Act CXII of 2011

on the Right of Informational Self-Determination and on Freedom of Information[1]

In order to ensure the right of informational self-determination and the freedom of information, and to facilitate the implementation of the Fundamental Law, pursuant to Article VI of the Fundamental Law, the Parliament hereby adopts the following Act on the fundamental rules applicable in connection with the protection of personal data and the enforcement of the right to access and disseminate data of public interest and data public on grounds of public interest, and on the authority empowered to monitor compliance with these rules:

CHAPTER I

GENERAL PROVISIONS

1. Object of the Act

Section 1

The purpose of this Act is to lay down the fundamental rules for data processing activities with a view to ensuring that the right to privacy of natural persons is respected by data controllers , and to enforcing of rights to access and disseminate data of public interest and data public on grounds of public interest.

2. Scope

Section 2

(1) This Act shall apply to all data control and data processing activities undertaken in Hungary relating to the data of natural persons as well as data of public interest and data public on grounds of public interest.

(2) The present Act shall apply to both data processing and data process, carried out wholly or partly, by automated means as well as manually.

(3) Provisions set out in the present Act shall apply if the controller processing personal data outside the territory of the European Union contracts a data processor with a seat, site, branch or address or place of residence within the territory of Hungary to perform data processing, except if this device serves data traffic exclusively within the territory of the European Union. Such controllers are obliged to designate a representative in Hungary.

(4) Provisions set out in the present Act are not applicable to natural persons processing data exclusively for their own personal purposes.

(5) Concerning further use of public sector information, provisions in derogation from this Act may be established by another act concerning the procedures and conditions for the disclosure of data, the consideration payable therefore, and as regards remedies.

3. Definitions

Section 3

[1]Updated: 11-10-2013 by NAIH

For the purposes of this Act:

1. *'data subject' shall mean* any natural person directly or indirectly identifiable by reference to specific personal data;

2. *'personal data'* shall mean data relating to the data subject, in particular by reference to the name and identification number of the data subject or one or more factors specific to his physical, physiological, mental, economic, cultural or social identity as well as conclusions drawn from the data in regard to the data subject;

3. *'special data'* shall mean:

a) personal data revealing racial origin or nationality, political opinions and any affiliation with political parties, religious or philosophical beliefs or trade-union membership, and personal data concerning sex life,

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

4. *'criminal personal data' shall mean* personal data relating 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;

5. '*data of public interest'* shall mean information or data other than personal data, registered in any mode or form, controlled by the body or individual performing state or local government responsibilities, as well as other public tasks defined by legislation, concerning their activities or generated in the course of performing their public tasks, irrespective of the method or format in which it is recorded, its single or collective nature; in particular data concerning the scope of authority, competence, organisational structure, professional activities and the evaluation of such activities covering various aspects thereof, the type of data held and the regulations governing operations, as well as data concerning financial management and concluded contracts;

6. *'data public on grounds of public interest'* shall mean any data, other than public information, that are prescribed by law to be published, made available or otherwise disclosed for the benefit of the general public;

7. *'the data subject's consent'* shall mean any freely and expressly given specific and informed indication of the will of the data subject by which he signifies his agreement to personal data relating to him being processed fully or to the extent of specific operations;

8. *'the data subject's objection'* shall mean a declaration made by the data subject objecting to the processing of their personal data and requesting the termination of data processing, as well as the deletion of the data processed;

9. *'controller'* shall mean natural or legal person, or organisation without legal personality which alone or jointly with others determines the purposes and means of the processing of data; makes and executes decisions concerning data processing (including the means used) or have it executed by a data processor[2];

10. *'data' processing' shall mean* any operation or the totality of operations performed on the data, irrespective of the procedure applied; in particular, collecting, recording, registering, classifying, storing, modifying, using, querying, transferring, disclosing, synchronising or connecting, blocking, deleting and destructing the data, as well as preventing their further use, taking photos, making audio or visual recordings, as well as registering physical characteristics suitable for personal identification (such as fingerprints or palm prints, DNA samples, iris scans);

11. *'data transfer'* shall mean ensuring access to the data for a third party;

12. *'disclosure'* shall mean ensuring open access to the data;

---

[2] In effect as of 1st July 2013

13. *'data deletion'* shall mean making data unrecognisable in a way that it can never again be restored;

14. *'tagging data'* shall mean marking data with a special ID tag to differentiate it;

15. *'blocking of data'* shall mean marking data with a special ID tag to indefinitely or definitely restrict its further processing;

16. *'data destruction'* shall mean complete physical destruction of the data carrier recording the data;

17. *'data process'* shall mean performing technical tasks in connection with data processing operations, irrespective of the method and means used for executing the operations, as well as the place of execution, provided that the technical task is performed on the data;

18. *'data processor'* shall mean any natural or legal person or organisation without legal personality processing the data on the grounds of a contract, including contracts concluded pursuant to legislative provisions[3];

19. *'data source'* shall mean the body responsible for undertaking the public responsibility which generated the data of public interest that must be disclosed through electronic means, or during the course of operation in which this data was generated;

20. *'data disseminator* shall mean the body responsible for undertaking the public responsibility which uploads the data sent by the data source it has not published the data;

21. *'data set'* shall mean all data processed in a single file;

22. *'third party'* any natural or legal person, or organisation without legal personality other than the data subject, the data controller or the data processor;

23. *'EEA Member State'* any Member State of the European Union and any State which is party to the Agreement on the European Economic Area, as well as any State the nationals of which enjoy the same legal status as nationals of States which are parties to the Agreement on the European Economic Area, based on an international treaty concluded between the European Union and its Member States and a State which is not party to the Agreement on the European Economic Area;

24. *'third country'* any State that is not an EEA State.

CHAPTER II

PROTECTION OF PERSONAL DATA

4. Principles of data processing

Section 4

(1) Personal data may be processed only for specified and explicit purposes, where it is necessary for the exercising of certain rights and fulfilment of obligations. The purpose of processing must be satisfied in all stages of data processing operations; recording of personal data shall be done under the principle of lawfulness and fairness.

(2) The personal data processed must be essential for the purpose for which it was recorded, and it must be suitable to achieve that purpose. Personal data may be processed to the extent and for the duration necessary to achieve its purpose.

(3) In the course of data processing, the data in question shall be treated as personal as long as the data subject remains identifiable through it. The data subject shall - in particular - be considered identifiable if the data controller is in possession of the technical requirements which are necessary for identification.

---

[3] In effect as of 1st July 2013

(4) The accuracy and completeness, and - if deemed necessary in the light of the aim of processing - the up-to-dateness of the data must be provided for throughout the processing operation, and shall be kept in a way to permit identification of the data subject for no longer than is necessary for the purposes for which the data were recorded.

(5) Processing of personal data shall be deemed lawful and fair if, for the objective of ensuring the right to freedom of expression of the data subject, the person, wishing to find out the opinion of the data subject, calls on him/her at his domicile or place of residence provided that the data subject's personal data are processed in compliance with this Act and the contacting is not intended for business purposes. This contacting is not permitted to happen on legal holiday as determined by the Labour Code.[4]

5. Legal basis of data processing

Section 5

(1) Personal data may be processed under the following circumstances:

a) when the data subject has given his consent, or

b) when processing is necessary as decreed by law or by a local authority based on authorization conferred by law concerning specific data defined therein for the performance of a task carried out in the public interest (hereinafter referred to as "mandatory processing").

(2) Special data may be processed according to Section 6, and under the following circumstances:

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

b) when processing is necessary for the implementation of an international agreement promulgated by an act concerning the data under Point 3.*a)* of Section 3, or if prescribed by law in connection with the enforcement of fundamental rights afforded by the Fundamental Law, or for reasons of national security or national defence, or law enforcement purposes for the prevention or prosecution of criminal activities, or

c) when processing is necessary for the performance of a task carried out in the public interest concerning the data under Point 3.*b)* of Section 3.

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

(4) 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 misdemeanour cases, civil cases and non-contentious proceedings may only be processed by central or local government authorities.

Section 6

(1) Personal data may be processed also if obtaining the data subject's consent is impossible or it would give rise to disproportionate costs, and the processing of personal data is necessary:

a) for compliance with a legal obligation pertaining to the data controller, or

b) for the purposes of the legitimate interests pursued by the controller or by a third party, and enforcing these interests is considered proportionate to the limitation of the right for the protection of personal data.

---

[4] In effect as of 30th March 2013

(2) If the data subject is unable to give his consent on account of lacking legal capacity or for any other reason beyond his control, the processing of his personal data is allowed to the extent necessary and for the length of time such reasons persist, to protect the vital interests of the data subject or of another person, or in order to prevent or avert an imminent danger posing a threat to the lives, physical integrity or property of persons.

(3) The statement of consent of minors over the age of sixteen shall be considered valid without the permission or subsequent approval of their legal representative.

(4) Where processing under consent is necessary for the performance of a contract with the controller in writing, 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, the recipients and the use of a data processor. The contract must clearly indicate the data subject's signature and explicit consent for having his data processed as stipulated in the contract.

(5) Where personal data is recorded under the data subject's consent, the controller shall - unless otherwise provided for by law - be able to process the data recorded where this is necessary:

a) for compliance with a legal obligation pertaining to the controller, or

b) for the purposes of legitimate interests pursued by the controller or by a third party, if enforcing these interests is considered proportionate to the limitation of the right for the protection of personal data,

without the data subject's further consent, or after the data subject having withdrawn his consent.

(6) In court proceedings and administrative proceedings of the authorities launched upon the data subject's request or initiative, as regards the personal data necessary to carry out the proceedings, and in other cases opened at the data subject's request, as regards the personal data he has supplied, the data subject's consent shall be deemed to have been granted.

(7) The consent of the data subject shall be considered granted in connection with any personal data he has conveyed to the public or has supplied for dissemination when making a public appearance.

(8) If there is any doubt, it is to be presumed that the data subject failed to provide his consent.

6. Data security requirement

Section 7

(1) Controllers shall make arrangements for and carry out data processing operations in a way so as to ensure full respect for the right to privacy of data subjects in due compliance with the provisions of this Act and other regulations on data protection.

(2) Controllers, 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.

(3) Data must be protected by means of suitable measures against unauthorized access, alteration, transmission, public disclosure, deletion or destruction, as well as damage and accidental loss, and to ensure that stored data cannot be corrupted and rendered inaccessible due to any changes in or modification of the applied technique.

(4) For the protection of data sets stored in different electronic filing systems, suitable technical solutions shall be introduced to prevent - unless this is permitted by law - the

interconnection of data stored in these filing systems and the identification of the data subjects.

(5) In respect of automated personal data processing, data controllers and processors shall implement additional measures designed to:

a) prevent the unauthorized entry of data;

b) prevent the use of automated data-processing systems by unauthorized persons using data transfer devices;

c) ensure that it is possible to verify and establish to which bodies personal data have been or may be transmitted or made available using data transfer devices;

d) ensure that it is possible to verify and establish which personal data have been entered into automated data-processing systems and when and by whom the data were input;

e) ensure that installed systems may, in case of malfunctions, be restored; and

f) ensure that faults emerging in automated data-processing systems is reported.

(6) In determining the measures to ensure security of processing, data controllers and processors shall proceed taking into account the latest technical development and the state of the art of their implementation. Where alternate data processing solutions are available, the one selected shall ensure the highest level of protection of personal data, except if this would entail unreasonable hardship for the data controller.

7. Data transfer to other countries

Section 8

(1) Personal data may be transmitted by a data controller covered by this Act to a data controller or processor[5] operating in a third country, or may be transferred to a data controller or processor operating in a third country if:

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

b) the conditions laid down in Section 5 and/or Section 6 for data processing are satisfied and - save where Subsection (2) of Section 6 applies – the adequate level of protection of the personal data have been ensured in the third country during the course of the control and processing of the data transferred.

(2) Adequate level of protection of personal data is ensured should:

a) this be stated in a binding legal act of the European Union, or

b) there is an international agreement between the third country and Hungary containing guarantees for the rights of data subjects referred to in Section 14, their rights to remedies, and for the independent supervision and control of data control and data processing operations.

(3) Personal data may be transferred to third countries in the interest of the implementation of an international agreement on international legal aid, exchange of information in tax matters and on double taxation, for the purpose and with the contents specified in the international agreement, also in the absence of the conditions specified in Subsection (2).

(4) Transfer of data to EEA Member States shall be considered as if the transmission took place within the territory of Hungary.

8. Restrictions to data processing

Section 9

[5] In effect as of 1st July 2013

(1) Where personal data is transmitted under this Act and in accordance with international agreement or a binding legal act of the European Union, and the transmitting data controller indicates to the recipient at the time of transmission of the personal data:

a) the purposes for which it can use those data,

b) the time limits for the retention of data,

c) the potential recipients of the data,

d) the restrictions of the data subject's rights ensured under this Act, or

e) specific other processing restrictions that may apply,

(hereinafter referred to collectively as "processing restrictions"), the recipient of such personal data (hereinafter referred to as "data recipient") shall process the personal data to the extent and by way of the means stipulated in the processing restrictions, and shall ensure the data subject's rights in line with the processing restrictions.

(2) The data recipient shall be allowed to process personal data irrespective of restrictions and may enforce the data subject's rights provided a prior consent has been granted by him/her to the transmitting data controller.

(3) Where personal data is transmitted under this Act and in accordance with international agreement or a binding legal act of the European Union, the transmitting data controller shall indicate to the recipient at the time of transmission the processing restrictions applicable.

(4) The data controller shall be able to give the consent referred to in Subsection (2) if it is not contrary to any legal provision applicable to legal subjects falling within the scope of jurisdiction of Hungary.

(5) The data recipient shall – upon request – inform the transmitting data controller concerning the use of the personal data received.

9. Data process

Section 10

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

(2) The data processor shall be permitted to subcontract another data processor according to the notice of the data controller.[6]

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

(4) Contracts for the process 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 process of such data.

10. Decision adopted by means of automated data-process systems

Section 11

(1) A decision which is based solely on automated process of data intended to evaluate certain personal characteristics relating to the data subject shall be permitted only if:

---

[6] In effect as of 1st July 2013

a) it is taken in the course of the entering into or performance of a contract, provided that the request for entering into or performance of the contract was lodged by the data subject, or

b) authorized by a law which also lays down measures to safeguard the data subject's legitimate interests.

(2) In connection with decisions adopted by means of automated data-process systems, the data subject shall, at his request, be informed of the method that is used and its essence, and shall be given the opportunity to express his opinion.

11. Processing personal data relating to scientific research

Section 12

(1) Personal data recorded for scientific reasons must be used only for scientific research projects.

(2) Personal data attributed to the data subject shall be made permanently anonymous when they are no longer required for scientific purposes. Until this is done, personal data that can attributed to an identified or identifiable natural person shall be stored separately. Such data may be linked to other data if it is necessary for the purposes of research.

(3) An organization or person conducting scientific research shall be allowed to disseminate 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.

12. Use of personal data for statistical purposes

Section 13

(1) Unless otherwise provided for by law, the Központi Statisztikai Hivatal (*Hungarian Central Statistical Office*) shall be entitled to receive for statistical purposes personal data processed within the framework of mandatory processing in a form which permits the identification of the data subject, and to process them in accordance with the relevant legislation.

(2) Unless otherwise provided for by law, personal data recorded, received or processed for statistical purposes may only be used for statistical purposes. The detailed regulations governing processing operations involving personal data are defined in specific other act.

13. Rights of data subjects; enforcement

Section 14

The data subject may request from the data controller:

a) information on his personal data being processed,

b) the rectification of his personal data, and

c) the erasure or blocking of his personal data, save where processing is rendered mandatory.

Section 15

(1) Upon the data subject's request the data controller shall provide information concerning the data relating to him, including those processed by a data processor on its behalf or

according to his/her notice[7], the sources from where they were obtained, the purpose, grounds and duration of processing, the name and address of the data processor and on its activities relating to data processing, and - if the personal data of the data subject is made available to others - the legal basis and the recipients.

(2) With a view to verifying legitimacy of data transfer and for the information of the data subject, the data controller shall maintain a transmission log, showing the date of time of transmission, the legal basis of transmission and the recipient, description of the personal data transmitted, and other information prescribed by the relevant legislation on data processing.

(3) The duration of retention of the data referred to in Subsection (2) in the transmission log, and the duration of the ensuing obligation of information may be limited by the legislation on data processing. The above-specified period of limitation shall not be less than five years in respect of personal data, and twenty years in respect of special data.

(4) Data controllers must comply with requests for information without any delay, and provide the information requested in an intelligible form, in writing at the data subject's request, within not more than thirty days.

(5) The information prescribed in Subsection (4) 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. The amount of such charge may be fixed in an agreement between the parties. Where any payment is made in connection with data that was processed unlawfully, or the request led to rectification, it shall be refunded.

Section 16

(1) The data controller may refuse to provide information to the data subject in the cases defined under Subsection (1) of Section 9 and under Section 19.

(2) Should a request for information be denied, the data controller shall inform the data subject in writing as to the provision of this Act serving grounds for refusal. Where information is refused, the data controller shall inform the data subject of the possibilities for seeking judicial remedy or lodging a complaint with the Nemzeti Adatvédelmi és Információszabadság Hatóság (*National Authority for Data Protection and Freedom of Information*) (hereinafter referred to as "Authority").

(3) Data controllers shall notify the Authority of refused requests once a year, by 31 January of the following year.

Section 17

(1) Where a personal data is deemed inaccurate, and the correct personal data is at the controller's disposal, the data controller shall rectify the personal data in question.

(2) Personal data shall be erased if:

a) processed unlawfully;

b) so requested by the data subject in accordance with Paragraph *c)* of Section 14;

c) incomplete or inaccurate and it cannot be lawfully rectified, provided that erasure is not disallowed by statutory provision of an act;

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

e) so ordered by court or by the Authority.

(3) Where Paragraph *d)* of Subsection (2) applies, the requirement of erasure shall not apply to personal data recorded on a carrier that is to be deposited in archive under the legislation on the protection of archive materials.

---

[7] In effect as of 1st July 2013

(4) Personal data shall be blocked instead of erased if so requested by the data subject, or if there are reasonable grounds to believe that erasure could affect the legitimate interests of the data subject. Blocked data shall be processed only for the purpose which prevented their erasure.

(5) If the accuracy of an item of personal data is contested by the data subject and its accuracy or inaccuracy cannot be ascertained beyond doubt, the data controller shall mark that personal data for the purpose of referencing.

Section 18

(1) When a data is rectified, blocked, marked or erased, the data subject and all recipients to whom it was transmitted for processing shall be notified. Notification is not required if it does not violate the rightful interest of the data subject in light of the purpose of processing.

(2) If the data controller refuses to comply with the data subject's request for rectification, blocking or erasure, the factual or legal reasons on which the decision for refusing the request for rectification, blocking or erasure is based shall be communicated in writing within thirty days of receipt of the request. Where rectification, blocking or erasure is refused, the data controller shall inform the data subject of the possibilities for seeking judicial remedy or lodging a complaint with the Authority.

Section 19

The rights of data subjects afforded under Sections 14-18 may be restricted by law in order to safeguard the external and internal security of the State, such as defence, national security, the prevention and prosecution of criminal offences, the safety of penal institutions, to 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 regulated professions, prevent and detect breaches of obligation related to labour law and occupational safety - including in all cases control and supervision - and to protect data subjects or the rights and freedoms of others.

14. Requirement of preliminary information of the data subject

Section 20

(1) Prior to data processing being initiated the data subject shall be informed whether his consent is required or processing is mandatory.

(2) Before processing operations are carried out 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 basis, the person entitled to control the data and to carry out the processing, the duration of the proposed processing operation, if the data subject's personal data is processed in accordance with Subsection (5) of Section 6, and the persons to whom his data may be disclosed. Information shall also be provided on the data subject's rights and remedies.

(3) In the case of mandatory processing such information may be supplied by way of publishing reference to the legislation containing the information referred to in Subsection (2).

(4) If the provision of personal information to the data subject proves impossible or would involve disproportionate costs, the obligation of information may be satisfied by the public disclosure of the following:

a) an indication of the fact that data is being collected;

b) the data subjects targeted;

c) the purpose of data collection;
d) the duration of the proposed processing operation;
e) the potential data controllers with the right of access;
f) the right of data subjects and remedies available relating to data processing; and
g) where the processing operation has to be registered, the number assigned in the data protection register, with the exception of Subsection (2) of Section 68.

15. The data subject's right to object to the processing of his personal data

Section 21

(1) The data subject shall have the right to object to the processing of data relating to him:
a) if processing or disclosure is carried out solely for the purpose of discharging the controller's legal obligation or for enforcing the rights and legitimate interests of the controller, the recipient or a third party, unless processing is mandatory;
b) if personal data is used or disclosed for the purposes of direct marketing, public opinion polling or scientific research; and
c) in all other cases prescribed by law.
(2) In the event of objection, the controller shall investigate the cause of objection within the shortest possible time inside a fifteen-day time period, adopt a decision as to merits and shall notify the data subject in writing of its decision.
(3) If, according to the findings of the controller, the data subject's 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 previously been transferred concerning the objection and the ensuing measures, upon which these recipients shall also take measures regarding the enforcement of the objection.
(4) If the data subject disagrees with the decision taken by the controller under Subsection (2), or if the controller fails to meet the deadline specified in Subsection (2), the data subject shall have the right under Section 22 to turn to court within thirty days of the date of delivery of the decision or from the last day of the time limit.
(5) If data that are necessary to assert the data recipient's rights are withheld owing to the data subject's objection, the data recipient shall have the right under Section 22 to turn to court against the controller within fifteen days from the date the decision is delivered under Subsection (2) in order to obtain the data. The controller is authorised to summon the data subject to court.
(6) If the data controller fails to send notice as specified in Subsection (3), the data recipient shall have the right to request information from the controller concerning the circumstances of non-disclosure, upon which the controller shall make available the information requested within eight days of receipt of the data recipient's request. Where information had been requested, the data recipient may bring an action against the controller within fifteen days from the date of receipt of the information, or from the deadline prescribed therefor. The controller is authorised to summon the data subject to court.
(7) 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.

16. Judicial remedy

Section 22

(1) In the event of any infringement of his rights, the data subject, and in the cases referred to in Section 21, the data recipient may turn to court action against the controller. The court shall hear such cases in priority proceedings.

(2) The burden of proof to show compliance with the law lies with the data controller. In the cases under Subsections (5) and (6) of Section 21, the burden of proof concerning the lawfulness of transfer of data lies with the data recipient.

(3) The action shall be heard by the competent tribunal. If so requested by the data subject, the action may be brought before the tribunal in whose jurisdiction the data subject's home address or temporary residence is located.

(4) Any person otherwise lacking legal capacity to be a party to legal proceedings may also be involved in such actions. The Authority may intervene in the action on the data subject's behalf.

(5) When the court's decision is in favor of the plaintiff, the court shall order the controller to provide the information, to rectify, block or erase the data in question, to annul the decision adopted by means of automated data-processing systems, to respect the data subject's objection, or to disclose the data requested by the data recipient referred to in Section 21.

(6) If the court rejects the petition filed by the data recipient in the cases defined in Section 21, the controller shall be required to erase the data subject's personal data within three days of delivery of the court ruling. The controller shall erase the data even if the data recipient does not file for court action within the time limit referred to in Subsection (5) or (6) of Section 21.

(7) The court may order publication of its decision, indicating the identification data of the controller as well, where this is deemed necessary for reasons of data protection or in connection with the rights of large numbers of data subjects under protection by this Act.

17. Compensation

Section 23

(1) Data controllers shall be liable for any damage caused to a data subject as a result of unlawful processing or by any breach of data security requirements. The data controller shall also be liable for any damage caused by data processor acting on its behalf. The data controller 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 serious negligent conduct on the part of the aggrieved party.

18. Internal data protection officer, data protection rules

Section 24

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

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

b) financial institutions;

c) providers of electronic communications and public utility services.

(2) The internal data protection officer shall:

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

b) monitor compliance with the provisions of this Act and other 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, call on the controller or processor in question to cease such operations;

d) draw up the internal data protection and data security rules;

e) maintain the internal data protection register;

f) organises 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 rules in accordance with this Act.

19. Conference of internal data protection officers

Section 25

(1) The conference of internal data protection officers (hereinafter referred to as "conference") is intended to maintain regular professional contacts between the Authority and internal data protection officers, the purpose of which is to ensure the consistency of the case-law as regards the protection of personal data and access to public information.

(2) The President of the Authority shall call the conference at least once every year, or as necessary, and shall determine its agenda.

(3) The internal data protection officers of all organizations where such office has to be maintained by law shall have a seat on the conference.

(4) The internal data protection officers of those organizations where such office is not required may also have a seat on the conference. To this end they may seek admission to the register of internal data protection officers maintained by the Authority.

(5) For communication purposes, the Authority shall maintain a register of internal data protection officers on members of the conference. The register contains the name, postal and electronic mail address of internal data protection officers, and the name of the organization they represent.

(6) The Authority shall record the data mentioned in Subsection (5) until the time of receiving information on the termination of the internal data protection officer's term in office.

CHAPTER III

ACCESS TO INFORMATION OF PUBLIC INTEREST

20. General provisions on access to information of public interest

Section 26

(1) Any person or body attending to statutory State or municipal government functions or performing other public duties provided for by the relevant legislation (hereinafter referred to collectively as "body with public service functions") shall allow free access to the data of public interest and data public on grounds of public interest under its control to any person, save where otherwise provided for in this Act.

(2) The name of the person undertaking tasks within the scope of responsibilities and authority of the body undertaking public duties, as well as their scope of responsibilities, scope of work, executive mandate and other personal data relevant to the provision of their responsibilities to which access must be ensured by law qualify as data public on grounds of public interest. These data may be disseminated in compliance with the principle of purpose limitation. Provisions on the disclosure of data public on the grounds of public interest shall be regulated by Appendix 1 of this Act and the specific laws relating to the status of the person undertaking public duties.

(3) Unless otherwise prescribed by law, any data, other than personal data, that is processed by bodies or persons providing services prescribed mandatory by law or under contract with any governmental agency, central or local, if such services are not available in any other way or form relating to their activities shall be deemed data public on grounds of public interest.

Section 27

(1) Access to data of public interest or data public on grounds of public interest shall be restricted if it has been classified under the Act on the Protection of Classified Information.

(2) Right of access to data of public interest or data public on grounds of public interest may be restricted by law - with the specific type of data indicated - where considered necessary to safeguard:

a) national defense;

b) national security;

c) prevention and prosecution of criminal offenses;

d) environmental protection and nature preservation;

e) central financial or foreign exchange policy;

f) external relations, relations with international organizations;

g) court proceedings or administrative proceedings;

h) intellectual property rights.

(3) Access to business secrets shall be governed by the relevant provisions of the Civil Code.

(4) Access to 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, fiscal and tax policies.

(5) Any information compiled or recorded by a body with public service functions as part of, and in support of, a decision-making process for which it is vested with powers and competence, shall not be made available to the public for ten years from the date it was compiled or recorded. Access to these information may be authorized by the head of the body

that controls the information in question upon weighing the public interest in allowing or disallowing access to such information.

(6) A request for disclosure of information underlying a decision may be rejected after the decision is adopted, but within the time limit referred to in Subsection (5), if disclosure is likely to jeopardize the legal functioning of the body with public service functions or the discharging of its duties without any undue influence, such as in particular free expression of the position of the body which generated the data during the preliminary stages of the decision-making process.

(7) The time limit for restriction of access as defined in Subsection (5) to certain specific information underlying a decision may be reduced by law.

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

21. Access to public information upon request

Section 28

(1) Data of public interest shall be made available to anyone upon a request presented verbally, in writing or by electronic means. Access to data public on grounds of public interest shall be governed by the provisions of this Act pertaining to data of public interest.

(2) Unless otherwise provided for by law, the processing of personal data in connection with any disclosure upon request is permitted only to the extent necessary for disclosure, including the collection of payment of charges for copies, where applicable. Following the disclosure of data and upon receipt of the said payment, the personal data of the requesting party must be erased without delay.

(3) If any part of the request is unclear, the data controller shall ask the requesting party to clarify.

Section 29

(1) The body with public service functions that has the data of public interest on record must comply with requests for public information at the earliest opportunity within not more than fifteen days.

(2) If a request for information is substantial in terms of size and volume, the time limit referred to in Subsection (1) may be extended by fifteen days on one occasion, of which the requesting party shall be informed within eight days of the date of receipt of the request.

(3) The requesting party may also be provided a copy of the document or part of a document containing the information in question, irrespective of the form of storage. The body with public service functions processing the data in question may charge a fee covering only the costs of making the copy, and shall communicate this amount to the requesting party in advance.

(4) If the document or part of a document of which the copy had been requested is substantial in size and/or volume, the copy shall be provided within fifteen days from the date of payment of the fee as charged. The requesting party shall be notified within eight days from the date of receipt of his request if the document or part of a document of which the copy had been requested is considered substantial in size and/or volume, as well as of the amount of the fee chargeable, and if there is any alternate solution available instead of making a copy.

(5) The items covered by the fee chargeable, and the highest amount that can be taken into account in determining the amount of the fee, and the aspects for determining whether a

document is to be considered substantial in terms of size and/or volume shall be laid down by specific other legislation.

Section 30

(1) If a document that contains data of public interest also contains any data that cannot be disclosed to the requesting party, this data must be rendered unrecognizable on the copy.

(2) Information shall be supplied in a readily intelligible form and by way of the technical means asked for by the requesting party, provided that the body with public service functions processing the information is capable to meet such request without unreasonable hardship. If the information requested had previously been made public electronically, the request may be fulfilled by way of reference to the public source where the data is available. A request for information may not be refused on the grounds that it cannot be made available in a readily intelligible form.

(3) When a request for information is refused, the requesting party must be notified thereof within eight days in writing, or by electronic means if the requesting party has conveyed his electronic mailing address, and must be given the reasons of refusal, including information on the remedies available. The controller shall keep records on the requests refused, including the reasons, and shall inform the Authority thereof each year, by 31 January.

(4) A request for data of public interest by a person whose native language is not Hungarian may not be refused for reasons that it was written in his native language or in any other language he understands.

(5) If, as regards the refusal of any request for access to data of public interest, the data controller is granted discretionary authority by law, refusal shall be exercised within narrow limits, and the request for access to data of public interest may be refused only if the underlying public interest outweighs the public interest for allowing access to the public information in question.

(6) Bodies with public service functions shall adopt regulations governing the procedures for satisfying requests for access to public information.

(7) The requests for data with the purpose of a comprehensive, account level as well as an itemized control of the financial management of the body with public service functions are regulated in specific relevant laws. Should such data request be rejected, the requesting party may initiate an investigation of the Authority pursuant to Section 52.

Section 31

(1) In the event of failure to meet the deadline for the refusal or compliance with a request for access to public information, or with the deadline extended by the data controller pursuant to Subsection (2) of Section 29, and - if the fee chargeable has not been paid - the requesting party may bring the case before the court for having the fee charged for the copy reviewed.

(2) The burden of proof to verify the lawfulness and the reasons of refusal, and the reasons for determining the amount of the fee chargeable for the copy lies with the data controller.

(3) Litigation must be launched against the body with public service functions that has refused the request within thirty days from the date of delivery of the refusal, or from the time limit prescribed, or from the deadline for payment of the fee chargeable. If the requesting party notifies the Authority with a view to initiating the Authority's proceedings in connection with the refusal of or non-compliance with the request, or on account of the amount of the fee charged for making a copy, litigation may be launched within thirty days from the time of receipt of notice on the refusal to examine the notification on the merits, on the termination of the inquiry, or its conclusion under Paragraph *b)* of Subsection (1) of Section 55, or the notice

under Subsection (3) of Section 58. Justification may be submitted upon failure to meet the deadline for bringing action.

(4) Any person otherwise lacking legal capacity to be a party to legal proceedings may also be involved in such legal proceedings. The Authority may intervene on the requesting party's behalf.

(5) Actions against bodies with public service functions of nation-wide jurisdiction shall be brought at the competent tribunal. Actions falling within the jurisdiction of local courts shall be heard by the local court of the seat of the tribunal, or by the Pesti Központi Kerületi Bíróság (*Pest Central District Court*) in Budapest. Jurisdiction shall be determined by reference to the place where the head offices of the body with public service functions, being the respondent, is located.

(6) The court shall hear such cases in priority proceedings.

(7) When the decision is in favor of the request for access to public information, the court shall order the data controller to disclose the information in question. The court shall have powers to modify the amount charged for making a copy, or may order the body with public service functions to re-open its proceedings for determining the amount of the fee chargeable.

CHAPTER IV

DISSEMINATION OF DATA OF PUBLIC INTEREST

22. Obligation to disclose data of public interest

Section 32

Bodies with public service functions shall promote and ensure that the general public is provided with accurate information in a prompt manner concerning the matters under their competence, such as the budgets of the central and municipal governments and the implementation thereof, the management of assets controlled by the central and municipal governments, the appropriation of public funds, and special and exclusive rights conferred upon market actors, private organizations or individuals.

23. Obligation of publication by electronic means

Section 33

(1) Access to public information whose publication is rendered mandatory under this Act shall be made available through the internet, in digital format, to the general public without any restriction, in a manner not to allow the identification of specific individuals, in a format allowing for printing or copying without any loss or distortion of data, free of charge, covering also the functions of consultation, downloading, printing, copying and network transmission (hereinafter referred to as "electronic publication"). Access to information disseminated as per the above shall not be made contingent upon the disclosure of personal data.

(2) Unless otherwise provided for by law, the following shall disseminate specific information defined on the publication lists referred to in Section 37:

a) Köztársasági Elnök Hivatala (*President of the Republic*), Országgyűlés Hivatala (*Parliament*), Alkotmánybíróság Hivatala (*Constitutional Court*), Alapvető Jogok Biztosának Hivatala (*Commissioner for Fundamental Rights*), Állami Számvevőszék (*State Audit Office*), Magyar Tudományos Akadémia (*Hungarian Academy of Sciences*), Magyar Művészeti

Akadémia (*Hungarian Academy of Arts*), Országos Bírósági Hivatal *(National Office for the Judiciary)*, Legfőbb Ügyészség (*Prosecutor General's Office*);

b)

c) central administrative authorities with the exception of governmental committees as well as national chambers; and

d) county and capital Government Offices.

(3) The bodies with public service functions, other than those listed in Subsection (2), shall have the option to fulfil their obligation of publication by electronic means, defined in Section 37, through their own website or other websites maintained jointly with their associations, or by other bodies appointed to supervise their organizational and professional infrastructure, or coordinating their operations, or through a central website set up for this purpose.

(4) Any public education institution having no national or regional duties shall discharge their obligation of publication by electronic means under this Act by way of data disclosure to the information systems specified by the relevant legislation governing the given sector.

Section 34

(1) The data source, if disseminating information through the website of others shall transfer the data - in accordance with Section 35 - to the data disseminator, who shall take measures for having the data published on a website, and shall ascertain that the name of the body from which public information originates or to which it pertains is clearly indicated.

(2) The data disseminator shall design the website used for publication with facilities to disseminate data and information, and shall ensure that the website runs without interruption and it is properly maintained, and that data are updated on a regular basis.

(3) The website used for dissemination shall offer easily understandable information concerning the rules of access to public information, including the remedies available.

(4) In addition to the public information specified on the publication lists, other public information and information of public interest may also be published on the website used for dissemination by way of electronic means.

Section 35

(1) The head of the data source subject to electronic publication shall provide for having the data and information specified on the publication lists defined in Section 37 published accurately, up-to-date and on a regular basis, and for having them sent to the data disseminator.

(2) Responsibility for the publication of the data by electronic means, continuous access, and for keeping them authentic and regularly updates lies with the data disseminator.

(3) The data source and the data disseminator shall adopt internal regulations for laying down the detailed rules for discharging the obligations referred to in Subsection (1) and Subsection (2), respectively.

(4) Information published electronically may not be removed from the website, unless otherwise provided for by this Act or other legislation. In the event of dissolution of a body, the obligation of publication shall devolve upon the successor.

Section 36

Dissemination of the information specified in the publication lists referred to in Section 37 shall be without prejudice to the obligation of the given body concerning the publication of public information or information of public interest prescribed in other legislation.

24. Disclosure lists

Section 37

(1) The bodies referred to in Subsections (2)-(4) of Section 33 (hereinafter referred to collectively as "body subject to disclosure requirement") shall - subject to the exception set out in Subsection (4) - disseminate the data specified in the standard disclosure list referred to in Schedule No. 1 - as pertaining to their activities - by way of the means defined in Annex No. 1.

(2) Additional data may be prescribed by law to be disseminated by certain types of bodies with public service functions regarding certain specific sectors (hereinafter referred to as "special disclosure list").

(3) The publication of specific other data may be rendered mandatory by the head of the body subject to disclosure requirement - upon consulting with the Authority -, as well as by statutory provisions for bodies with public service functions, and other agencies controlled and/or supervised by such bodies, or sections of such agencies (hereinafter referred to as "ad hoc disclosure list").

(4) The Government shall decree - upon consulting with the Authority - the information to be made public by the national security services.

(5) In the case of collegiate bodies subject to disclosure requirement, these bodies shall have powers to establish, and amend, the ad hoc disclosure list, upon consulting with the Authority.

(6) The head of the body subject to disclosure requirement shall review the disclosure list he has published under Subsection (3), taking into consideration any demand shown for public information that was not included in the publication list, and shall include such public information where demand is considered substantial in terms of the amount and number of requests received.

(7) The disclosure list may also provide for the frequency of publication, depending on the type of data in question.

(8) The Authority may present a recommendation for having special and ad hoc publication lists drawn up, or amended.

24/A. Central electronic register of public information and the single data retrieval system

Section 37/A

(1) In the interest of providing fast and easy access to information that has been published electronically, the central electronic register posted on a designated website - set up by the minister in charge for the implementation of infrastructure requirements for administrative information technology systems - contains all relevant descriptive information on the websites of bodies subject to the obligation of publication of public information by electronic means under this Act, pertaining also to their databases and registers.

(2) Electronic access using a single platform to the public information of the bodies referred to in Subsection (1) and facilities for searching among public information shall be ensured by

the single data retrieval system set up by the minister in charge for the implementation of infrastructure requirements for administrative information technology systems.

Section 37/B

(1) The data source shall provide for having the descriptive information on websites, databases and registers containing public information made available to the minister in charge for the implementation of infrastructure requirements for administrative information technology systems and for updating on a regular basis the public information thus forwarded, and shall be responsible for the contents of public information forwarded to the single data retrieval system, as well as for having such public information updated on a regular basis.

(2) Maintaining the databases and registers containing public information and linking up with the single data retrieval system shall not exonerate the data source from the obligation of publication by electronic means.

CHAPTER V

NEMZETI ADATVÉDELMI ÉS INFORMÁCIÓSZABADSÁG HATÓSÁG (NATIONAL AUTHORITY FOR DATA PROTECTION AND FREEDOM OF INFORMATION)

25. Legal status of the Authority

Section 38

(1) The Authority is an autonomous administrative organ.

(2) The Authority shall be responsible to supervise and promote the enforcement of the rights to the protection of personal data and access to public information and information of public interest.

(3) Within its scope of responsibilities conferred under Subsection (2), the Authority:

a) shall conduct investigations upon notification;

b) may conduct *ex officio* administrative proceedings for data protection;

c) may conduct *ex officio* administrative proceedings for the control of classified data;

d) may turn to court in connection with any infringement concerning public information and information of public interest;

e) may intervene in court actions brought by others;

f) maintain the data protection register;

in accordance with this Act.

(4) Within its scope of responsibilities conferred under Subsection (2), the Authority:

a) shall have powers to make recommendations for new regulations and for the amendment of legislation pertaining to the processing of personal data, to public information and information of public interest, and shall express its opinion on drafts covering the same subject;

b) shall publish a report on its activities each year, by 31 March, and shall present this report to Parliament;

c) shall make recommendations in general, or to specific controllers;

d) shall give an opinion on special and ad hoc disclosure lists prescribed mandatory by this Act relating to the activities of the given body with public service functions;

e) shall collaborate with the bodies and persons defined in specific other legislation to represent Hungary in the joint data protection supervisory bodies of the European Union;

f) organize the conference of internal data protection officers;

g)-h)

(5) The Authority is an independent body that is subject to Hungarian law only, it may not be instructed in its official capacity, shall operate independent of any outside interference, without any bias. Tasks may only be prescribed for the Authority by acts of Parliament.

26. Budget and financial management of the Authority

Section 39

(1) The Authority shall be a central budgetary organ with the powers of a budgetary chapter, and its budget shall constitute an independent title within the budgetary chapter of Parliament.

(2) The main totals of expenditures and receipts of the Authority for the current budgetary year may only be reduced by Parliament, with the exception of natural disasters endangering life and property as defined in the Act on Public Finances, of temporary measures adopted to relieve the consequences of such disasters, or of measures taken by the Authority within its own competence or in its competence as directing organ.

(3)

(4) The remainder of receipts from the previous year may be used by the Authority in the following years for the performance of its tasks.

27. President of the Authority

Section 40

(1) The head of the Authority is the President. The President of the Authority is appointed by the President of the Republic on a recommendation by the Prime Minister from among those Hungarian citizens with a law degree, who have the right to stand as candidates in parliamentary elections, having at least ten years of experience in supervising proceedings related to data protection or freedom of information, or holding an academic degree in either of those fields.

(2) Persons who served as a Member of Parliament or as a Member of the European Parliament, as the President of the Republic, member of the Government, state secretary, representative of a municipal government, mayor or deputy mayor, lord mayor or deputy lord mayor, chairman or deputy chairman of a county assembly, member of a national minority self-government, or an officer or employee of a political party in the four-year period before the time of the recommendation for appointment may not be appointed as President of the Authority.

(3) The President of the Authority shall be appointed by the President of the Republic for a term of nine years.

(4) The President of the Authority - upon being appointed - shall take an oath before the President of the Republic in accordance with the Act on the Oath and Deposition of Public Officials.

Section 41

(1) The President of the Authority may not be a member of any political party, may not engage in political activities, and his mandate shall be considered incompatible with other state or local government office or mandate.

(2) The President of the Authority shall not be otherwise gainfully employed and shall not accept remuneration for other activities, with the exception of scientific, educational and artistic activities under copyright protection, and other than revisory and editorial activities.

(3) The President of the Authority may not hold any executive office or membership in the supervisory board of a business association; and he may not be a member of a business association requiring personal involvement.

Section 42

(1) The President of the Authority shall submit a declaration of personal assets in accordance with the provisions on the declarations of personal assets of Members of Parliament within thirty days of the time of appointment, and subsequently by 31 January of each year, and also within thirty days after the date of termination of his mandate.

(2) In the event of non-compliance with the requirement to file a declaration of personal assets the President of the Authority shall not be able to execute his office and shall not receive any remuneration insofar as his declaration of personal wealth is submitted.

(3) The declaration of personal assets shall be made public and an authentic copy teherof shall be posted on the Authority's website without delay. The declaration of personal assets may not be removed from the website for a period of one year following termination of the mandate of the President of the Authority.

(4) The Prime Minister's proceedings relating to the declaration of personal assets of the President of the Authority may be requested by anyone with reference to specific sections of the declaration, and the contents of such sections, that is disputed. If the petition submitted is not in conformity with the requirements set out in this Subsection, or if it is manifestly unfounded, or if the petition is re-submitted and it offers no new argument or evidence, the Prime Minister shall refuse the petition without the opening of an examination as to merits. The Prime Minister shall check the authenticity and credibility of the information supplied in the declaration of personal assets.

(5) In proceedings related to the declaration of personal wealth, the President of the Authority shall - at the Prime Minister's request - submit a statement without delay, offering proof for the data and information contained in the declaration of personal wealth concerning his personal finances, income and other financial interests to the Prime Minister in writing. The Prime Minister shall send the findings of the proceedings to the President of the Republic along with the relevant data and information. Access to such data and information is restricted to the Prime Minister and the President of the Republic.

(6) The evidence submitted by the President of the Authority in connection with his declaration of personal wealth shall be deleted on the thirtieth day following the date of conclusion of the proceedings.

Section 43

(1) The President of the Authority shall be entitled to the same remuneration and benefits as the salary and benefits of ministers, including an executive bonus in the amount equal to one and a half times of the executive bonus of ministers.

(2) The President of the Authority is entitled to forty working days of paid annual leave per calendar year.

Section 44

(1) In terms of eligibility for social security benefits, the President of the Authority shall be regarded as employed in public service relationship.

(2) The time period of the President's mandate shall be recognized as spent in public service at an administrative body.

Section 45

(1) The mandate of the President of the Authority shall terminate:

a) upon expiry of his term of office;

b) upon resignation;

c) upon death;

d) if the requirements for appointment are no longer satisfied or upon violation of the rules regarding the declaration of assets;

e) upon declaration of incompatibility;

f) - g)

(2) The President of the Authority shall be able to resign from office any time, by means of tendering his resignation in writing submitted to the Prime Minister and addressed to the President of the Republic. The mandate of the President of the Authority shall terminate on the day subsequent to the date of resignation, as indicated in the resignation, or failing this on the day when the resignation is submitted. A declaration of acceptance is not required for the effectiveness of the resignation.

(3) If the President of the Authority fails to resolve the conflict of interest specified under Section 41 within thirty days from the date of appointment, or if any conflict of interest arises while in office, the President of the Republic shall decide as to incompatibility, on a proposal by the Prime Minister, within thirty days following the date of receipt of the proposal.

(4)- (5)

(6) The President of the Republic shall decide upon the declaration of non-compliance with the requirements for the appointment of the President of the Authority on a proposal by the Prime Minister. The President of the Republic shall - on a proposal by the Prime Minister - establish the infringement of the provisions on the declaration of personal wealth, if the President of the Authority has knowingly disclosed false data or information in his declaration of personal wealth.

(6a) The Prime Minister shall send a copy of his proposal made under Subsections (3) and (6) to the President of the Republic and to the President of the Authority as well.

(6b) The President of the Authority may contest the proposal and bring the case before the court within thirty days from the date of receipt of the proposal. No application for continuation will be accepted upon failure to meet this deadline. The action shall be brought against the Prime Minister. The court shall proceed in accordance with the provisions of the Code of Civil Procedure on actions relating to contracts of employment and other similar relationships, with the proviso that the case shall be heard by the Fővárosi Közigazgatási és Munkaügyi Bíróság (*Budapest Administrative and Labour Tribunal*) in priority proceedings under exclusive jurisdiction, and the action and the final decision shall be communicated to the President of the Republic as well.

(6c) If based on the action brought by the President of the Authority according to Subsection (6b) the court in its final decision finds the Prime Minister's proposal made under Subsections (3) and (6) unsubstantiated, the President of the Republic shall not declare the mandate of the President of the Authority terminated.

(6d) The President of the Republic shall decide on the Prime Minister's proposal made under Subsections (3) and (6):

a) if the President of the Authority did not file for court action inside the time limit specified in Subsection (6b), within fifteen days past the time limit,

b) if the President of the Authority did file for court action inside the time limit specified in Subsection (6b), within fifteen days from the date of the final decision adopted on the merits of the case.

(7) If the mandate of the President of the Authority terminates under Paragraph *a)* or *b)* of Subsection (1), the President shall be entitled to an extra payment of three times the monthly remuneration in effect at the time of termination.

(8) As regards the decisions conferred by Subsections (3) and (6) of this Section and by Section 40 under the competence of the President of the Republic, no endorsement is required.

Section 45/A

The President of the Authority shall have the right to participate in and address the Parliament committee meetings.

28. Vice-President of the Authority

Section 46

(1) The President of the Authority shall appoint a Vice-President for an indefinite period to assist in his work. The President of the Authority shall exercise the employer's rights in respect of the Vice-President.

(2) The Vice-President shall be able to satisfy the requirements set out in Subsections (1) and (2) of Section 40 for the appointment of the President of the Authority but with a distinction of having at least five years of experience in supervising proceedings related to data protection or freedom of information, or holding an academic degree in either of those fields.

(3) The provisions of Section 41 on conflict of interest shall apply to the Vice-President as well.

(4) In the event that the President is temporarily prevented from attending to his duties, or if the office of the President is vacant, the powers and responsibilities of the President shall be exercised by the Vice-President.

Section 47

The provisions of Section 42 shall also apply to the obligation of the Vice-President to file a declaration of personal assets, and also to the related proceedings, with the exception that the President of the Authority shall hear cases related to the declaration of personal assets instead of the Prime Minister, and that the President of the Republic need not be informed of the findings of the proceedings.

Section 48

(1) The Vice-President shall be entitled to the same remuneration and benefits as the salary and benefits of state secretaries.

(2) The Vice-President is entitled to forty working days of paid annual leave per calendar year.

(3) In terms of eligibility for social security benefits, the Vice-President shall be regarded as employed in public service relationship.

(4) The time period of the Vice-President's mandate shall be recognized as spent in public service at an administrative body.

Section 49

(1) The mandate of the Vice-President of the Authority shall terminate:
a) upon resignation;
b) upon death;
c) if the requirements for appointment are no longer satisfied;
d) upon declaration of incompatibility;
e) upon dismissal;
f) upon removal from office.

(2) The Vice-President of the Authority shall be able to resign from office any time, by means of tendering his resignation in writing submitted to the President of the Authority. The mandate of the Vice-President of the Authority shall terminate on the day subsequent to the date of resignation, as indicated in the resignation, or failing this on the day when the resignation is submitted. A declaration of acceptance is not required for the effectiveness of the resignation.

(3) If the Vice-President of the Authority fails to resolve the conflict of interest specified under Section 41 within thirty days from the date of appointment, or if any conflict of interest arises while in office, the President of the Authority shall decide as to incompatibility.

(4) The President of the Authority shall dismiss the Vice-President of the Authority, if the Vice-President of the Authority is unable to attend to his vested duties for a period of over ninety days for reasons beyond his control.

(5) The President of the Authority shall be entitled to dismiss the Vice-President of the Authority and shall, at the same time, offer a civil service relationship to the Vice-President at the Authority and an examiner's position even in the absence of the requirements set out in Subsection (1) of Section 51.

(6) The President of the Authority shall remove the Vice-President of the Authority from office, if the Vice-President fails to attend to his vested duties for a period of over ninety days for reasons within his control, or if he has knowingly disclosed false data or information in his declaration of personal wealth.

(7) The President of the Authority shall decide upon the declaration of non-compliance with the requirements for the appointment of the Vice-President of the Authority.

(8) If the mandate of the Vice-President of the Authority terminates under Paragraph *a)* or *e)* of Subsection (1), the Vice-President shall be entitled to an extra payment of three times the monthly remuneration in effect at the time of termination.

29. Staff of the Authority

Section 50

The President of the Authority shall exercise employer's rights in respect of the Authority's public servants and employees.

Section 51

(1) The President of the Authority shall be entitled to appoint examiners - up to twenty per cent of all civil servants of the Authority - from among the civil servants in the Authority's employ who have a degree of higher education in information technology or law, and at least three years of experience as a data protection expert or data protection officer, and who have passed a professional examination in public administration or professional examination in law.

(2) Examiners are appointed for indefinite terms, and may be dismissed by the President of the Authority any time without cause. If the President of the Authority has withdrawn the appointment of an examiner, the civil servant in question shall be reinstated in his last position before the appointment.

(3) Examiners are entitled to the salary of head of unit, exclusive of executive bonus.

CHAPTER VI

PROCEEDINGS OF THE AUTHORITY

30. Investigation by the Authority

Section 52

(1) Any person shall have the right to notify the Authority and request an investigation alleging an infringement relating to his or her personal data or concerning the exercise of the rights of access to public information or information of public interest, or if there is imminent danger of such infringement.

(2) The Authority's investigations ensuing shall not be treated as administrative proceedings, and shall not fall within the scope of the Act on the General Rules of Administrative Proceedings.

(3) Having submitted a notification to the Authority may not entail any discrimination against the notifier. The Authority may reveal the person of the notifier only if the inquiry cannot be carried out otherwise. If so requested by the notifier, the Authority may not disclose his identity even if the inquiry cannot be carried out otherwise. The notifier must be informed by the Authority of this circumstance.

(4) The Authority shall carry out the investigation free of charge; the costs thereof shall be advanced and borne by the Authority.

Section 53

(1) Subject to the exceptions set out in Subsections (2) and (3), the Authority shall examine the notifications received as to merits.

(2) The Authority may refuse the notification without examination thereof as to merits if:

a) the infringement alleged in the notification is considered minor, or

b) the notification is anonymous.

(3) The Authority shall refuse the notification without examination thereof as to merits if:

a) court proceedings are in progress, or a final court ruling has previously been rendered concerning the case in question,

b) the notifier maintains his request for not having his identity disclosed despite the information provided under Subsection (3) of Section 52,

c) the notification is manifestly unfounded,

d) the notification has been re-submitted and it contains no new facts or information as to merits.

(4) The Authority may only refuse a notification that has been submitted by the Commissioner of Fundamental Rights without examination thereof as to merits if court proceedings are in progress, or a final court ruling has previously been rendered concerning the case in question.

(5) The Authority shall terminate the investigation if:

a) the petition should have been refused pursuant to Subsections (3)-(4), however, the authority obtained information concerning the grounds for refusal following the opening of the investigation;

b) the reason for continuing the investigation no longer exists.

(6) The Authority shall inform the notifier concerning the refusal of the notification without examination thereof as to merits and on the termination of the investigation, including the reasons for refusal and termination.

(7) The Authority shall refer a case for which it has no competence to the proper authority, of which the notifier shall be informed, provided that there is sufficient information available to determine the identity of the relevant authority. If, based on the notification received in a case for which it has no competence, the Authority comes to the conclusion that the case should be brought before the court, the notifier shall be informed thereof.

Section 54

(1) In the course of that investigation, the Authority:

a) shall have powers to inspect all documents of the controller inspected, presumed to have any bearing on the case at hand, and may request copies of such documents,

b) shall be given access to any data processing operation presumed to have any bearing on the case at hand, and shall be authorized to enter any premises where data processing takes place,

c) shall have the right to request information from the controller inspected, and from any employee or associate of the controller in writing or verbally,

d) shall have the right to request information in writing from any organization or person presumed to have any connection to the case at hand, and

e) may request the head of the supervisory body of the data controller authority to conduct an investigation.

(2) The data controller inspected and the organization or person involved in the case at hand shall comply with the Authority's request under Subsection (1) within the time limit prescribed by the Authority. The time limit prescribed by the Authority may not be less than fifteen days in the cases referred to in Paragraphs *d)* and *e)* of Subsection (1).

(3) The person asked for information according to Paragraphs *c)* and *d)* of Subsection (1) may refuse to comply if:

a) the person affected by the notification underlying the Authority's proceedings is his close relative or former spouse by definition of the Act on the General Rules of Administrative Proceedings;

b) giving the information would implicate himself, or his close relative or former spouse defined in the Act on the General Rules of Administrative Proceedings in the commission of a crime, as regards the question related thereto.

Section 55

(1) Within two months from the date of receipt of the notification, the Authority shall:

a) if it finds in favour of the notification,

aa) take the measures defined in Section 56 and Section 57,

ab) terminate the investigation, and shall launch administrative proceedings for data protection in accordance with Section 60, or

ac) terminate the investigation, and shall launch administrative proceedings for the supervision of classified data in accordance with Section 62;

b) terminate the investigation if it finds against the notification.

(2) The Authority shall inform the notifier on the findings of its investigation, on the reasons for terminating the proceedings and on any measures taken or on the opening of administrative proceedings.

Section 56

(1) Where the Authority considers that any infringement relating to personal data or concerning the exercise of the rights of access to public information or information of public interest, or the imminent danger of such infringement exist, it shall call on the data controller affected to eliminate the infringement, and the imminent danger of such infringement.

(2) The controller - if in agreement - shall take the measures indicated in the notice referred to in Subsection (1) without delay, and shall inform the Authority concerning the measures it has taken, or - if in disagreement - of its argument within thirty days from the date of receipt of the notice.

(3) If the data controller authority has a supervisory body, the Authority - if the notice referred to in Subsection (1) failed to obtain satisfaction - may present a recommendation to the controller's supervisory body, of which the controller has to be notified concurrently. The Authority may also present a recommendation directly, without sending a notice to the controller under Subsection (1), if it is of the opinion that this is a more efficient way to remedy the infringement and to eliminate the imminent danger of such infringement.

(4) The supervisory body shall notify the Authority in writing of its position concerning the recommendation as to merits, or on the measures taken within thirty days from the date of receipt of the recommendation.

Section 57

If, based on the findings of the investigation, the Authority considers that the infringement or the imminent danger thereof is attributable to any provision of legislation or regulatory instrument for the governance of bodies governed by public law that is deemed redundant, unclear or inadequate, or the lack of legal regulation of issues relating to data processing, or the deficiency thereof, it may present a proposal for legislative step, or for the issue of a regulatory instrument for the governance of bodies governed by public law in the interest of eliminating such infringements and the imminent danger thereof in the future, to the appropriate bodies for the issue of a legal act for the governance of bodies governed by public law or for drafting bills of legislation. In the recommendation the Authority may propose the amendment, repeal or adoption of legislation or legal act for the governance of public organizations. The body contacted shall inform the Authority within sixty days concerning its opinion, or on the measures taken in conformity with the recommendation.

Section 58

(1) Should, pursuant to the notification issued or the recommendation presented in accordance with Article 56, the anomaly not have been addressed and its immediate threat not have been ceased, the Authority shall make a decision regarding further necessary measures to be taken within a period of 30 days following the expiry of the deadline date for notification specified in Article 56 (2), or Article 56 (4) if a recommendation was not issued.

(2) Where Subsection (1) applies, the Authority shall take further action as per the following:

a) open administrative proceedings for data protection under Section 60;

b) open administrative proceedings for the control of classified data under Section 62;

c) initiate court proceedings according to Section 64; or

d) draw up a report according to Section 59.

(3) The Authority shall inform the notifier concerning the outcome of the measures taken under Sections 56 and 57, and on taking further action according to Subsection (2) hereof.

31. The Authority's report

Section 59

(1) The Authority may draw up a report on the findings of an investigation conducted on basis of notification in a case where the Authority did not open administrative proceedings and did not file for court action.

(2) The report shall contain the facts revealed by the investigation, and the resulting findings and conclusions.

(3) The Authority's report shall be public. The President of the Authority shall classify the report if it contains any classified information, or shall confirm its existing classification. If the report contains any classified information or any secrets protected by law, it shall be made available to the public with the classified information or secrets protected by law properly concealed.

(4) The report made by the Authority on the examination of the activities of bodies authorized for using secret service means and methods may not contain any data or information that may suggest any covert investigation conducted by these bodies in a given case.

(5) The Authority's report may not be contested in court or before any other authority.

32. Administrative proceedings for data protection

Section 60

(1) In the interest of the enforcement of the right to the protection of personal data the Authority may open administrative proceedings.

(2) The provisions of the Act on the General Rules of Administrative Proceedings shall apply to administrative proceedings for data protection, subject to the exceptions set out in this Act.

(3) Administrative proceedings for data protection may be opened *ex officio* only, and it shall not be deemed to have been opened upon request even if the administrative proceedings for data protection were preceded by the Authority investigation launched upon notification. If, however, the Authority has conducted an investigation launched upon notification before the administrative proceedings for data protection, the notifier shall be informed on the opening of such proceedings, including its conclusion as well.

(4) The Authority shall open administrative proceedings for data protection if, the findings of an investigation launched upon notification or other evidence suggest any unlawful processing of personal data, and such unlawful processing:

a) concerns a wide scope of persons,

b) concerns special data, or

c) is likely to cause a significant harm or damage.

(5) The administrative time limit in administrative proceedings for data protection is two months.

Section 61

(1) In its resolution adopted in administrative proceedings for data protection, the Authority may:

a) order the rectification of any personal data that is deemed inaccurate,

b) order the blocking, erasure or destruction of personal data processed unlawfully,

c) prohibit the unlawful control or process of personal data,

d) prohibit the transfer of personal data to other countries,

e) order the information of the data subject, if it was refused by the data controller unlawfully, and

f) impose a fine.

(2) The Authority may order publication of its resolution, indicating the identification data of the controller as well, where this is deemed necessary for reasons of data protection or in connection with the rights of large numbers of data subjects under protection by this Act.

(3) The amount of the financial penalty imposed pursuant to Paragraph *f)* of Subsection (1) shall be between one hundred thousand and ten million forints.

(4) The Authority shall decide whether or not to impose a fine, and the amount of the penalty taking into account all circumstances of the case, such as in particular the number of data subjects affected by the infringement, the gravity of the infringement and whether it is a repeated offense.

(5) Before the expiry of the deadline for filing a petition for judicial review, and if judicial review has been requested, before the final court decision the data affected by the processing operation in dispute may not be erased and may not be destroyed.

33. Administrative proceedings for the control of classified data

Section 62

(1) If the findings of an investigation launched upon notification or other evidence suggest that the classification of certain national security information is unlawful, the Authority may open administrative proceedings for the control of classified data. The administrative proceedings for the control of classified data conducted by the Authority shall not concern the tasks conferred upon the Nemzeti Biztonsági Felügyelet (*National Security Authority*) by the Act on the Protection of Classified Information.

(2) The provisions of the Act on the General Rules of Administrative Proceedings shall apply to administrative proceedings for the control of classified data, subject to the exceptions set out in this Act.

(3) Administrative proceedings for the control of classified data may be opened *ex officio* only, and it shall not be deemed to have been opened upon request even if the administrative proceedings for the control of classified data were preceded by the Authority investigation launched upon notification. If, however, the Authority has conducted an investigation launched upon notification before the administrative proceedings for the control of classified data, the notifier shall be informed on the opening of such proceedings, including its conclusion as well.

Section 63

(1) In its resolution adopted in conclusion of administrative proceedings for the control of classified data, the Authority - in the event of any infringement of the regulations pertaining to the classification of certain national security information - shall call upon the classifier to

modify - in accordance with the law - the level or term of classification of information classified at the national level, or to have it declassified.

(2) The classifier, if it finds the Authority's resolution under Subsection (1) unsubstantiated, may request judicial review within sixty days following the date of delivery of the resolution. Upon receipt of the petition for judicial review, enforcement of the resolution shall be delayed. If the classifier did not seek legal action in the court of law within sixty days following the date of delivery of the resolution, the information classified at the national level shall be considered declassified on the sixty-first day following the date of delivery of the resolution, or the level or term of classification shall be modified in accordance with the resolution.

(3) The regulations of the Act on the Code of Civil Procedure on administrative actions shall apply to these court proceedings, where they shall be heard in closed session in priority proceedings.

(4) The court shall either sustain or reverse, or abolish the Authority's resolution, and may order the Authority to re-open the proceedings where deemed necessary.

(5) The court ruling or the Authority's resolution shall not affect the obligation of the classifier for the review of classified national security information, as defined by the Act on the Protection of Classified Information.

(6) The presiding judge must have the highest level of security clearance accorded under the Act on National Security Agencies.

(7) Persons other than the judge, the plaintiff and the defendant shall be allowed access to the said classified information only if they have the highest level of security clearance accorded under the Act on National Security Agencies.

34. Litigation Options for the Authority

Section 64

(1) If the data controller fails to comply with the request made under Subsection (1) of Section 56, the Authority may bring the case before the court - alleging infringement of the regulation relating to public information and information of public interest - within thirty days following the date of expiry of the time limit for providing the information under Subsection (2) of Section 56, seeking a court's ruling for ordering the data controller to act in accordance with the Authority's request.

(2) The court referred to in Subsection (5) of Section 31 shall have competence and jurisdiction to adjudicate the action aforementioned.

(3) The burden of proof to show compliance with the law lies with the data controller.

(4) Any person otherwise lacking legal capacity to be a party to legal proceedings may also be involved in such actions.

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

35. Data protection register

Section 65

(1) The Authority shall maintain official records on the processing operations of controllers in respect of personal data (hereinafter referred to as "data protection register") for the

purpose of providing assistance to data subjects containing - with the exceptions set out in Subsection (2) - the following information:

a) the purpose of data processing;

b) the legal basis of data processing;

c) scope of data subject;

d) description of the data pertaining to the data subjects;

e) the source;

f) the duration of processing;

g) the categories of data transferred, the recipients and the grounds for transfer, including transfers made to third countries;

h) name and address of the data controller 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 processing operations;

i) the nature of the data process technology used;

j) the name of and contact details of the internal data protection officer, where applicable.

(2) As regards national security agencies, the data protection register shall indicate the name and address of the given national security agency, and the purpose of and legal basis for data processing.

(3) The Authority's data protection register shall not cover operations:

a) concerning the data of the data controller's employees or members, students engaged under kindergarten education agreement, or under student or apprenticeship agreement, with or without dormitory services, or customers, other than the customers of financial institutions, public utility companies and electronic telecommunications service providers;

b) carried out in accordance with the internal rules of the recognized church;

c) that 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, or it concerns personal data processed by penal institutions in the execution of a sentence;

f) where it contains personal data for official statistical purposes, provided there are adequate guarantees that the verification of the link between the data and the data subject is definitively severed in such a way that the data subject is no longer identifiable in accordance with the relevant legislation;

g) where it concerns the data of a media content provider defined by the Act on Media Services and on the Mass Media, which are used solely for its own information activities;

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

i) where it concerns documents deposited in archive.

(4) The data protection register shall be open to the general public; it may be inspected by any person, including taking notes.

Section 66

(1) Controllers shall apply to the Authority for having their personal data processing operation registered before the commencement of processing, with the exception of mandatory processing. Apart from mandatory processing and with the exception set out in Subsection (2) of Section 68, processing may not commence prior to registration.

(2) Registration of mandatory processing shall be requested by the controller from the Authority within twenty days following the coming into force of the relevant legislation in which data processing is prescribed.

(3) In terms of registration, data controls with alternative objectives qualify as independent data control even if the same set of data is controlled.

(4) The application for registration shall contain the information specified in Subsection (1) or Subsection (2) of Section 65.

Section 67

With the exception of mandatory processing, admission to the data protection register shall be subject to an administrative service fee payable in the amount decreed by the relevant minister.

Section 68

(1) With the exception set out in Subsection (3), the Authority shall register the data processing operation within eight days from the date of receipt of the application, if it contains the information specified in Subsection (1) or Subsection (2) of Section 65.

(2) With the exception set out in Subsection (3), if the Authority fails to adopt a decision regarding the application for registration in due time, the controller may commence the processing operation according to what is contained in the application.

(3) The Authority shall register the data processing operation referred to in Subsections (4) and (5) within forty days from the date of receipt of the application, if it contains the information specified in Subsection (1) or Subsection (2) of Section 65, and if the controller is able to meet the conditions for lawful processing.

(4) If the application for registration is submitted in respect of processing operations under Subsection (5), pertaining to data files unaffected by any previous data processing operation of the controller, or for which a new process technology that the controller has never used before for any previous processing operation is required, registration shall be granted on condition that the controller is able to meet the conditions for lawful processing.

(5) The condition for registration under Subsection (4) pertains, in accordance with what is contained therein, to:

a) data files concerning authorities of nation-wide jurisdiction, employment related national data bases and national criminal records;

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

c) data files from the customer records of providers of electronic communications services.

(6) The resolution adopted by the Authority for admission into the data protection register shall contain the registration number, that the controller is required to indicate for all operations with data, such as when data is transferred or published, or when provided to the data subject. The registration number is assigned to identify the data processing operation, and it is not intended to verify the lawfulness of the operation.

(7) In the event of any change in the data specified in Paragraphs *b)-j)* of Subsection (1) of Section 65, the data controller is required to submit an application for the registration of change to the Authority within eight days from the effective date of the change. The provisions of Subsections (1), (3) and (5) shall also apply to the registration of changes, where the application shall suffice to contain the changes only.

36. Data protection audit

Section 69[8]

(1) The data protection audit is a service provided by the Authority designed to evaluate and assess data processing operations in progress or proposed along technical merits, intended to effectively implement a high level of data protection and data security system. Proposed data processing operations may be audited if deemed justified based on the elaboration of the data processing concept.

(2) Data protection audits are conducted by the Authority at the data controller's request. For the data protection audit an administrative service fee shall be charged in the amount decreed by the relevant minister.

(3) The Authority shall record the results of the data protection audit in an audit report. The audit report may also contain recommendations for the data controller. The audit report shall be considered public, unless the controller requests otherwise.

(4) The data protection audit shall not exclude the exercise of the Authority's other competencies defined in this Act.

37. Initiating criminal, infringement and disciplinary proceedings

Section 70

(1) In the event of having reasonable suspicion of alleged criminal activities in the course of its proceedings, the Authority shall initiate criminal proceedings at the body having jurisdiction to open criminal proceedings. In the event of having reasonable suspicion of alleged misdemeanour offenses or disciplinary infraction in the course of its proceedings, the Authority shall initiate infringement or disciplinary proceedings at the body having competence for conducting infringement or disciplinary proceedings.

(2) The body referred to in Subsection (1) shall notify the Authority of its opinion concerning the opening of proceedings within thirty days, unless otherwise provided for by law, and of the outcome of the proceedings within thirty days from the time of conclusion thereof.

38. Data processing and confidentiality

Section 71

(1) In its proceedings the Authority shall be entitled to process - to the extent and for the duration required - those personal data, and classified information protected by law and secrets obtained in the course of professional activities, which are related to the given proceedings, or which are to be processed with a view to concluding the procedure effectively.

(2) The Authority may use the data obtained in the course of conducting its examination for administrative proceedings.

(3) The Authority shall have access to data specified in Subsection (2) of Section 23 of Act CXI of 2011 on the Commissioner of Fundamental Rights as defined in Subsection (7) of Section 23 of Act CXI of 2011 on the Commissioner of Fundamental Rights.

(4) In proceedings related to the processing of classified information the Vice-President of the Authority, including executive officers and examiners shall - in possession of a personal

[8] Entered into force: as of 01.01.2013.

security certificate of appropriate level of clearance - be allowed access to classified information without the authorization prescribed in the Act on the Protection of Classified Information for use.

(5) The President and Vice-President of the Authority, and persons currently or formerly employed by the Authority as civil servants or in any other work-related relationship shall keep confidential any personal data, classified information, secrets protected by law and secrets obtained in the course of professional activities they may have learnt in relation to the operation and actions of the Authority as well as any other data, fact or circumstance that the Authority is not required to make available to the public - except for any disclosure or supply of data to other organizations under the relevant legislation -, during the term of their employment and after the termination thereof.

(6) According to the confidentiality requirement, the persons mentioned in Subsection (5) may not disclose unlawfully any data, facts or circumstance they obtained in connection with the performance of their official duties, nor shall they be allowed to use or reveal such information to third persons.

CHAPTER VII

CLOSING PROVISIONS

Section 72

(1) The Government is hereby authorized to decree:

a) the detailed regulations for disclosure of public information by electronic means;

b) the items covered by the fee chargeable for copies provided in connection with requests for public information, and the highest amount that can be taken into account in determining the amount of the fee, and the aspects for determining whether a document is to be considered substantial in terms of size and/or volume;

c) the compilation of special disclosure lists;

d) the data contents of the single data retrieval system and the central register, and the rules for data integration.

e) the scope of information to be made public by the national security services which they control, upon consultation with the Authority.

(2) Authorizations:

a) the minister having relevant competence is hereby authorized to publish special disclosure lists in respect of the bodies he supervises or controls, by means of a decree;

b) the minister in charge of e-administration is hereby authorized to decree the models for the standard forms to be used for the dissemination of data contained in the disclosure lists;

c)

(3) The minister in charge of the judicial system is hereby authorized to decree - upon consulting with the Authority and in agreement with the minister in charge of taxation - the amount of the administrative service fee payable for admission to the data protection register and for data protection audits, and the detailed rules relating to the collection, management, recording and refund of such fees.

Section 73

(1) This Act - with the exceptions set out in Subsections (2) and (3) - shall enter into force on the day following promulgation.

(2) Sections 1-37, Subsections (1)-(3) of Section 38, Paragraphs *a)-f)* of Subsection (4) of Section 38, Subsection (5) of Section 38, Section 39, Sections 41-68, Sections 70-72, Sections 75-77 and Sections 79-88, and Schedule No. 1 shall enter into force on 1 January 2012.

(3) Paragraphs *g)* and *h)* of Subsection (4) of Section 38 and Section 69 shall enter into force on 1 January 2013.

Section 73/A

(1)[50] Sections 26 (2) and 30 (7) of this Act amended by the Act XCI of 2013 shall be applied in procedures pending at the time of entry into force of Act XCI of 2013.

Section 74

The Prime Minister shall present a recommendation for the first President of the Authority to the President of the Republic by 15 November 2011. The President of the Republic shall appoint the first president of the Authority effective as of 1 January 2012.

Section 75

(1) The cases submitted to the data protection commissioner before 1 January 2012 shall be handled by the Authority in accordance with the provisions of this Act.

(2) The data controlled by the data protection commissioner before 1 January 2012 in an official capacity shall be transferred to the Authority effective as of 1 January 2012.

(3) Data processing operations having commenced prior to 1 January 2012, that fall within the scope of registration in the data protection register under this Act that had not been notified for registration before 1 January 2012 shall be notified to the Authority by 30 June 2012 for registration according to the relevant provisions of this Act. In the event of non-compliance data processing operations may not be carried out past 30 June 2012. Moreover, data processing operations under this Subsection may not be pursued if the Authority refused the application submitted for registration after 31 December 2011.

Section 76

Chapter V of this Act shall be considered a cardinal provision pursuant to Article VI(3) of the Fundamental Law.

Section 77

This Act facilitates compliance with:

a) 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;

b) Directive 2003/4/EC of the European Parliament and of the Council of 28 January 2003 on public access to environmental information and repealing Council Directive 90/313/EEC;

c) Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information;

d) Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

Section 78

(1)-(2)[9]

(3) The term “descending” to be found in Section 9 (7) of the Law Decree 17 of 1982 on Registers, Marriage Proceedings and the Use of Name shall be replaced by the term “descending found”.

(4) Section 25 (3) of the Act XXIV of 2011 on legal harmonisation of Acts on Europol, on Security Services and the Activities of Private Investigators (SSAPI), on Firearms and Pyrotechnic Devices enters into with the following wording:

„(3) Section 31 (1) g) shall be replaced by „the Chamber shall keep a register of its natural person members and enterprises till the termination of membership in accordance with the provisions of this Act and also supplies statistical data anonymously.”

(5) Section 41 (3) b) of the Act XXIV of 2011 on legal harmonisation of Acts on Europol, on Security Services and the Activities of Private Investigators (SSAPI), on Firearms and Pyrotechnic Devices enters into force with the following wording:

(Repealed):

„b) the wording „gas and alarm weapon” in Section 27 (4) on SSAPI, „which can be prolonged in every second year upon request of the member” in Section 40 (2), „period” in Section 54 (1)-(2).

(6) Section 42 j) of the Act XXIV of 2011 on legal harmonisation of Acts on Europol, on Security Services and the Activities of Private Investigators (SSAPI), on Firearms and Pyrotechnic Devices enters into force with the following wording:

(SSAPI)

j) the wording „security technology- property protection” in Section 26 (1) e) shall be replaced by „electronic property protection”, „electronic security technology” in Section 28 (2) d) by „electronic property protection”, the Act LXIII of 1992 by this Act, „security technology” in Section 32 (5) by „electronic property protection”, „the kind of security technology- property protection” in Section 74 (7) by „electronic property protection”.

(7) Section 42 l) of the Act XXIV of 2011 on legal harmonisation of Acts on Europol, on Security Services and the Activities of Private Investigators (SSAPI), on Firearms and Pyrotechnic Devices enters into force with the following wording:

(SSAPI)

„l) in Sections 30 (1) and (4), 32 (1) the text “Avtv.” shall be replaced by “Infotv.”, in Section 63 (4) the text „an unauthorised person and property protection as well as private investigator” shall be replaced by „unauthorised person and property protection” in accordance with Section 13 of Government decree 218/1999. (XII. 28.) on Misdemeanours, in

[9] Repealed by Section 110 of the Act LXXVI of 2013 as of 01.07.2013.

Section 39 (3) the text „presenting his ID pass" shall be replaced by „in his application for chamber membership".

(8) Section 34 (1) c) enacted by Section 23 of the Act XXIV of 2011 on legal harmonisation of Acts on Europol, on Security Services and the Activities of Private Investigators (SSAPI), on Firearms and Pyrotechnic Devices enters into force with the following wording:

(The private investigator in order to conclude the contract)

„may produce or use visual or audiovisual recordings in accordance with the framework of the relevant contract and in compliance with the regulations of this Act on data protection and personality rights",

(9) Section 15 (3) of the Act LXXVII. Of 2011 on World Heritage shall not enter into force.

Section 80

(1) The following Point n) shall be added to Article 51 (2) of Act CXII of 1996 on credit institutions and financial corporations:

[Pursuant to Point b) of paragraph (2), the obligation to safeguard bank secrets does not apply]

"*n)* to the National Authority for Data Protection and Freedom of Information within its competent scope of responsibilities"

(contrary to requests made in writing by these bodies to the financial institution.)

(2) The following Point r) shall be added to Article 157 (1) of Act LX of 2003 on insurance companies and insurance activities:

(The obligation to safeguard insurance secrets does not apply)

"*r)* in the case of the National Authority for Data Protection and Freedom of Information within their respective scope of responsibilities"

[contrary to how should the body or individual specified under Points a)-j), n) and s) be entitled to submit a request in writing containing the name of the client or the insurance contract number, the type of data requested, the objective of the data request and its legal grounds on condition that the body or individual specified under points k), l), m), p) and q) is exclusively obliged to provide the type of data requested and its legal grounds. Reference to the legislation authorising data access equally qualifies as certification of the objective indicated and the legal status.]

(3) The following Point m) shall be added to Article 8 (2) of Act LVII of 2004 on the legal status of Hungarian MPs delegated to the European Parliament:

"*m)* The President and Vice-President of the National Authority for Data Protection and Freedom of Information."

(cannot be a Member of the European Parliament)

(4) The following Point k) shall be added to Article 118 (3) of Act CXXXVIII of 2007 on investment companies and commodity exchange service providers, as well as rules concerning the activities they may engage in:

(The confidentiality obligation defined under paragraph [1] does not apply)

"*r)* to the National Authority for Data Protection and Freedom of Information within its respective scope of responsibilities"

(contrary to requests made in writing by these bodies to the investment companies or commodity exchange service providers.)

(5) The following Point q) and final text shall be added to Article 88 (1) of Act CLIX of 2007 on collaterals:

(In accordance with the present Act, the obligation to safeguard insurance secrets does not apply)

"*q)* to the National Authority for Data Protection and Freedom of Information within its respective scope of responsibilities."

(6) The following Point h) shall be added to Article 13 (3) of Act CLV of 2009 on the protection of confidential information:

(In regard to the provision of state or public duties)

"*h)* the President of the National Authority for Data Protection and Freedom of Information"

[is authorised to exercise regulatory licenses defined in Point a) and b) of Article 18 (2) without holding any national security clearance, personal security attestation, as well as a confidentiality statement and user permit in connection with classified information within their respective scope of responsibilities and authority.]

Section 81

(1) The text "the minister competent for the professional supervision of the registration body, the data protection commissioner or the individual authorised by this commissioner" in Article 21/H of Act I of 1998 on road transport shall be replaced by the text " the minister competent for the professional supervision of the registration body or the individual authorised by this minister, as well as the President, Vice-President and civil servant of the National Authority for Data Protection and Freedom of Information".

(2) The text "the Office of the Constitutional Court" in Article 1 (2) of Act XXIII of 1992 on the legal status of civil servants (hereinafter Civil Service Act) shall be replaced by the text " Office of the Constitutional Court and the National Authority for Data Protection and Freedom of Information".

(3) The text "at the Hungarian Competition Authority" in Article 44 (1) of the Civil Service Act shall be replaced by the text "at the Hungarian Competition Authority and the National Authority for Data Protection and Freedom of Information" .

(4) The text "the data protection commissioner" in Point i) of Article 63 (1) of the Civil Service Act shall be replaced by the text "the National Authority for Data Protection and Freedom of Information".

(5) The text "the data protection commissioner" in Article 7 (3) of Act XLVI of 1993 on statistics shall be replaced by the text "President of the National Authority for Data Protection and Freedom of Information"; the text "data protection commissioner" in Article 19 (3) shall be replaced by the text "the National Authority for Data Protection and Freedom of Information".

(6) The text "within the scope of the Data Protection Act" in Article 5 (1) of Act CXIX of 1995 on the control of name and address data facilitating research and direct business acquisition shall be replaced by the text "within the scope of the Act on informational self-

determination and freedom of information"; the text "Data Protection Act" in Article 19 shall be replaced by the text "the Act on informational self-determination and freedom of information".

(7) The text "the minister competent for the professional supervision of the infringement registration body" in Article 27/F of Act LXIX of 1999 on infringements shall be replaced by the text "the minister competent for the professional supervision of the infringement registration body or the individual authorised by the minster, as well as the President, Vice-President and civil servant of the National Authority for Data Protection and Freedom of Information".

(8) The text "within the framework of the data protection procedure, the data protection commissioner" in Point b) of Article 4/G (2) of Act LXXV on regulations governing action against organised crime and specific phenomena associated with this and related legislative amendments shall be replaced by the text "the National Authority for Data Protection and Freedom of Information".

(9) The text "the data protection commissioner" in Article 32 (4) and (7) of Act LXXXIV of 1999 on road transport registration shall be replaced by the text "the National Authority for Data Protection and Freedom of Information"; the text "data protection commissioner" in paragraph of Article 32 (8) shall be replaced by the text "the National Authority for Data Protection and Freedom of Information".

(10) The text "the data protection commissioner" in Article 75/O of Act CXXX of 2003 on cooperation in criminal cases with EU Member States shall be replaced by the text " the National Authority for Data Protection and Freedom of Information".

(11) The text "the data protection commissioner" in Article 164 (5) and in Point a) of Article 174 (3) of Act CXL of 2004 on the general rules on administrative proceedings and services shall be replaced by the text "the National Authority for Data Protection and Freedom of Information".

(12) The text "the data protection commissioner" in Article 85 (3) of Act I of 2007 on the entry and residence of persons with the right of the freedom of movement and residence shall be replaced by the text "the National Authority for Data Protection and Freedom of Information".

(13) The text "within the scope of the procedure defined under the Act on the protection of personal data and the disclosure of data of public interest, the data protection commissioner" in Article 6 of Act CI of 2007 on ensuring access to data required for decision preparation shall be replaced by the text "the National Authority for Data Protection and Freedom of Information".

(14) The text "the data protection commissioner" in Article 18 (6) and Article 20 (2) of Act CV of 2007 on cooperation and information exchange carried out within the framework of the Convention implementing the Schengen Agreement shall be replaced by the text "the National Authority for Data Protection and Freedom of Information"; the text "pursuant to regulations set out under the Act on the protection of personal data and the disclosure of data of public interest, the data protection commissioner" in Article 20 (1) shall be replaced by the text "the National Authority for Data Protection and Freedom of Information".

(15) The text "the data commissioner competent to act in respect of Act on the protection of personal data and the disclosure of data of public interest and controlling compliance with the Act on the control of personal data" in Article 88 (2) of Act XLVII of 2009 on the criminal database, the registration of verdicts brought against Hungarian nationals in the courts of

European Union Member States and the registration of criminal and biometric data shall be replaced by the text "the National Authority for Data Protection and Freedom of Information competent to act in respect of controlling compliance with provisions governing the Act on the control of personal data"; the text "together with data protection commissioner" in Article 91/A (2) shall be replaced by the text "together with the National Authority for Data Protection and Freedom of Information"; the text "data protection commissioner" in Article 91/A (3) shall be replaced by the text "the National Authority for Data Protection and Freedom of Information".

(16) The text "as well as within the scope of authority ensured in Act LXIII of 1992 on the protection of personal data and the disclosure of data of public interest, the data protection commissioner" in Article 7 (8) of Act CIV of 2009 on the proclamation of the agreement regarding processing the data of passenger number records (PNR) between the European Union and the United States of America and the transfer of this data to the Department of Home Security amending Act XCII of 1995 on air transport shall be replaced by the text "as well as within the scope of authority ensured in the Act on the right of informational self-determination and freedom of information, the National Authority for Data Protection and Freedom of Information".

(17) The text "the data protection commissioner" in the eighth paragraph of Article 6 of Act CLV of 2009 on the protection of classified information shall be replaced by the text "the National Authority for Data Protection and Freedom of Information"; the text "together with the data protection commissioner" in Point r) of the second paragraph of Article 20 shall be replaced by the text "together with the National Authority for Data Protection and Freedom of Information".

(18) The text "the data protection commissioner and an authorised associated employee" in Point j) of the first paragraph of Article 76 of Act CXXII of 2010 on the National Tax and Customs Authority shall be replaced by the text "President, Vice-President and civil servant of the National Authority for Data Protection and Freedom of Information".

(19) The text "the data protection commissioner shall undertake supervision within their respective scope of authority ensured by Act LXIII of 1992 on the protection of personal data and the disclosure of data of public interest" in the fifth paragraph of Article 7 of Act LVI of 2011 on the proclamation of the Convention on the South-East European Law Enforcement Centre signed in Bucharest on 9 December 2009 and the Protocol on the privileges and immunities of the South-East European Law Enforcement Centre signed in Bucharest on 24 November 2010 shall be replaced by the text "the National Authority for Data Protection and Freedom of Information shall undertake the supervision".

Section 82-89

Annex No. 1 to Act CXII of 2011

STANDARD DISCLOSURE LIST

I. Organizational information, staff particulars

	Data description	Updating	Duration of processing
1.	Official name, registered office, postal address, telephone and fax number, electronic mail address, website and customer service contact information of	Immediately upon the change taking effect	Previous data shall be deleted

	the body with public service functions		
2.	Organizational structure of the body with public service functions, showing the departments, and the tasks and duties of each department	Immediately upon the change taking effect	Previous data shall be deleted
3.	Name and title of the executive employees of the body with public service functions and its departments, including contact information (telephone and fax number, electronic mail address)	Immediately upon the change taking effect	Previous data shall be deleted
4.	Name of the head of customer relations, including contact information (telephone and fax number, electronic mail address) and customer service hours	Immediately upon the change taking effect	Previous data shall be deleted
5.	In respect of collegiate bodies, number of members and composition, name, title and contact information of members	Immediately upon the change taking effect	Previous data shall be deleted
6.	Name of any other body with public service functions under the control, supervision or oversight of, or subordinated to the body with public service functions, including the particulars specified in Point 1	Immediately upon the change taking effect	Previous data shall be archived for a period of one year
7.	Name, registered office and contact information (postal address, telephone and fax number, electronic mail address) of any economic operator in which the body with public service functions has a majority ownership share or participation, including scope of activities, name of representative, and the percentage of the share the body with public service functions controls	Immediately upon the change taking effect	Previous data shall be archived for a period of one year
8.	Name, registered office and contact information (postal address, telephone and fax number, electronic mail address) of any public foundation established by the body with public service functions, including the bylaws, and the name of the managing body	Immediately upon the change taking effect	Previous data shall be archived for a period of one year
9.	Name and registered office of any publicly-financed entity founded by the body with public service functions, reference to the legislation or resolution based on which the publicly-financed entity is established, charter document, head of the publicly-financed entity, website address, operating permit	Immediately upon the change taking effect	Previous data shall be archived for a period of one year

10.	Name of any publication founded by the body with public service functions, editor's and publisher's name and address, name of the editor in chief	Immediately upon the change taking effect	Previous data shall be archived for a period of one year
11.	Particulars specified in Point 1 of the superior or supervisory body of the body with public service functions, or the body empowered to hear appeal cases relating to its regulatory decisions, or failing this, of the body exercising legal supervision of the body with public service functions	Immediately upon the change taking effect	Previous data shall be archived for a period of one year

II. Information relating to activities and operations

	Data description	Updating	Duration of processing
1.	Unabridged version of the laws governing the responsibilities, competence and core activity of the body with public service functions, legal act for the governance of bodies governed by public law, organizational and operational regulations or operating procedures, data protection and data security regulations	Immediately upon the change taking effect	Previous data shall be archived for a period of one year
2.	In connection with bodies of nation-wide jurisdiction and county and capital government offices, an information pamphlet on the duties and activities of the body with public service functions in Hungarian and English	Immediately upon the change taking effect	Previous data shall be deleted
3.	Voluntary tasks of municipal governments	Quarterly	Previous data shall be archived for a period of one year
4.	In connection with public administration, municipal government and other regulatory cases, name of the body having competence separately for each type of case and procedure, or the name and area of jurisdiction of the body actually proceeding where powers had been transferred, description of documents and other deeds required, procedural fees (administrative service fees), basic procedural rules, means (place and time) for the submission of documents for the opening of proceedings, office hours, administrative time limits (deadlines for processing and for appeals), guidelines, general information on handling cases and standard forms for downloading, access to electronic programs available for use,	Immediately upon the change taking effect	Previous data shall be deleted

	appointments, list of legislation for different types of cases, information on clients' rights and obligations		
5.	Description and contents of public services provided by the body with public service functions or financed from budget, rules of access to public services, amount of fees charged for public services, any allowances from such fees	Immediately upon the change taking effect	Previous data shall be archived for a period of one year
6.	Descriptive information on databases and registers maintained by the body with public service functions (name, format, purpose and legal basis of processing, duration of processing, data subjects involved, data sources, questionnaire, where applicable), particulars for the identification of records to be notified for the data protection register; type of data collected and processed by the body with public service functions within the framework of its principal activity, means of access, costs of making copies	Immediately upon the change taking effect	Previous data shall be archived for a period of one year
7.	Title and subject of publications of the body with public service functions, means of access, price of the publication, if any	Quarterly	Previous data shall be archived for a period of one year
8.	In respect of collegiate bodies, decision-making process, means of participation by the general public (opinionate), procedural rules, place and time of settings of the collegiate body, publicity, decisions, minutes or summaries of meetings; information on voting in the collegiate body, if this is not restricted by law	Immediately upon the change taking effect	Previous data shall be archived for a period of one year
9.	Legislative proposals and related documents to be published by virtue of law; motions and proposals submitted to public meetings of the councils of local self-governments from the time of submission	Unless otherwise provided for by law, immediately from the time of submission	Previous data shall be archived for a period of one year
10.	Public announcements and statements made by the body with public service functions	Continuously	Archived for a period of at least one year
11.	Technical description of tenders published by the body with public service functions, the outcome of such procedure and the reasons	Continuously	Previous data shall be archived for a period of one year
12.	Public findings of examinations and inspections carried out in connection with the core activity of the body with public service functions	Immediately upon receiving the report on the examination	Previous data shall be archived for a period of one year

13.	Procedure for handling requests for access to public information, name and contact information of the competent department, and the name of the data protection officer or the person handling information rights, where applicable	Quarterly	Previous data shall be deleted
14.	Results of gathering statistical information relating to the activity of the body with public service functions, showing changes over time thereof	Quarterly	Previous data shall be archived for a period of one year
15.	Information pertaining to a given body from mandatory data disclosure relating to public information	Quarterly	Previous data shall be archived for a period of one year
16.	List of contracts for the use of public information to which the body with public service functions is a party	Quarterly	Previous data shall be archived for a period of one year
17.	Standard contract conditions relating to the use of public information processed by the body with public service functions	Immediately upon the change taking effect	Previous data shall be archived for a period of one year
18.	Special and ad hoc publication lists pertaining to the body with public service functions	Immediately upon the change taking effect	Previous data shall be deleted

III. Financial data

	Data description	Updating	Duration of processing
1.	Annual (fiscal) budget of the body with public service functions, annual accounts under the Accounting Act or the annual budget report	Immediately upon the change taking effect	For ten years following the time of publication
2.	Consolidated data on the staff of the body with public service functions, including personal benefits provided, and the remuneration, salary and regular benefits of executive officers and managers, in total, including their expense accounts, description and amounts of benefits provided to other employees	Quarterly	For the time period defined by specific other legislation, archived for at least one year
3.	Information as to the names of beneficiaries to whom the body with public service functions provided any central subsidies, the purpose and the amount of the aid, showing also the place of implementation of the support program, except if the central subsidies are withdrawn before the time of publication or if the beneficiary declined to accept	By the sixtieth day following the date of the decision	For five years following the time of publication
4.	Description of contracts relating to the allocation of public funds, management of public assets concerning the purchases of	By the sixtieth day following the date of the decision	For five years following the time of publication

	supplies and services, and works contracts worth five million forints or more, or to the sale or utilization of assets, for the transfer of assets or rights, as well as concession contracts, including the type and subject matter of such contracts, names of the parties to the contract, the contract amounts, and the duration of fixed term contracts, including changes in the data abovementioned, with the exception of information on procurements directly related to and deemed necessary for reasons of national security or national defense, and with the exception of classified information Contract value shall mean the price agreed upon for the subject matter of the contract - exclusive of value added tax -, or in the case of gratuitous transactions, the market value or book value of the asset in question, whichever is higher. As regards periodically recurring contracts concluded for more than one year the contract value shall indicate the price calculated for one year. The value of contracts concluded within the same financial year with the same party shall be applied cumulatively.		
5.	Information made public according to the Act on Concessions (tender notices, particulars of tenderers, memos on evaluation procedures, outcome of such tender procedures)	Quarterly	For the time period defined by specific other legislation, archived for at least one year
6.	Payments of more than five million forints made by the body with public service functions outside the scope its basic functions (such as payments made to support association, to trade organizations representing the interests of its workers, to organizations active in educational, cultural, social and sports activities and services provided to its employees, and to foundations to support their activities)	Quarterly	For the time period defined by specific other legislation, archived for at least one year
7.	Description of developments implemented from European Union funding, including the related contracts	Quarterly	Archived for a period of at least one year
8.	Public procurement information (annual plan, summary of the evaluation of tenders, contracts awarded)	Quarterly	Archived for a period of at least one year