registration, each data processor shall be issued a registration number. This registration number shall be used for all operations with data, such as when data is transferred or published, or when provided to the data subject.

(2) Any changes in the data specified Subsection (1) of Section 28 shall be reported to the data protection commissioner within 8 days, and the records shall be revised accordingly.

Section 30.

Data processing shall not be notified to the register of processing operations

a) when it concerns the data of the data processor's employees, members, students or customers;

b) when carried out in accordance with the internal rules of the church or other religious organization;

c) if it concerns the personal data of a person undergoing medical treatment, for the purposes of health care and preventive measures or for settling claims for benefits and services in the social insurance system;

d) where it contains information concerning the provision of social and other benefits to the data subject;

e) where it contains the personal data of persons implicated in an official regulatory, public prosecutor or court proceeding to the extent required for such proceeding;

f) if it contains personal data for official statistical purposes, provided there are adequate guarantees that the data is rendered anonymous in such a way that the data subject is no longer identifiable;

g) where it contains data of organizations and bodies falling under the scope of the Media Act, if they are used solely for their own information;

h) if it serves the purposes of scientific research, and if the data are not made available to the public;

i) if the data is transferred to a public archive;

j) if it serves the own purposes of a natural person.

Preliminary Inspection

Section 31.

(1) The data protection commissioner shall have powers to conduct preliminary inspections prior to registration.

(2) Prior to the processing of any new data files or the use of new data processing technologies, the data protection commissioner may conduct preliminary inspections at controllers processing the following data:

a) data files concerning authorities of nationwide jurisdiction, data files concerning employment and criminal records;

b) data files from the customer records of financial institutions and public utility companies;

c) data files from the customer records of telecommunications service providers;

d) data files containing the individual statistical data defined in specific other legislation.

(3) Controllers shall be required to notify the data protection commissioner 30 days prior to the commencement of the processing of any new data files or the use of new data processing technologies. The data protection commissioner shall notify a controller of his intention to conduct a preliminary inspection within eight days of

receiving the above-specified notification and shall carry out the inspection within 30 days. Processing operations may commence only upon completion of the inspection conducted by the data protection commissioner.

(4) On the basis of the findings of the inspection, the data protection commissioner may prohibit the processing of specific data or may instruct the controller to change the processing technology. If the data protection commissioner disagrees with the legal regulation prescribing data processing, he may submit a proposal to amend the legal regulation in question.

Internal Data Protection Officer, Data Protection Regulations

Section 31/A.

(1) The following controllers and processors shall appoint or commission an internal data protection officer - who shall hold a law degree, a degree in economics or computer sciences or an equivalent degree in higher education - who is to report directly to the head of the organization:

a) authorities of nationwide jurisdiction, and controllers and processors engaged in processing data files of employment and criminal records;

b) financial institutions;

c) telecommunications service providers and public utility companies.

(2) The internal data protection officer shall:

a) participate and assist in the decision-making process with regard to data processing and in enforcing the rights of data subjects;

b) monitor compliance with the provisions of this Act and other legal regulations on data processing as well as with the provisions of internal data protection and data security regulations and the data security requirements;

c) investigate complaints conveyed to him and, if he detects any unauthorized data processing operations, request the controller or processor in question to cease such operations;

d) prepare the internal data protection and data security regulations;

e) maintain the internal data protection register;

f) arrange training sessions on the subject of data protection.

(3) The controllers referred to in Subsection (1) and central and local government controllers - other than controllers not required to report to the data protection register - shall be required to adopt data protection and data security regulations in accordance with this Act.

Chapter V

SPECIAL PROVISIONS

Processing and Use of Personal Data by Research Institutions

Section 32.

(1) Personal data collected and stored for scientific reasons must be used only for scientific research projects.

(2) Any personal data that no longer serves research purposes must be rendered anonymous. Any data relating to an identified or identifiable natural person must be stored separately. Such data may be related to other data if it is necessary for the purposes of research.

(3) An agency or person performing scientific research shall be allowed to publish personal data only if

a) the data subject has given his consent, or

b) it is necessary to demonstrate the findings of research in connection with historical events.

Use of Personal Data for Statistical Purposes

Section 32/A.