

**on the
Protection of Personal Data and
Public Access to Data of Public Interest**

In accordance with the provisions of the Constitution of the Republic of Hungary, Parliament hereby passes the following Act on the fundamental rules governing the protection of personal data and the implementation of the right of access to data of public interest:

Chapter I

GENERAL PROVISIONS

Purpose of the Act

Article 1

(1) The purpose of this Act is to guarantee the right of everyone to exercise control over his or her personal data and to have access to data of public interest, except as otherwise provided by a rule of law under this Act.

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

(3) Exceptions under this Act shall be made only for specific types of data and specific data controllers together.

Scope of the Act

Article 1/A

(1) This Act shall apply to all data processing and technical data processing carried out in the territory of the Republic of Hungary that pertain to the data of natural persons or contain data of public interest or data public on grounds of public interest.

(2) This Act shall apply to the processing and technical processing of data carried out wholly or partially by automatic means, as well as to the manual processing and technical processing of data.

(3) This Act shall not apply to data processing carried out by natural persons exclusively for their own personal purposes.

Definitions

Article 2

For the purposes of this Act:

1. '*personal data*' shall mean any data relating to a specific (identified or identifiable) natural person (hereinafter referred to as 'data subject') as well as any conclusion with respect to the data subject which can be inferred from such data. In the course of data processing such data shall be considered to remain personal as long as their relation to the data subject can be restored. An identifiable person is in particular one who can be identified, directly or indirectly, by reference to his name, identification code or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

2. '*special data*' shall mean any personal data relating to

- a) racial, or national or ethnic minority origin, political opinion or party affiliation, religious or ideological belief, or membership in any interest representing organisation;
- b) state of health, pathological addictions, sexual life or criminal personal data;

3. '*criminal personal data*' shall mean any personal data which originated – during criminal proceedings or prior to such proceedings in connection with the criminal offence or the criminal proceedings – by the organs authorised to conduct criminal proceedings or to investigate criminal offences or by the penal authorities and which can be related to the data subject, as well as personal data relating to previous criminal convictions;

4. '*data of public interest*' shall mean any information or knowledge, not falling under the definition of personal data, processed by an organ or person performing a state or local government function or other public function determined by a rule of law, or any information or knowledge pertaining to the activities thereof, recorded in any way or any form, irrespective of the manner it is processed and its independent or collected character;

5. '*data public on grounds of public interest*' shall mean any data, not falling under the definition of data of public interest, the making public or accessibility of which is provided for by an Act on grounds of public interest;

6. '*consent*' shall mean any freely given, specific and informed indication of the wish of the data subject by which he signifies his unmistakable agreement to the processing, either wholly or partially, of personal data relating to him.

7. '*objection*' shall mean the statement of the data subject by which he objects to the processing of his personal data and requests termination of the data processing and/or deletion of the processed data;

8. '*data controller*' shall mean any natural or legal person or any organisation without legal personality that determines the purpose of the processing of data, makes decisions on data processing (including those as to the means of the processing) and implements these decisions or has them implemented by the technical data processor he has commissioned;

9. '*data processing*' shall mean any operation or set of operations which is performed upon data, irrespective of the applied procedure, such as collection, obtaining, recording, organisation, storage, alteration, use, transfer, making public, alignment or combination, blocking, deletion or destruction, as well as the barring of their further use. Photographing, sound or image recording, as well as the recording of physical characteristics suitable for personal identification (such as fingerprints, and palm prints, DNA samples and iris images) shall also be considered as data processing;

10. '*data transfer*' shall mean making data accessible for a specific third party;

11. '*making public*' shall mean making data accessible to any person;

12. '*deletion of data*' shall mean making data unrecognisable in such a way that they are not possible to restore any more;

13. '*blocking of data*' shall mean the making it impossible, for a definite period of time or finally, to transfer, access, make public, adapt, alter, destroy, delete, align or combine, or use the data;

14. '*destruction of data*' shall mean the complete physical destruction of data or of the data carrier containing them;

15. '*technical data processing*' shall mean the performance of technical tasks related to data processing operations, regardless of the methods or means employed or of the place of application;

16. *'technical data processor'* shall mean any natural or legal person or organisation without legal personality that carries out the technical processing of personal data, either on commission by the data controller or pursuant to a rule of law;

17. *'personal data filing system' ('filing system')* shall mean any structured file of personal data, whether centralised, decentralised or dispersed on a functional or geographical basis, that is accessible according to specific criteria;

18. *'data file'* shall mean the totality of data processed in a filing system;

19. *'third person'* shall mean any natural or legal person or organisation without legal personality, other than the data subject, the data controller or the technical data processor;

20. *'third country'* shall mean any country that is not a member of the European Economic Area.

Chapter II

PROTECTION OF PERSONAL DATA

Data Processing

Article 3

(1) Personal data shall not be processed unless

a) the data subject has given his consent; or
b) ordered by an Act, or – based on authorisation conferred by an Act, and within the range of data specified therein – ordered by a local government decree.

(2) Special data shall not be processed unless

a) the data subject has given his written consent; or
b) regarding data set out in point a) of paragraph (2) of Article 2, an international agreement prescribes it or it is ordered by an Act, either in order to enforce a fundamental right provided for in the Constitution or in the interest of national security, crime prevention or criminal investigation; or
c) ordered by an Act in other cases.

(3) Where data processing is obligatory, the purpose and conditions of data processing, the range and accessibility of data to be processed, the duration, as well as the person of the data controller shall be determined by the Act or local government decree ordering the data processing.

(4) On grounds of public interest, an Act may order the making public of an explicitly defined range of personal data. In all other cases data may not be made public without the consent, in the case of special data without the written consent, of the data subject. In cases of doubt it shall be presumed that the data subject has not given his consent.

(5) The data subject shall be presumed to have given his consent in the case of data communicated by him in the course of his public appearances or handed over by him for making them public.

(6) In proceedings commenced at the request of the data subject he shall be presumed to have given his consent to the processing of his data necessary therefor. The data subject's attention shall be drawn to this fact.

(7) For the performance of tasks determined in a contract, the data subject may give his consent in the contract concluded in writing with the data controller. In this case the contract shall contain all the information on the processing of personal data the data subject must be aware of under this Act, especially the range of data to be processed, the duration of data processing, the purpose of utilisation, the transfer of data and, the employment of the services of a technical data processor. The contract shall contain explicitly that the data subject consents, by signing the document, to the processing of his data as set out in the contract.

(8) If the data subject, due to physical causes or his physical incapacity to act, is unable to give his consent to the processing of his data, his personal data, including special data, may be processed, to the extent necessary, in order to protect the vital interests of the data subject or of another person, or in order to avert or prevent a catastrophe or emergency.

Article 4

Unless otherwise provided for by an Act, the right to the protection of personal data and the personality rights of the data subject may not be prejudiced by other data processing interests, including public access to data of public interest (Article 19).

Technical Data Processing

Article 4/A

(1) The rights and obligations of technical data processors in connection with the technical processing of personal data shall be determined by the data controller under this Act and other separate Acts regulating data processing. The data controller shall be responsible for the lawfulness of instructions given for data processing operations.

(2) The technical data processor shall be responsible, within his scope of activities and the framework determined by the data controller, for the technical processing, alteration, deletion, transfer and making public of personal data. In performing his tasks the technical data processor may not employ the services of other technical data processors.

(3) The technical data processor may not make any decisions in merit concerning data processing, shall technically process the personal data entrusted to him exclusively as instructed by the data controller, may not technically process data for his own purposes, and shall store and preserve personal data according to the instructions of the data controller.

(4) Contracts commissioning technical data processing shall be concluded in writing. Companies interested in business activities using the personal data to be technically processed may not be commissioned to technically process data.

(5) [repealed]

(6) The provisions of this Act shall apply where a data controller performing the processing of personal data outside the territory of the European Union commissions, for the technical processing of data, a technical data processor having his seat or premises (branch) or residence (place of sojourn) in the territory of the Republic of Hungary, or uses equipment in this country, except when the equipment is solely used for the transit of data through the territory of the European Union. Such data controllers shall appoint a representative in the territory of the Republic of Hungary.

Purpose-bound Nature of Data Processing

Article 5

(1) Personal data shall be processed only for a specified purpose, in order to exercise a right or perform an obligation. This purpose shall be complied with in all phases of the data processing.

(2) No personal data shall be processed unless indispensable and suitable for the achievement of the purpose of the data processing, and only to the extent and for the duration necessary to achieve that purpose.

(3) Data processing based on compulsory supply of information may be ordered on grounds of public interest.

(4) Personal data may be processed – either with the data subject’s consent or when ordered by a rule of law – in particular where it is necessary for the performance of a task of public interest, for the data controller to perform his obligations prescribed by an Act, for the data controller or data recipient third person to perform their official duties, for the protection of the vital interests of the data subject, for the meeting of the obligations laid down in the contract between the data subject and the data controller, for the assertion of a legitimate interest of the data controller or a third person, or for the lawful operation of social organisations.

(5) Criminal personal data for the purpose of performing the State’s tasks of criminal investigation, crime prevention, as well as public administration and judicial tasks, and data files pertaining to minor offences, civil lawsuits and non-litigious cases may only be processed by state or local government organs.

Article 6

(1) Prior to the collection of data the data subject shall be informed whether it is voluntary or compulsory to supply the data. In cases of compulsory supply the rule of law ordering data processing shall also be indicated.

(2) The data subject shall be given unambiguous and detailed information on all the facts relating to the processing of his data, in particular on the purposes and legal basis of the data processing, on the person authorised to carry out the data processing and the technical data processing, the duration of data processing, as well as on who is authorised to have access to the data. Information shall also be given on the rights and remedies of data subjects in connection with the data processing.

(3) The information on data processing shall be considered to have been given where a rule of law orders the collection of data from an existing data file by transfer or combination.

(4) If it is impossible to inform each data subject or if it would entail disproportionate expenses, particularly in the case of processing data for statistical or scientific (including historical research) purposes, information may be given by making public, in a way that it will be accessible to all, the fact of data collection, the data subjects concerned, the purpose of the data collection, the duration of the data processing, and the accessibility of the data.

Quality of Data

Article 7

(1) Personal data undergoing processing shall be:

- a) obtained and processed fairly and lawfully,
- b) accurate, complete and, where necessary, kept up to date,
- c) stored in a way that allows identification of data subjects for no longer than it is required for the purpose for which these data are stored.

(2) The application of general and uniform personal identification codes which can be used without restriction shall be prohibited.

Data Transfer and Combination of Data Processing Operations

Article 8

(1) Personal data shall not be transferred and data processing operations shall not be combined unless consented to by the data subject or provided for by an Act, and unless the conditions for data processing are met with regard to each personal datum.

(2) Paragraph (1) shall apply to the combination of data processing operations by the same data controller, or by state or local government organs.

Data Transfer to Foreign Countries

Article 9

(1) Regardless of the data carrier or the way of the data transfer, personal data (including special data) shall not be transferred to data controllers or technical data processors in third countries unless:

- a) the data subject has given his explicit consent, or
- b) provided for by an Act and the adequate level of protection of the personal data in the third country is ensured during the processing or technical processing of the transferred data.

(2) The adequate level of protection of personal data is not ensured unless

- a) the Commission of the European Communities on the basis of a legal act determined by a separate Act recognizes that the third country ensures adequate level of protection,
- b) there is an international agreement in force between the third country and the Republic of Hungary including safeguard regulations on the enforcement right of data subjects arising from Article 11, on securing the right of legal remedy and on the independent control of data processing and technical data processing, or
- c) the data controller or technical data processor in the third country proves by introducing the rules of data processing and technical data processing, that the protection of personal data is adequately ensured during the data processing and technical data processing, in particular when he performs the data processing or technical data processing according to the legal act of the Commission of the European Union as determined by a separate Act.

(3) Personal data shall be transferred into third countries in order to implement an international legal assistance agreement for the purpose and with the content laid down in the agreement.

(4) Data transfer to Member States of the European Economic Area shall be considered as data transfer within the territory of the Republic of Hungary.

Automated Individual Decisions

Article 9/A

(1) No evaluation of the personal characteristics of data subjects shall be carried out by automated technical data processing performed exclusively with information technology equipment without the express consent of the data subject or unless provided for by an Act. The data subject shall be given the opportunity to state his point of view.

(2) In the case of automated technical data processing the data subject shall be informed, upon his request, of the applied mathematical method and its essentials.

Data Security

Article 10

(1) The data controller and, within its scope of activities the technical data processor, shall ensure data security and shall take all technical and organisational measures and elaborate the rules of procedure necessary to enforce compliance with this Act and other rules pertaining to data protection and confidentiality.

(2) Data shall be protected in particular against unauthorised access, alteration, transfer, making public, deletion or destruction, as well as against accidental destruction or damage. If personal data are transferred via a network or other information technology equipment, the data controller, technical data processor and the operator of the telecommunications or information technology equipment shall take special protective measures to ensure the technical protection of personal data.

The Data Subject's Rights and their Enforcement

Article 11

(1) The data subject may request

a) information on the processing of his personal data (Articles 12 and 13); as well as

b) the rectification, or – except for data processing ordered by a rule of law – deletion of his personal data (Articles 14 to 16).

(2) Anyone may inspect the Data Protection Register (paragraph (1) of Article 28), and may take notes or request extracts thereof. A fee shall be paid for the extracts.

Article 12

(1) The data controller shall inform the data subject, upon his request, of the data processed by the data controller or technically processed by the technical data processor, of the purpose of the data processing, of its legal basis and duration, of the name, address (seat) and activity of the technical data processor in connection with the data processing, as well as of those who received or will receive data and for what purpose. The duration of records on transfer and, on the basis thereof the obligation to give information, may be limited by rules of law on data processing. The limitation may not be shorter than five years with regard to personal data, or twenty years with regard to special data.

(2) The data controller shall give the information in writing and in an easy to understand way, within the shortest possible time, but not later than within 30 days, of the lodging of the request.

(3) The information referred to in paragraph (2) is free of charge, unless in the given calendar year the person requesting information has already filed a request with the data controller for the same field. In other cases expenses may be charged. Such expenses shall be refunded where the data have been unlawfully processed or where the request for information has resulted in rectification.

Article 13

(1) The data controller shall not deny data subjects the information except where, in cases specified in Article 16, an Act authorises him to do so.

(2) The data subject shall be informed by the data controller of the grounds for the denial of information.

(3) The data controller shall annually report on requests which have been refused to the Parliamentary Commissioner of Data Protection.

Article 14

(1) The data controller shall be bound to rectify any inaccurate personal data.

(2) Personal data shall be deleted if

- a) the processing thereof is unlawful;
- b) requested so by the data subject in accordance with point b) of paragraph (1) of Article 11;
- c) they are incomplete or inaccurate and they can not be corrected in a lawful way, provided that deletion is not precluded by an Act;
- d) the purpose of processing has ceased to exist, or the time limit for the storage of data, as specified in an Act, has expired;
- e) it has been ordered by the court or the Data Protection Commissioner.

(3) Except in cases of unlawful data processing, such obligation to delete shall not apply to personal data the data carrier of which is to be deposited in the archives according to the rule of law regulating the protection of archive materials.

Article 15

The data subject and those to whom the data were previously transferred for processing shall be informed of any rectification or deletion. Such information may be dispensed with if, in view of the purpose of processing, no legitimate interests of the data subject are infringed thereby.

Article 16

The rights of the data subject (Articles 11 to 15) may be restricted by an Act in the interest of the external and internal security of the State, such as national defence, national security, crime prevention or criminal investigation, for the economic or financial interests of the State or the local government, for important economic or financial interests of the European Union, for the prevention or exposure (including in all cases supervision and control) of professional disciplinary or ethical offences or of breaches of labour law or labour safety obligations, as well as for the protection of the rights of data subjects or of other people.

The Right to Object

Article 16/A

(1) The data subject may object to the processing of his data if

- a) the processing (transfer) of personal data is necessary solely for enforcing a right or legitimate interest of the data controller or data recipient, except if the data processing has been ordered by an Act;
- b) personal data are used or transferred for the purposes of direct marketing, public opinion polling or scientific research;
- c) the exercise of the right to object is otherwise made possible by an Act.

(2) The data controller shall investigate the objection, and at the same time suspend the data processing, within the shortest time, but not later than 15 days, of the lodging of the request, and inform the applicant in writing of the results thereof. Where the objection is justified, the data controller shall discontinue the processing of data, including further collection or transfer, and block all data, and he shall inform of the objection and the measures taken on the basis thereof all those to whom the personal data the objection aimed at were previously transferred,

and who, on their part, shall take the necessary measures for the enforcement of the right to object.

(3) If the data subject does not agree with the decision taken by the data controller under paragraph (2), he may institute court proceedings under this Act, within 30 days of being notified thereof.

(4) If, due to the data subject's objection, the data recipient fails to receive the data necessary for the enforcement of his statutory rights, in order to have access to the data he may institute court proceedings under this Act against the data controller within 15 days of the notification referred to in paragraph (2). The data controller may give third party notice to the data subject as well.

(5) If the court turns down the application of the data recipient, the data controller shall delete the data subject's personal data within 3 days of notification of the judgement. The data controller shall delete the data even if the recipient fails to institute court proceedings within the time limit laid down in paragraph (4).

(6) The data controller may not delete the data of the data subject, if the data processing has been ordered by an Act. The data, however, may not be transferred to the recipient, if the data controller agrees with the objection or if the court has found the objection justified.

Judicial Enforcement of Rights

Article 17

(1) In case of infringement of his rights the data subject, or the person specified in paragraph (4) of Article 16/A, may institute court proceedings against the data controller. The court shall hear the case out of turn.

(2) The burden of proof that the data processing has been in compliance with the pertaining rules of law shall lie with the data controller.

(3) The court according to the seat (residence) of the data controller shall have competence to hear the case. At the data subject's discretion the action may also be instituted by the court competent according to the residence (place of sojourn) of the data subject. A person otherwise legally incapable of suing or being sued may also be a party to the lawsuit.

(4) If the application is granted by the court, it shall order the data controller to provide the requested information, to rectify or delete the data involved, to annul the automated individual decision, to take account of the data subject's right to object, or to supply the data requested by the person specified in paragraph (4) of Article 16/A.

(5) Where necessitated by the interests of data protection and the rights of a large number of data subjects protected by this Act, the court may order the making public of its judgement together with the publication of the identification data of the data controller.

Compensation for Damages

Article 18

(1) The data controller shall be liable for any damage suffered by data subjects as a result of an unlawful processing of their data or as a result of an infringement of the technical requirements of data protection. The data controller shall also be liable for any damage suffered by the data subject resulting from the actions of a technical data processor. The data controller shall be exempted from liability if he proves that the damage was the result of *force majeure* beyond the sphere of data processing.

(2) No compensation shall be paid for the part of damage suffered by the damaged person as a result of his intentional or grossly negligent conduct.

Chapter III

PUBLIC ACCESS TO DATA OF PUBLIC INTEREST

Article 19

(1) The organ or person (hereinafter referred to collectively as 'organ') performing state or local government function, or other public function determined by a rule of law shall promote and ensure the accurate and prompt information of the general public concerning matters within its sphere of tasks, in particular concerning the state and local government budgets and their implementation, the management of state and local government assets, the utilisation of public funds and contracts involving the same, as well as concerning the granting of special or exclusive rights to market operators, private organisations and private persons.

(2) The organs laid down in paragraph (1) shall regularly electronically or otherwise publish or in case of a claim aimed at this enable access to the most important data pertaining to their activities, in particular to their powers, competence, structure, professional activities including the evaluation of the effectiveness thereof, the categories of data possessed by them, the rules of law governing their operation, and to their management according to the provisions of Article 20. A rule of law may determine the way of the information and the scope of the related data.

(3) The organs mentioned in paragraph (1) shall grant access for anyone to the data of public interest processed by them, except for those data which are classified as state or service secret by organs authorized to do so under an Act, or for data classified on grounds of an obligation resulting from an international agreement, or furthermore except, if the right to public access to specified categories of data of public interest is not restricted by an Act in the interest of

- a) national defence,
- b) national security,
- c) criminal investigation and crime prevention,
- d) financial or foreign exchange policy of the State,
- e) international relations and relations to international organisations,
- f) judicial and administrative authoritative proceedings.

(4) Unless otherwise provided for by an Act, personal data relating to the sphere of tasks of a person exercising the sphere of tasks and powers of organs laid down in paragraph (1), furthermore the personal data relating to the sphere of tasks of a person performing public function shall be regarded as data public on grounds of public interest. The provisions on access to data of public interest of this Act shall apply to the access to these data.

(5) Unless otherwise provided for by an Act, data not falling under the definition of personal data, which data are processed by organs or persons providing mandatory services or services which otherwise cannot be provided on the basis of a rule of law or a contract entered into with an organ performing state or local government function or any data pertaining to the activities thereof shall be regarded as data public on grounds of public interest.

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

(7) Public access to data of public interest may further be restricted by European Union legislation with a view to important financial or economic interests of the European Union, including monetary, budgetary and fiscal interests.

Article 19/A

(1) The data prepared or recorded, on which the decision was made during the process aiming at decision making in the field of the sphere of tasks and powers of the organs laid down in paragraph (1) of Article 19 shall not be public until 10 years of their creation. The head of the organ processing the data may permit access to these data taking into account paragraph (1) of Article 19.

(2) The claim for the access to data upon which the decision was made can be refused following the decision making within the period given in paragraph (1), when the access to data would endanger the lawful operational order or the performance of the sphere of tasks and powers void of unauthorized external influence of the organ thus particularly the free publishing of the standpoint creating the data during the preparation of the decisions.

(3) Regarding the limitation for the access of some data shorter period than the one determined by paragraph (1) may be ruled for by a rule of law.

Article 20

(1) Anyone may claim the access to data of public interest either orally, in writing or electronically.

(2) The claim shall be granted by the organ processing the data, as soon as possible after being notified of the claim, but at the latest within 15 days.

(3) A copy of the document or a part of it containing the data regardless of the manner of its storage may be provided to the claimant. The data processing organ may charge expenses, up to the actual extent thereof, for the preparation of the copy. Upon his request the claimant shall be informed in advance about the amount of expenses.

(4) If the document containing data of public interest contains data not accessible by the claimant, such data shall be made unrecognizable.

(5) The claim shall be granted in an easy to understand way and by a technical device or way required by the claimant if this does not entail disproportionate expenses. The claim for access cannot be refused by reference thereto that the application cannot be granted in an easy to understand way.

(6) The claimant shall be notified in writing or electronically, if the claimant has disclosed his electronic mailing address in the claim, within 8 days, of the refusal of his claim and of the reasons therefor.

(7) The claim for access to data of public interest shall not be refused because the claimant, whose mother tongue is a language other than Hungarian, drafted his claim in his mother tongue or in another language spoken by him.

(8) The organs performing a state or local government function or other public function determined by a rule of law shall prepare a regulation establishing the order of fulfilment of claims for access to data of public interest.

(9) The organs laid down in paragraph (1) of Article 19 shall annually report to the Data Protection Commissioner on the claims refused and the reasons therefor.

Article 21

(1) The claimant may institute court proceedings if his demand for data of public interest is refused.

(2) The burden of proof that the refusal was lawful and well-founded shall lie with the data processing organ.

(3) The court proceedings shall be instituted, within 30 days from the notification of refusal or in case of its absence from the lapse of the period specified in paragraph (2) of Article 20 without any result, against the organ which refused the requested information.

(4) A person otherwise legally incapable of suing or being sued may also be a party to the lawsuit.

(5) A legal action against an organ with nation-wide competence shall belong to the competence of the county (Metropolitan) court. Cases within the competence of local courts shall be decided by the local court at the seat of the county court or by the Central District Court of Pest in Budapest. The seat (place of business) of the organ refusing to disclose the data shall determine the court competent to hear the case.

(6) The court shall conduct the proceedings out of turn.

(7) If the application is granted by the court, it shall order the organ to disclose the requested data of public interest.

Article 21/A

(1) Organs specified in paragraph (1) of Article 19 shall not make access to disclosed data subject to the disclosure of personal identification data. Personal data may only be processed for ensuring access to data of public interest disclosed in electronic way if it is technically indispensable, personal data shall be deleted afterwards without delay.

(2) In case of data supply on demand the personal identification data of the applicant may only be processed if it is indispensable for fulfilling the demand – including the payment of probable costs. Following the fulfilment of the demand and the payment of the costs personal data of the applicant shall be deleted without delay.

(3) Different provisions from the ones in paragraphs (1) and (2) may be provided for by Act.

Article 22

The provisions of this Chapter shall not apply to the supply of data from authentic records which are regulated by a separate Act.

Chapter IV

THE DATA PROTECTION COMMISSIONER AND THE DATA PROTECTION REGISTER

The Data Protection Commissioner

Article 23

(1) In order to safeguard the constitutional right to the protection of personal data and to public access to data of public interest, Parliament shall elect a Data Protection Commissioner from among Hungarian citizens with a university degree, a clean criminal record and an outstanding academic knowledge or at least 10 years of professional practice, who are widely esteemed persons with significant experience either in conducting or supervising proceedings involving data protection or in the scientific theory thereof.

(2) Subject to the derogations laid down by this Act, the provisions of the Act on the Parliamentary Commissioner for Civil Rights shall apply to the Data Protection Commissioner.

Article 24

The Data Protection Commissioner

- a) shall supervise compliance with this Act and other rules of law on data processing on notice or – if there is no judicial proceeding pending concerning the case in question – ex officio;
- b) shall investigate complaints lodged with him;
- c) shall ensure the maintenance of the data protection register;
- d) shall promote a uniform application of statutory provisions on the processing of personal data and on public access to data of public interest; and
- e) may issue a recommendation within his sphere of tasks generally or for a specific data controller;
- f) shall practise the right to form opinion in connection with the activity of an organ performing state or local government function, or other public function determined by a rule of law considering special and individual publication lists regarding data to be disclosed according to the provisions of a separate Act;
- g) shall represent the Republic of Hungary, co-operating with organs and persons specified in a separate Act, in joint data protection supervisory authorities of the European Union;
- h) shall exercise the powers and perform the tasks as laid down in this Act.

Article 24/A

(1) Provisions of Act LIX. of 1993 on the Parliamentary Commissioner for Civil Rights (hereinafter referred to as 'Act on Ombudsman') shall be applied with differences specified in this Act to the procedure and measures of the Data Protection Commissioner.

(2) Paragraphs (1) and (2) of Article 16, paragraphs (3) and (4) of Article 17, paragraphs (1), (6) and (8) of Article 18 of the Act on Ombudsman shall not be applicable to the procedure of the Data Protection Commissioner.

Article 25

(1) The Data Protection Commissioner shall monitor the conditions of the protection of personal data and of the realisation of public access to data of public interest and data public on grounds of public interest. He shall make proposals for the adoption or amendment of legislation on data processing or on public access to data of public interest and data public on grounds of public interest, and give an opinion on such draft legislation. He may initiate a narrowing or broadening of data categories classified as state or service secrets.

(2) Upon observing any unlawful processing of data, the Data Protection Commissioner shall call on the data controller to discontinue the data processing. The data controller shall take the necessary measures without delay and inform in writing the Data Protection Commissioner thereof within 30 days.

(3) The Data Protection Commissioner may inform the public of the launching of his investigation, of the fact of the unlawful processing (technical processing) of data, of the person of the data controller (technical data processor) and of the range of processed data, as well as of the measures initiated and decisions made by him.

(4) If the data controller or technical data processor fails to discontinue the unlawful processing (technical processing) of personal data, the Data Protection Commissioner may order in a decision the blocking, deletion or destruction of unlawfully processed data, prohibit the unlawful processing or technical processing of data, and suspend the transfer of data to foreign countries. The decision may not be remedied in administrative way.

(5) The data controller, the technical data processor or the data subject may request judicial review from the court against the decision of the Data Protection Commissioner pursuant to paragraph (4) – within 30 days after its receipt – on the grounds of infringement. The Court shall

proceed according to the regulations on lawsuits against public administration of the Civil Procedure Act. Until a final court decision the data concerned may not be deleted or destroyed; the processing of data, however, shall be suspended and the data shall be blocked.

Article 26

(1) In performing his tasks the Data Protection Commissioner may request the data controller to supply information on any question that might be related to personal data, data of public interest or data public on grounds of public interest, and he may inspect all such documents and request a copy of and have access to all such data processing operations.

(2) The Data Protection Commissioner may enter any premises where data are processed.

(3) The data controller shall reply to the recommendation issued to him on the merits within thirty days.

(4) State and service secrets shall not prevent the Data Protection Commissioner from exercising his rights laid down in this Article, but the provisions on confidentiality shall be binding on him as well. In cases of data processing involving state or service secrets the Data Protection Commissioner shall exercise his rights in person or through members of his staff who passed the national security screening initiated by him.

(5) If in the course of his proceedings the Data Protection Commissioner finds the classification of certain data – excepting those classified so under an international agreement – unjustified, he shall call on the person or organ by whom they were classified to change or terminate the classification. The classifier may, within 30 days, go to the Metropolitan Court of Justice to have it established that the demand has not been well-founded. The Court shall conduct its proceedings in camera and out of turn.

Article 27

(1) Anyone may report to the Data Protection Commissioner if he thinks his rights have been violated, or that there is an imminent danger thereof, in connection with the processing of his personal data or with the exercise of his right to have access to data of public interest or data public on grounds of public interest, except when judicial proceedings are already pending concerning the case in question.

(2) No one shall suffer any prejudice on grounds of his reporting to the Data Protection Commissioner. The person having made the report shall enjoy the same protection as persons making reports of public interest.

The Data Protection Register

Article 28

(1) Prior to commencing his activity, the data controller processing personal data shall notify the Data Protection Commissioner of the following to be registered:

- a) the purpose of the data processing;
- b) the data categories and the legal basis for the processing thereof;
- c) the range of data subjects;
- d) the source of data;
- e) the categories and recipients of transferred data, and the legal basis of the transfer;
- f) the time limits for the deletion of certain types of data;
- g) the name and address (seat) of the data controller and of the technical data processor, the actual place of data processing or technical data processing, as well as any activity of the technical data processor related to the processing of data; and
- h) the name and contact information of the internal data protection officer.

(2) Data processing ordered by a rule of law shall be reported within 15 days of the entry into force of the relevant legislation by the minister or the head of the national organ competent according to the field regulated therein, or by the mayor, Lord Mayor, or president of the county assembly.

(3) National security organs shall report the purpose and legal basis of data processing carried out by them.

Article 29

(1) Upon registration for the first time, each data controller shall receive a registration number. This registration number shall be indicated whenever data are transferred, made public or supplied to the data subject.

(2) Any change in data specified in paragraph (1) of Article 28 shall be reported to the Data Protection Commissioner within 8 days, and the register shall be modified accordingly.

Article 30

Registration in the data protection register shall not be required where data processing operations

- a) involve the data of persons having an employment, membership, student or customer relationship with the data controller;
- b) are governed by the internal rules of churches, religious denominations or religious communities;
- c) involve personal data relating to the diseases or state of health of persons receiving medical care, for purposes of medical treatment or preservation of health or for social insurance claims;
- d) involve data collected with the purpose of granting financial or other social assistance to the data subject or data registering such assistance;
- e) involve personal data of persons concerned by administrative, prosecutorial or judicial proceedings that are related to the conducting of such proceedings;
- f) involve personal data for the purpose of official statistics, provided that the identification of individuals with such data can be finally made impossible in a manner specified by the provisions of a separate Act;
- g) involve data of companies or organs under the Press Law that serve solely their own informational activity;
- h) serve the purposes of scientific research, provided that the data are not made public;
- i) were transferred from the data controller to the archives; or
- j) serve a natural person's own purposes.

Prior Checking

Article 31

(1) The Data Protection Commissioner may perform prior checking before registration.

(2) The Data Protection Commissioner may perform prior checking before the technical processing of new data files or the application of new technical data processing technologies at data controllers processing the following:

- a) data files of national authorities, or national labour or criminal data files;
- b) customer files of financial organisations or public utility providers;
- c) files of telecommunications service providers relating to the users of their services; or
- d) data files containing specific statistical data specified in a separate Act.

(3) The data controller shall notify the Data Protection Commissioner of his intention to technically process new data files or to apply a new technical data processing technology 30

days prior to commencing such activities. The Data Protection Commissioner shall inform, within 8 days of receiving the above notification, the data controller of his intention to perform prior checking, and shall carry out the checking within 30 days. The data controller shall not start to technically process the data until the Data Protection Commissioner has completed his prior checking.

(4) On the basis of the checking the Data Protection Commissioner may call on the data controller to change the range of data to be processed or the method of technical data processing. If the Data Protection Commissioner objects to the rule of law ordering the data processing, he may issue a recommendation for the amendment of that rule of law.

The Internal Data Protection Officer and the Data Protection Rules

Article 31/A

(1) An internal data protection officer holding a higher education degree in law, public administration or information technology, or a qualification equivalent thereto, shall be appointed or commissioned within the organisation of the data controller or of the technical data processor and he shall report directly to the head of the following organs:

- a) data controllers or technical data processors performing the processing or technical processing of data files of national authorities, or of national labour or criminal data files;
- b) financial organisations; and
- c) providers of telecommunications and public utility services.

(2) The internal data protection officer shall

- a) contribute to or assist in making decisions related to data processing and to the enforcement of the rights of data subjects;
- b) monitor compliance with this Act and other rules of law on data processing, as well as with the provisions of internal data protection and data security rules and with data security requirements;
- c) investigate reports submitted to him, and call on the data controller or technical data processor to discontinue any unlawful data processing observed by him;
- d) draw up the internal data protection and data security rules;
- e) maintain the internal data protection register; and
- f) ensure the training of the staff in data protection.

(3) In order to implement this Act, data controllers specified in paragraph (1) and state and local government data controllers – other than data controllers not required to give notification to the data protection register – shall be required to adopt data protection and data security rules.

Chapter V

SPECIAL PROVISIONS

Technical Processing and Use of Personal Data in Research Institutes

Article 32

(1) Data collected or stored for purposes of scientific research shall not be used for other purposes.

(2) Personal data shall be made anonymous as soon as the purpose of research allows it. Any data relating to identified or identifiable persons shall be stored separately from the very beginning. These data shall not be connected with other data unless this is required for the purpose of research.

(3) An organ or person performing scientific research shall not make personal data public, unless

- a) the data subject has given his consent thereto, or
- b) it is necessary for the presentation of the findings of research on historical events.

Use of Personal Data for Statistical Purposes

Article 32/A

(1) Personal data collected, received or technically processed for statistical purposes shall not be used for other purposes. Specific statistical data, including personal data, regulated by a separate Act shall not be transferred, received, technically processed except for archives research in compliance with the special Act, or made public in any way or on any legal grounds for other than statistical purposes.

(2) The detailed rules on the processing of personal data for statistical purposes shall be regulated by a separate Act.

Chapter VI

CLOSING PROVISIONS

Amendments to Other Acts

Article 33

[repealed]

Article 33/A

This Act shall serve for the compliance with Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Entry into Force

Article 34

(1) This Act – with the exception of the provisions contained in paragraphs (2) and (3) – shall enter into force on the 1st day of the sixth month following the date of its promulgation.

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

(3) Chapter IV (Articles 23 to 31) of this Act shall enter into force simultaneously with the entry into force of the Act on the Parliamentary Commissioner for Civil Rights.

Article 35

[repealed]

Article 36

(1) [repealed]

(2) [repealed]

Article 37

The Minister of Finance shall be authorised to determine the fee referred to in paragraph (2) of Article 11, as well as the detailed rules governing the administration thereof.