

# **ACT LXIII OF 1992 ON THE PROTECTION OF PERSONAL DATA AND THE PUBLICITY OF DATA OF PUBLIC INTEREST**

In harmony with the contents of the Constitution of the Republic of Hungary, Parliament creates the following Act on the basic rules serving the protection of personal data and the enforcement of the right of access to data of public interest:

## **Chapter I**

### **GENERAL PROVISIONS**

#### **Purpose of the Act**

##### **Section 1**

(1) The purpose of this Act, unless a legal rule defined in this Act provides otherwise, is to guarantee that everybody may dispose of his personal data himself, and that everybody may have access to data of public interest.

(2) Any deviation from the contents of this Act is only possible if expressly permitted by this Act.

(3) Any exception permitted in accordance with this Act may only be established jointly with regard to particular types and handlers of data. Interpretative Provisions

##### **Section 2**

In the course of the application of this Act

1. personal data: data which can be associated with a particular natural person (hereinafter: person concerned), the conclusion, which can be drawn from the data, relating to the person concerned. Personal data keep their above defined quality in the course of data handling until their connection with the person concerned can be restored;

2. special data:

personal data relating to

a) racial origin, national, nationality and ethnic status, political opinion or party affiliation, religious or other conviction,

b) health condition, abnormal addiction, sexual life and criminal record;

3. data of public interest: data handled by organs and persons fulfilling state or local government duties or other public duties defined in legal rules, not coming under the concept of personal data;

4. data handling: irrespective of the procedure applied, recording and storage, processing and utilization of personal data (including forwarding and publication), the

change of data and the prevention of their further use shall also be considered data handling;

5. forwarding of data: if the data are made accessible to particular third parties;
6. publication: if the data are made accessible to anybody;
7. data handler: organs or persons carrying out or making others carry out the activities defined in paragraph 4;
8. deletion of data: the rendering of data unrecognizable in a manner that their restoration is not possible;
9. legal rule: the Act, and local government decrees in respect of Section 1, subsection (1), Section 6, subsection (1), Section 12, subsection (1), Section 24, Section 25 and Section 28, subsection (2) of this Act.

## **Chapter II**

# **PROTECTION OF PERSONAL DATA**

## **Data Handling**

### **Section 3**

(1) Personal data may be handled, if

- a) the person concerned agrees thereto, or b) it is ordered by an Act or a local government decree on the basis of the authorization of an Act, within the sphere defined therein.

(2) Special data may be handled, if

- a) the person concerned consents to data handling in writing, or
- b) in the case of the data contained in Section 2, paragraph 2 a), it is based on an international agreement, or is ordered by an Act in the interest of the enforcement of a fundamental right provided in the Constitution, furthermore, in the interest of national security, crime prevention and criminal investigation;
- c) required by the law in other cases.

(3) An Act may order the publication of personal data for reasons of public interest, expressly specifying the sphere of data. In all other cases, the consent, or in the case of special data, the written consent of the person concerned is required for publication. In the case of any doubt, it shall be presumed that the person concerned did not give his consent.

(4) The consent of the person concerned shall be considered given in respect of the data disclosed by him in the course of his public appearance, or delivered by him for the purpose of publication.

(5) In the proceedings instituted at the request of the person concerned, his consent to the handling of his necessary data shall be presumed. The attention of the person concerned shall be drawn to this fact.

## **Section 4**

Unless an Act provides exemption, any other interests attached to data handling, also including the publicity of the data of public interest (Section 19) may not violate the right attached to the protection of personal data and the right to privacy of the person concerned.

## **Attachment of Data Handling to a Purpose**

### **Section 5**

(1) Personal data may only be handled for a particular purpose, exercise of rights or fulfilment of obligations. Each phase of data handling shall comply with this purpose.

(2) Only such personal data may be handled which are indispensable for accomplishing the purpose of data handling, are suitable for achieving the purpose, and only to the extent and for the time required for the accomplishment of the purpose.

(3) Data handling based on mandatory data supply may be ordered for reasons of public interest.

### **Section 6**

(1) Prior to recording the data, the person concerned shall be notified whether the data supply is voluntary or mandatory. In the case of mandatory data supply, the legal rule ordering data handling shall also be indicated.

(2) The person concerned shall be notified of the purpose of data handling and of the identity of the persons who will handle the data. Notification shall also have been effected if a legal rule provides for recording the data on the basis of the existing data handling through forwarding or connection.

## **Quality of Data**

### **Section 7**

(1) The personal data handled shall meet the following requirements:

- a) their recording and handling are fair and lawful;
- b) they are precise, complete and, if required, up-to-date;
- c) the manner of their storage is suitable for enabling identification of the person concerned only for the time required for the purpose of storage.

(2) The application of a general and uniform personal identification mark, which can be used without restriction, is prohibited.

## **Forwarding of Data, Connection of Various Forms of Data Handling**

### **Section 8**

(1) Data may be forwarded and the various forms of data handling may be connected if the person concerned consents thereto, or it is permitted by law, and the conditions of data handling are satisfied in respect of each personal data.

(2) Subsection (1) shall apply to the connection of data handled by the same data handler or by the state and local government organs.

## **Forwarding of Data Abroad**

### **Section 9**

Irrespective of the data carrier or the manner of data transmission, personal data may only be forwarded from Hungary to a foreign data handler, with the consent of the person concerned, or if it is permitted by law, provided that the conditions of data handling are satisfied by the foreign data handler in respect of each data.

## **Security of Data**

### **Section 10**

(1) The data handler shall provide for the security of the data, shall take the technical and organizational measures and establish the procedural rules which are required for the enforcement of this Act and other rules related to the protection of data and secrets.

(2) Data shall be protected particularly against illegal access, change, publication or deletion, and/or against damage or destruction.

## **Rights of the Persons Concerned and Enforcement Thereof**

### **Section 11**

(1) A person concerned may

a) request information on the handling of his personal data (Sections 12 and 13), and

b) request the correction of his personal data, or their deletion, with the exception of the data handled as ordered by legal rules (Sections 14 to 16).

(2) Anybody may have access to the data protection register [Section 28, subsection (1)], may take notes and request extracts from its contents. Fee shall be paid for an extract.

## **Section 12**

(1) At the request of the person concerned, the data handler shall give information on the data handled by it, on the purpose, legal ground and period of time of data handling, and on who and for what purpose will receive or have received the data. The legal rule regulating data handling may restrict the period of time for keeping of records relating to the forwarding of data, and on the basis thereof, the period of obligation to provide information. The period of restriction may not be shorter than five years in the case of personal data, and twenty years in the case of special data.

(2) The data handler shall provide the information within the shortest possible time reckoned from the submission of the application, but within not more than 30 days, in writing, in a form which is easy to understand.

(3) The information contained in subsection (2) is free of charge, if applicant did not submit an application for information regarding the same field to the data handler in the current year. In other cases, cost compensation may be established. The cost compensation, which has already been paid, shall be refunded if the data were handled illegally or if the application for information led to correction.

## **Section 13**

(1) The data handler may only refuse to inform the person concerned, if this is permitted by law in the cases defined in Section 16.

(2) The data handler shall notify the person concerned of the reasons for refusing the disclosure of information.

(3) The data handler shall notify annually the data protection commissioner of the applications refused.

## **Section 14**

(1) The data handler shall correct data which do not correspond to the facts.

(2) Personal data shall be deleted, if

a) their handling is unlawful;

b) requested by the person concerned in accordance with the contents of Section 11, subsection (1), paragraph b);

c) the purpose of data handling has ceased.

(3) The obligation of deletion, with the exception of unlawful data handling shall not apply to personal data whose data carrier shall be left in the archival custody pursuant to the legal rule applicable to the protection of archival material.

## **Section 15**

The person concerned and all those to whom the data were forwarded earlier for the purpose of data handling shall be notified of correction and deletion. The notification may not be necessary if it does not violate the lawful interest of the person concerned, taking into account the purpose of data handling.

## **Section 16**

An Act may restrict the rights of the person concerned (Sections 11 to 15) in the interest of the external and internal security of the state, thus in the interest of national defence, national security, prevention of crime or criminal investigation, furthermore, in the financial interest of the state or a local government, as well as in the interest of the protection of the rights of the person concerned or of those of other persons.

## **Enforcement of Rights through Courts**

### **Section 17**

(1) In the case of the violation of his rights, the person concerned may submit an application to the court against the data handler.

(2) The data handler shall prove whether the handling of data corresponds to the contents of legal rules.

(3) The court where the head office of the data handler is located is competent to conduct the lawsuit. All those who otherwise have no contentious legal capacity may also be parties to the lawsuit.

(4) If the court sustains the application, it shall oblige the data handler to give information, to correct or delete the data, and/or shall oblige the data protection commissioner to provide access to the data protection register.

(5) The court may order the entry of its judgment in the data protection register, if required by data protection interests and by the rights of a large number of persons concerned, as protected in this Act.

## **Compensation**

### **Section 18**

(1) The data handler shall pay compensation for the damage caused to others by the unlawful handling of the data of the person concerned or by violating the requirements of technical data protection. The data handler shall be exempted from liability if he proves that the damage was caused by an unavoidable reason beyond the sphere of data handling.

(2) No compensation shall be paid for the damage to the extent that it was caused by the wilful or seriously negligent conduct of the damaged party. Chapter III

## **Publicity of the Data of Public Interest**

### **Section 19**

(1) Organs and persons (hereinafter collectively: organ) fulfilling state or local government duties and other public duties defined in legal rules, shall promote the precise and rapid information of the public in connection with the matters coming under their sphere of duties, also including matters related to their financial management.

(2) The organs referred to in subsection (1) shall publish or make accessible in any other manner the most important data related to their activities, in particular, the data relating to their sphere of authority, competence, organizational structure, the types of data in their possession and the legal rules applicable to their operation. Unless an Act provides otherwise, the names and positions of persons acting within the competence of these organs shall be public data accessible to anybody.

(3) Those referred to in subsection (1) shall make possible that anybody may have access to the data of public interest handled by them, unless declared a state or service secret by the organ entitled to do so, on the basis of the given Act, furthermore, if the right to the publicity of the data of public interest is restricted by an Act, by defining the types of data, in the interest of

- a) national defence;
- b) national security;
- c) criminal investigation or crime prevention;
- d) for central financial or foreign exchange policy reasons;
- e) in respect of the conduct of foreign relations, relations with international organizations, and
- f) of court proceedings.

(4) The personal data related to their sphere of duties, of the persons, acting within the competence of the organs defined in subsection (1), shall not restrict access to data of public interest.

(5) Unless an Act provides otherwise, data generated for internal use and in connection with the preparation of decisions shall not be public within thirty years following their inception. At request, the head of the organ may permit access to the data even within the above time limit.

## **Section 20**

(1) The organ handling the data shall satisfy the application for access to data of public interest within the shortest possible time following the taking cognizance of the application, but within not more than 15 days, in a form which is easy to understand. The applicant may request copies of the documents or parts thereof containing the data irrespective of the manner of their storage.

(2) The applicant shall be notified of the refusal of an application, together with the reasons therefor, in writing, within 8 days.

(3) The head of the data handling organ may establish cost compensation for the communication of data of public interest, up to not more than the extent of costs incurred in connection with the communication. At the request of the applicant, the amount of such cost shall be communicated in advance.

(4) The organs referred to in Section 19, subsection (1) shall notify annually the data protection commissioner of the applications refused and the reasons for the refusals.

## **Section 21**

(1) The applicant may appeal to the court, if his application for data of public interest

is not satisfied.

(2) The organ handling the data shall prove the lawfulness and well-foundedness of any refusal.

(3) The action shall be instituted against the organ, within 30 days reckoned from the communication of the refusal, which refused to issue the information requested.

(4) All those who otherwise have no contentious legal capacity may also be parties to the action.

(5) Actions instituted against organs whose authority extends to the whole country shall come under the jurisdiction of the county (metropolitan) court. The local court located at the seat of the county court shall act in matters coming under the jurisdiction of the local court, while the Central District Court of Pest shall act in Budapest. The competence of the court shall be established by the head office (place of operation) of the organ which failed to perform the disclosure of data.

(6) The court shall act in priority procedure.

(7) If the court sustains the application, it shall oblige the data handling organ to disclose the requested data of public interest in its decision. Section 22

The provisions of this Chapter may not apply to the data supplied from the authentic register, regulated in a separate Act.

## **Chapter IV**

# **DATA PROTECTION COMMISSIONER AND DATA PROTECTION REGISTER**

## **Data Protection Commissioner**

### **Section 23**

(1) In the interest of the protection of the constitutional right attached to the protection of personal data and to the publicity of data of public interest, Parliament shall elect a data protection commissioner from among Hungarian citizens with university degree, clean criminal record, outstanding knowledge, theoretical experience or at least 10-year professional practice, with considerable experience in conducting proceedings affecting data protection, as well as the supervision or scientific theory thereof, and are held in high public esteem.

(2) With the differences contained in this Act, the provisions of the Act on the Parliamentary Commissioner for Citizens' Rights shall apply to the data protection commissioner.

### **Section 24**

The data protection commissioner shall

- a) control the observance of the Act and other legal rules applicable to data handling;
- b) examine the reports submitted to him;



c) provide for keeping the data protection register.

## **Section 25**

(1) The data protection commissioner shall monitor the conditions of the enforcement of the protection of personal data and the publicity of the data of public interest. He shall make a proposal for creating and amending the legal rules affecting data handling and the publicity of the data of public interest, and shall express opinion on the draft of such legal rules. He may initiate the narrowing or widening of the types of data defined within the sphere of state secrets and service secrets.

(2) In the case of noticing unlawful data handling, the data protection commissioner shall request the data handler to terminate data handling. The data handler shall take the necessary measures without delay, and shall notify the data protection commissioner thereof, in writing, within 30 days.

(3) If the data handler does not terminate unlawful data handling, the data protection commissioner shall inform the public of the fact of data handling, the person of the data handler and the sphere of the data handled.

## **Section 26**

(1) In the course of fulfilling his duties, the data protection commissioner may request information from data handlers in respect of all issues, may have access to all documents and may acquaint himself with instances of data handling which may be in connection with personal data or the of public interest.

(2) The data protection commissioner may enter all premises where data handling is carried out.

(3) State secrets and service secrets may not prevent the data protection commissioner from exercising his rights regulated in this Section, but the provisions relating to keeping the secret shall also be binding on him. In cases of data handling affecting state secrets or service secrets, the data protection commissioner may only exercise his rights at the armed forces, the police, and the national security organs in person.

(4) If in the course of his activities, the data protection commissioner considers the qualification of certain data unjustified, he shall request the qualifying party to change them, or to terminate the qualification. The qualifying party may appeal to the Metropolitan Court within 30 days in order to establish the unfounded nature of the request. The court shall act in the matter in priority proceedings, at a closed hearing.

## **Section 27**

(1) Anybody may contact the data protection commissioner if, in his opinion, he suffered injury in connection with the handling of his personal data or the exercising of his rights of access to data of public interest, or if a direct danger thereof exists, unless the given matter is sub judice at the time.

(2) Nobody may suffer disadvantage as a result of his report to the data protection commissioner. The reporting party shall be given the same protection as those making reports of public interest.

# **Data Protection Register**

## **Section 28**

(1) Prior to commencing this activity, the data handler shall report the following to the data protection commissioner for the purpose of registration:

- a) purpose of data handling;
- b) types of data and legal grounds of their handling;
- c) sphere of persons concerned;
- d) sources of data;
- e) types and addressees of the data forwarded, and legal grounds of forwarding;
- f) deadline for deleting each type of data;
- g) name and address (head office) of the data handler, as well as the place of actual data handling.

(2) Data handling ordered by a legal rule shall be announced by the Minister or the head of an organ with nationwide competence, and/or by the mayor, Lord Mayor or the Chairman of the County General Assembly, competent according to the subject of the regulation within 15 days following the coming into force of the legal rule.

(3) The national security organs shall announce the purposes and legal grounds of their data handling.

## **Section 29**

(1) A registration number shall be issued to the data handler at the time of first registration. The registration number shall be indicated in each case when data are forwarded, published or issued to the person concerned.

(2) Any changes in the data specified in Section 28, subsection (1) shall be reported to the data protection commissioner within 8 days and the register shall be amended accordingly.

## **Section 30**

The data handling which

- a) contains the data of persons maintaining employment, membership, students' or clients' legal relationship with the data handler;
- b) is effected in accordance with the internal rules of churches, religious denominations and religious communities;
- c) contains personal data relating to the illness or health condition of persons treated within the framework of health provision, for the purpose of medical treatment, health preservation, or the enforcement of a social insurance claim;
- d) contains data aimed at and recording the financial and other social support of the person concerned;

e) contains the personal data of persons affected by authority's, prosecutor's or court proceedings, relating to the conducting thereof;

f) contains personal data serving official statistics, provided that the establishment of the connection between the data and the given person is rendered definitively impossible, as defined in a separate Act;

g) contains such data of companies and organs coming under the scope of the Press Act which exclusively serve their own information activities;

h) serves the purposes of scientific research, if the data are not published;

i) was transferred to the archives from the data handler;

j) serves the own purposes of natural persons

do not have to be reported to the data protection register.

## **Data Protection Office**

### **Section 31**

## **Chapter V**

## **SPECIAL PROVISIONS**

### **Processing and Use of Personal Data in Research Institutes**

#### **Section 32**

(1) Personal data recorded or stored for the purpose of scientific research may only be used for the purpose of scientific research.

(2) Personal data, as soon as made possible by the purpose of the research, shall be rendered anonymous. Even until then, data which are suitable for the identification of defined or definable natural persons shall be stored separately. These data may only be connected with other data if it is required for the purpose of the research.

(3) Organs or persons carrying out scientific research may only publish personal data, if

a) the person concerned agreed thereto, or

b) it is required for presenting the results of research pursued in connection with historical events.

## **Chapter VI**

### **CLOSING PROVISIONS**

#### **Legal Rules to Be Amended**

##### **Section 33**

Coming into Force

##### **Section 34**

(1) This Act, with the exception contained in subsections (2) and (3), shall come into force on the first day of the 6th month following its promulgation.

(2) Chapter III (Sections 19 to 22) of the Act shall come into force on the 15th day following its promulgation.

(3) Chapter IV (Sections 23 to 31) of the Act shall come into force simultaneously with the coming into force of the Act on the Parliamentary Commissioner for Citizens' Rights.

##### **Section 35**

(1) Wherever this Act provides for regulation in an Act, with the exception of subsection (3), Section 4 and Section 13, subsection (1), preliminary work on legal regulation shall have been prepared by 31 December 1992.

(2) The legal directives related to data handling may not apply after the promulgation of this Act.

##### **Section 36**

(1) (repealed)

(2) Data handlers shall report the various instances of data handling existing at the time of the coming into force of this Act to the data protection register within 3 months following the election of the data protection commissioner.

##### **Section 37**

The Minister of Finance is hereby authorized to establish the fee referred to in Section 11, subsection (2), as well as the detailed rules applicable to the handling thereto, in a Decree.