Act CXII of 2011

On Informational Self-determination and Freedom of Information[1]

In order to ensure the right to informational self-determination and freedom of information, and to facilitate the implementation of the Fundamental Law, the National Assembly 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, as well as on the authority competent to control these rules pursuant to Article VI of the Fundamental Law:

CHAPTER 1

GENERAL PROVISIONS

1. Object of the Act

Section 1

The object of this Act is to define the fundamental rules applied in connection with controlling data with the aim of ensuring that the controllers respect the private sphere of natural persons and ensuring public transparency through the enforcement of rights to access and disseminate data of public interest and data public on grounds of public interest.

2. Scope of Effect of the Act

Section 2

(1) The scope of the present Act encompasses 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 control and data processing fully or partially undertaken by automated devices, as well as manually.

(3) Provisions set out in the present Act shall apply if the controller controlling 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 controlling data exclusively for their own personal purposes.

(5) Concerning further use of public sector information, other rules can be laid down by law for the mode and conditions of data provision the consideration to be paid for it, as well as in respect of legal redress, to the rules defined within the scope of the present Act.

3. Definitions

Section 3

For the purposes of the present Act:

1. *Data subject*: any natural person identified or directly or indirectly identifiable on the basis of personal data.

2. *Personal data*: data relating to the data subject, in particular the name and identification number of the data subject, as well as 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*:

a) personal data concerning racial or national origin, political opinion or party membership, religious or other philosophical belief, membership in an interest representation organisation, sex life;

b) personal data concerning health, addiction, as well as criminal personal data.

4. *Criminal personal data*: personal data relating to the data subject or a criminal record, generated in the course of or prior to the criminal proceedings, in connection with the offence or criminal proceedings, at the bodies authorised to carry out criminal proceedings or to detect offences, as well as at penal institutions.

5. *Data of public interest*: information or data other then personal data registered in any mode or form concerning activities undertaken and controlled by the body or individual carrying out state or local government responsibilities, as well as other public duties defined in relevant legislation, regardless of their mode of control, independent or collective nature; therefore, with special regard to data concerning the scope of authority, competence, organisational structure, professional activity and evaluation equally encompassing its effectiveness, the type of data held and legislation regulating operation, as well as data concerning financial management and concluded contracts.

6. *Data public on grounds of public interest*: data other then data of public interest, the disclosure of or the access to which is provided for by the law, in the public interest.

7. *Consent*: any freely 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 controlled fully or to the extent of specific operations.

8. *Objection*: declaration made by the data subject objecting to the control of his personal data to request the termination of data control, as well as the deletion of the data controlled.

9. *Controller*: natural or legal person, or organisation without legal personality which alone or jointly with others determines the purposes and means of the control of the data; makes and executes decisions concerning data control (including the means used) or contracts a data processor to execute it.

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

11. *Data transfer*: ensuring access to the data for a third party.

12. *Disclosure*: ensuring open access to the data.

13. *Data deletion*: making data unrecognisable in a way that it can never again be restored.

14. *Tagging data*: marking data with a special ID tag to differentiate such data.

15. *Blocking data*: marking data with a special ID tag to indefinitely or definitely restrict its further control.

16. *Data destruction*: complete physical destruction of the data carrier recording the data.

17. *Data processing*: undertaking technical tasks in connection with data control operations, regardless of the method and means used for executing the operations, as well as the place of use, provided that the technical task is performed on the data.

18. *Data processor*: natural or legal person or organisation without legal personality processing the data on the grounds of a contract concluded with the controller, including contracts conducted upon

legislative provisions.

19. *Data officer*: 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 publisher*: the body responsible for undertaking the public responsibility which uploads the data sent by the data control officer, if this officer has not published the data.

21. *Data set*: total data controlled 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 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 on the one hand and the State which is not party to the Agreement on the European Economic Area on the other hand.

24. *Third country*: any State that is not an EEA State.

CHAPTER 2

PROTECTION OF PERSONAL DATA

4. Principles of Data Control

Section 4

(1) Personal data may exclusively be controlled for a specific purpose to realize rights and fulfill obligations. Data control must at every stage comply with the objective of the data control; data must be recorded and controlled in a fair and legal manner.

(2) Only personal data essentially needed to satisfy the aim of the control, appropriate for achieving the goal may be controlled. Personal data may only be controlled to the extent and for the time required to achieve the goal.

(3) Throughout the data control process, personal data shall be classified as such until its connection with the data subject can be restored. The connection with the data subject can be restored if the data controller has the technical conditions required for restoration at his or her disposal.

(4) It has to be ensured during the course of control that the data are accurate, complete and – if required for the data control – updated, and that the data subject is only identifiable for the time required for the data control.

5. Legal Basis of Data Control

Section 5

(1) Personal data may be controlled if

a. the data subject agrees to it, or
b. it is provided for by law or – on the grounds of authorisation of law, within the scope defined in that law – by or pursuant to a local government decree for a purpose based on public interest (hereinafter mandatory data control).

(2) Special data may be controlled in cases listed in Section 6 or if

a. the data subject agrees to it in writing;
b. this is necessary to implement an international treaty adopted within the framework of a law in the case of data listed in Section 3 Subsection 3.a), or is provided for by law to enforce basic rights ensured in the Fundamental Law, serves the interests of national security,

prevents offences, assists prosecution or serves national defence interests, or

c. is provided for by law for purposes in the public interest in the case of data listed in Section 3 Subsection 3.

(3) In the case of mandatory data control, the law or local government decree providing for the data control determines the type of data to be controlled, the objective and conditions of data control, access to data, the duration of data control, as well as the person of the controller.

(4) Only state or local government bodies are entitled to control criminal personal data linked to the prevention and prosecution of offences and controlled to perform public administration and judicial administration tasks, as well as databases registering data in connection with infringements of the rule of law, civil litigation and non-litigation matters.

Section 6

(1) Personal data may also be controlled if it is not possible to obtain the consent of the data subject or even if the cost of doing so is excessively high and the personal data

a. must be controlled to fulfill legal obligations applicable to the controller, or
b. must be controlled to enforce the rightful interests of the controller or third parties and the enforcement of such interests is proportionate to the restrictions pertaining to the right to the protection of personal data.

(2) Should the data subject be unable to provide his consent because of his incapacity to act or other circumstances beyond his control, the personal data of the data subject may be controlled during the period in which consent is unavailable, to protect his own or others' vital interests, as well as to the extent required to avert and prevent direct risks posing a threat to the lives, corporal integrity or property of persons.

(3) The consent or subsequent approval of a legal guardian is not required in the case of legal declarations containing the consent of minors aged over 16.

(4) Should the aim of the control based on consent relate to executing the contract concluded in writing with the controller, such contract must include all the information the data subject must be aware of – on the grounds of the present legislation – relating to the control of personal data, and therefore, in particular, the determination of the data to be controlled, the duration of control, the purpose of use, evidence of the transfer of data, its recipients and the evidence of the use of a data processor. The contract must clearly and explicitly include that by signing it, the data subject consents to the control of its data in accordance with the conditions set out in the contract.

(5) If personal data was recorded with the consent of the data subject, the controller may, should it not otherwise be regulated by law, also control the data recorded

a. to fulfil their relevant legal obligations, or
b. to enforce the rightful interest of the controller or third party should the enforcement of these interests be proportionate to restrictions pertaining to the protection of personal data

without having to secure any additional special consent, even after the data subject withdraws their consent.

(6) A legal opinion must be issued in respect of the personal data provided in the consent by the data subject and required to conduct the legal or administrative proceedings launched pursuant to the request or initiative of the data subject, or in respect of the personal data they provided in the event of other matters being launched pursuant to the request of the data subject.

(7) The consent of the data subject shall be considered as a fact in regard to personal data announced or disclosed by the data subject during public appearances.

(8) Should doubts arise, a legal opinion must be issued setting forth how the data subject failed to provide their consent.

6. The Requirement of Data Protection

Section 7

(1) The controller must plan and execute control operations in a way that these ensure the protection of the private sphere throughout the application of the present Act and other regulations applicable in connection with data control.

(2) The controller, as well as the data processor within their respective scope of activities, is obliged to ensure data security, institute technical and organisational measures and develop procedural rules required to enforce the present Act, as well as other data protection and confidentiality rules.

(3) Through the institution of the appropriate measures the data must be particularly protected from unauthorised access, modification, transfer, disclosure, deletion or destruction, accidental destruction and damage as well as disabled access occurring due to changes to the technology applied.

(4) In order to protect data sets controlled electronically in various files it is necessary to ensure that – unless otherwise permitted by law - data stored in files cannot be directly connected and linked to the data subject by ensuring the appropriate technological solutions.

(5) During the course of the automated processing of personal data, the controller and data processor ensures the following by taking additional measures:

a. prevents unauthorised data entry;
b. prevents the use of automatic data processing systems by unauthorised persons by using data transfer devices;
c. ensures the ability to control and determine which bodies the personal data have or can be sent to by using a data transfer device;
d. ensures the ability to control and determine which personal data has been registered in the automatic data processing systems, when this was done and who did it;
e. ensures the ability to restore the systems installed in the event of malfunctions and;
f. compiles a report on errors occurring during the course of automated processing.
    a. The controller and data processor must take account of the current level of development of the relevant technology when determining and applying measures taken to protect the data. The solution which ensures a higher level protection of the personal data must be selected from among several possible control solutions, unless this proves far too difficult for the controller.

7. Data Transfer to Other Countries

Section 8

(1) Data processors under the scope of the present Act are authorised to transfer personal data to controllers or data processors undertaking data control in third countries should

a. the data subject have provided their explicit consent, or
b. conditions set out under Section 5 and Section 6 have been fulfilled and the adequate level 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 control of the personal data is ensured should

a. this be stated in a binding legal act of the European Union, or
b. an international treaty specifically containing the enforcement of rights specified under Section 14 and the assurance of legal redress for the data subject, as well as rules guaranteeing the independent control of the control and data processing procedure concluded between the third country and Hungary be in effect.

(3) Personal data may be transferred to third countries to execute an international agreement to

facilitate mutual legal assistance between authorities and the avoidance of double taxation for the purpose, in accordance with the conditions and scope of data defined in the international agreement, even if conditions set out in subsection (2) do not prevail.

(4) Data transfer to an EEA State shall be considered data transfer performed within the territory of Hungary.

8. Restrictions to Data Control

Section 9

(1) Should pursuant to provisions governing relevant legislation, international treaties or EU standard contractual clauses, the controller receive personal data in a manner that the data transferring controller concurrently to the transferral of the data indicates

a. the possible objective of the control,
b. possible duration of the control,
c. possible recipients of the data transferred,
d. restriction to rights ensured for the data subject within the scope of present Act, or
e. other restrictions regarding control

in connection with the personal data (hereinafter jointly referred to as control restrictions), the controller receiving the personal data (hereinafter data recipient) controls the personal data in accordance with the extent and mode of restrictions applicable to control and guarantees the rights of the data subject in accordance with restrictions applicable to control.

(2) The data recipient is also entitled to control the personal data irrespective of control restrictions and to guarantee the rights of the data subject should the data transfer controller have been provided their preliminary consent to do so.

(3) Pursuant to provisions governing relevant legislation, international treaties or EU standard contractual clauses, the controller shall notify the recipient of the control restrictions to be applied concurrently to transferring the personal data.

(4) The controller is entitled to provide the consent specified in subsection (2), should this not conflict with legal provisions to be applied in respect of legal subjects under the scope of the jurisdiction of Hungary.

(5) Pursuant to their request, the data recipient notifies the data transferring controller of the use of the personal data received.

9. Data Processing

Section 10

(1) The controller defines the rights and obligations of the data processor in regard to the processing of personal data within the framework of the present Act, as well as relevant special legislation adopted in connection with the control of data. The controller is responsible for the legitimacy of the instructions they issue.

(2) The data processor is not permitted to collaborate with other data processors during the course of the provision of their respective activities.

(3) The data processor is not authorised to make any decision effectively affecting the control of the data; is exclusively authorised to process the personal data they acquired knowledge of in accordance with the instructions issued by the controller; is not authorised to process data for their own personal purposes and shall store and safeguard the personal data in compliance with the instructions issued by the controller.

(4) The contract concerning data processing must be concluded in writing. Any organisation with vested interests in the use of the personal data to be processed for business purposes cannot be

contracted to undertake data processing.

10. A Decision made on the Grounds of Automated Data Processing

Section 11

(1) A decision based on the evaluation of the personal characteristics of the data subject exclusively by means of automated data processing can only be made, should the decision

a. Have been made when the given contract was concluded or during its performance on condition that the data subject initiated this, or
b. this have been authorised by relevant legislation which also specifies measures protecting the rightful interests of the data subject.

(2) Pursuant to their request, the data subject must be notified of the method applied and its key components in the case of decisions made by means of automated data processing and the data subject must be ensured the opportunity to present their position.

11. Personal Data Control in Scientific Research

Section 12

(1) Personal data recorded for scientific research purposes can only be used for scientific research.

(2) Linking the personal data to the data subject – as soon as the objective of the research permits – must be definitively blocked. Data that can be used to identify specific or identifiable individuals must also be stored separately until this is completed. This data can only be linked to other data should this be required for the purpose of the research.

(3) The organisation or individual conducting the scientific research is only entitled to disclose the personal data should

a. the data subject consent to this, or
b. this be required to present the results of research conducted in connection with historical events.

12. Use of Personal Data for Statistical Purposes

Section 13

(1) Unless otherwise regulated by law, the Hungarian Statistical Office may receive personal data that can be used for individual identification controlled within the framework of mandatory control for statistical purposes and is entitled to control these in accordance with the mode defined under the relevant legislation.

(2) Unless otherwise regulated by law, personal data recorded, received or processed for statistical purposes may only be used for statistical purposes. Regulations pertaining to the control of personal data for statistical purposes are defined in separate legislation.

13. Rights of Data Subjects and their Enforcement

Section 14

The data subject may request the following from the controller:

a. information on the control of personal data,
b. correction of personal data, and
c. deletion, blocking of personal data, with the exception of mandatory control.

Section 15

(1) Pursuant to the request of the data subject, the controller is entitled to provide information on the subject's data they control, as well as the data processed by the data processor they contracted, their sources, the objective of the control, its legal grounds and duration, the name and address of the

data processor and the activities they undertake in connection with control, in addition to the legal grounds and recipients should the personal data of the data subject not be transferred.

(2) The controller keeps a record of data transferred to verify the legitimacy of the data transferral and informs the data subject which file details the date on which the personal data they controlled was sent, the legal grounds of this action and its recipients, the specific scope of the personal data sent, as well as other data specified in legislation prescribing control.

(3) The Act prescribing control may restrict the duration of the obligation to safeguard data set out in subsection (2) in the data transfer file, and therefore, the information notification period. Within the scope of this restriction, a minimum period of five years applies in the case of personal data and a minimum of 20 years in the case of special data.

(4) The controller shall provide clear information in writing within the shortest possible space of time following the submission of the request; however, no later than within 30 days.

(5) Information specified in subsection (4) is provided free of charge, if the individual requesting the information has not yet submitted a request for information to the controller in connection with the same scope of data in the same year. The rate of reimbursement of costs may also be specified in the contract concluded by the parties. Reimbursed costs that have already been paid must be reimbursed in the event that the data was illegitimately controlled, or the request for information leads to correction.

Section 16

(1) The controller is only entitled to deny a request for information in cases specified in Section 9 (1) and Section 19.

(2) Should a request for information be denied, the controller must notify the data subject of this in writing by referring to the relevant section of the present Act on what grounds the request for information was denied. Should a request for information be denied, the controller must inform the data subject of the means available to facilitate legal redress in court and contact the National Authority for Data Protection and Freedom of Information (hereinafter Authority) to seek help.

(3) The controller keeps the Authority informed about rejected requests each year up to 31 January following the year under review.

Section 17

(1) The controller shall correct the personal data should the personal data not be authentic and the controller has access to the authentic personal data.

(2) Personal data must be deleted should

a. its control be illegal;
b. it have been requested by the data subject in accordance with point c) of Section 14;
c. it be incomplete or incorrect – and this cannot be legitimately changed – on condition that the law does not rule out deletion;
d. the objective of the control have ceased to exist or the period defined in the relevant legislation for storing the data have expired;
e. it have been ordered by the court or the Authority.

(3) Deletion obligations do not apply to personal data which is recorded on a data carrier which must be placed in the archives in accordance with legislation governing the preservation of archival materials in cases specified in subsection (2)(d).

(4) Instead of deletion, the controller blocks the personal data should the data subject request this, or in the event that the basis of the information available, deletion would presumably violate the rightful interests of the data subject. Personal data blocked through such means may exclusively be controlled while the control objective remains valid which barred the deletion of the personal data.

(5) The controller tags the personal data they control should the data subject dispute its correctness or accuracy, yet it is not possible to explicitly verify the incorrectness or inaccuracy of the disputed personal data.

Section 18

(1) The data subject, as well as everyone to whom the data was transferred for control purposes, must be notified of any correction, blocking and deletion. Exemptions apply should this not violate the rightful interest of the data subject in respect of the objective of control.

(2) Should the controller fail to fulfil the request of the data subject regarding correction, blocking or deletion, the controller shall provide the reasons and legal grounds for rejecting the request submitted in connection with correction, blocking or deletion within a period of 30 days following the receipt of the request. Should the request for correction, blocking or deletion be rejected, the controller shall notify the data subject of the opportunities available to seek legal redress via the courts and on the help available from the Authority.

Section 19

Rights defined for the data subject under Sections 14–18 may be restricted by law for reasons pertaining to domestic and external national security, and therefore, to national defence, to ensure national security, prevent or prosecute offences, ensure the security of penal institutions, as well as the economic and financial interests of the state or local governments; to disciplinary and ethical offenses, prevent and expose labour law related and occupational safety infringements – including control and supervision in every case – in addition to protecting the rights of the data subject or others.

14. The Requirement to Preliminarily Inform the Data subject

Section 20

(1) Prior to control being initiated the data subject must be informed of whether the control is to be conducted on the grounds of consent or is mandatory.

(2) Prior to control being initiated the data subject must be explicitly informed in detail of every fact relating to the control of their data, and therefore in particular, of the objective of the control and its legal grounds, the individual authorised to control and process the data, the duration of the control process, should the controller be controlling the personal data of the data subject in accordance with Section 6 (5), as well as of who is authorised to acquire knowledge of this data. This information must equally detail the rights and legal redress opportunities the data subject has in connection with control.

(3) In the case of mandatory control, information may also be provided by publically referring to legislative provisions specifying information set out in subsection (2).

(4) Should it not possible to personally inform the data subject or the cost of this proves excessively high, information may also be provided by disclosing the following information:

a. the event of the data collection,
b. scope concerned,
c. purpose of the data collection,
d. duration of the control,
e. possible controllers authorised to acquire knowledge of the data,
f. providing information on the rights and legal redress opportunities in connection with the control of the data pertaining to the data subjects, and
g. control registration number, except in the case specified in Section 68 (2), should the control be subject to data protection registration.

15. Objection to the Control of Personal Data

Section 21

(1) The data subject is entitled to object to the control of their personal data

a. should the personal data have to be controlled or transferred to fulfil the legal obligations of the controller, or validate the rightful interests of the controller, data recipient or third party except in the case of mandatory data control;
b. should the personal data be used or transferred directly for business benefits, public opinion surveys or scientific research purposes, or
c. other cases defined in relevant legislation.

(2) The controller shall assess the objection lodged within the shortest possible space of time following the submission of the request; however, he or she shall assess the document within a maximum period of 15 days and make a decision on the grounds of the objection and notify the applicant of the decision in writing.

(3) The controller shall suspend the control process – including data entry and data transfer – block the data and notify everyone to whom the personal data constituting the object of objection was transferred of the objection lodged, as well as measures taken on the grounds of this, which individuals are obliged to take measures to enforce the right to object, should the controller deem that the objection lodged is legitimate and justifiable.

(4) The data subject is entitled to initiate legal proceedings – in accordance with the mode specified in Section 22 - within a period of 30 days following the announcement of the decision or the final day of the deadline period, should the data subject disagree with the decision made by the controller on the grounds of subsection (2), or should the controller fail to observe the deadline set in subsection (2).

(5) The data subject is entitled to initiate legal proceedings – in accordance with the mode specified in Section 22 - within a period of 15 days following the announcement of the decision pursuant to subsection (2), should the data required to assert the rights of the data recipient not have been received because of the objection lodged by the data subject. The controller is authorised to summon the data subject to court.

(6) The data recipient is entitled to request information on the circumstances causing data transfer problems from the controller, should the controller fail to send the notification specified in subsection (3), which information the controller is obliged to provide for the data recipient within a period of eight days following the sending of the request submitted in this matter. Should information be requested, the data recipient is entitled to turn to the courts and initiate proceedings against the controller after the information is provided, however, no later than within 15 days following the deadline date specified in this regard. The controller is authorised to summon the data subject to court.

(7) The controller is not authorised to delete the data of the data subject if the control of the data was ordered by law. However, the data of the subject data cannot be transferred to the data recipient if the controller agreed with the objection made, or the court deems that the objection is legally justified.

16. Assertion of Rights in Court

Section 22

(1) The controller is entitled to initiate legal proceedings against the data recipient should the rights of the data subject be infringed, as well as in cases listed under Section 21. The courts shall take immediate action in such cases.

(2) The controller shall be obliged to prove that the data has been controlled in compliance with the relevant legislation. The data recipient shall be obliged to prove the legitimacy of the data transfer in respect of the data transferred to this party in cases listed in Section 21 (5) and (6).

(3) The litigation shall be assessed within the scope of the jurisdiction of the County Court, or Municipal Court in Budapest (hereinafter jointly referred to as county court). The legal procedure may be launched at the county court competent in the place of residence of the data subject, according to their choice of court.

(4) Persons normally not having the capacity to be a party to legal proceedings may also be parties to the litigation The Authority is entitled to intervene in the proceeding in favor of the data subject.

(5) The controller shall be obliged to provide information, correct, block and delete the data, reverse the decision made with the help of automated data processing should the court entertain the motion, by taking account of issuing the data requested by the data recipient defined under Section 21.

(6) The controller shall be obliged to delete the personal data of the data subject within three days following the announcement of the verdict should the court reject the motion submitted in cases defined under Section 21. The controller shall also be obliged to delete the data should the data recipient fail to turn to the courts within the deadline period set in Section 21 (5) and (6).

(7) The court orders the public disclosure of the verdict – by disclosing the controller's ID data – should this be requested in the interest of data protection and the rights of a higher number of data subjects protected within the scope of the present Act.

17. Compensation

Section 23

(1) The controller shall be obliged to compensate for damages caused to others as an outcome of the illegitimate control of the data of the data subject or a breach of data security requirements. The controller shall be exempt from liability should they be able to prove that the damages were caused by circumstances beyond their immediate control.

(2) Damages do not need to be compensated should they have ensued from the deliberate or serious negligence of the aggrieved party.

18. Internal Data Protection Officer and Data Protection Rules

Section 24

(1) An internal data protection officer – with a higher education degree in law, economics, IT or equivalent - under the immediate supervision of the head of the organisation must be appointed or designated within the organisation of the controller or data processor

a. at the controller and processor controlling or processing national official, labour or criminal files;
b. at the financial organisation;
c. at the electronic telecommunications and public service corporation.

(2) The internal data protection officer shall

a. cooperate and assist in making decisions in connection with data control and in guaranteeing the rights of the data subjects;
b. control compliance with provisions governing the present Act and other legislation relevant to data control, as well as rules defined in the internal data protection and data security regulation and data security requirements;
c. assess the reports received and draw the attention of the controller or data processor to terminating the procedure should unauthorised control be exposed;
d. compiles the internal data protection and data security regulation;
e. manages the internal data protection file;
f. organises data protection training.

(3) Controllers defined in subsection (1), as well as other state and local government controllers – with the exception of controllers not obliged to submit reports in the data protection file - are

required to compile an internal data protection and data security regulation to execute the present Act.

19. Conference of Internal Data Protection Officers

Section 25

(1) The purpose of the conference for internal data protection officers (hereinafter conference) is to establish regular professional contacts between the Authority and internal data protection officers with the aim of developing standard legal practices in regard to the application of legislation relevant to the protection of personal data and accessing data of public interest.

(2) The president of the Authority convenes the conference as required; although, at least once a year, and defines its agenda.

(3) The internal data protection officers of every organisation appointed by law, as a mandatory requirement, are members of this conference.

(4) The internal data protection officers who do not have to be appointed by law may also be members of this conference, in which regard these officers are entitled to register in the internal data protection officer database managed by the Authority.

(5) The Authority manages an internal data protection officer database of conference members for networking purposes. The name of the internal data protection officer, postal and email address, as well as the organisation they represent is registered in this database.

(6) The Authority maintains the data defined in subsection (5) in the databases until the mandate of the data protection officer expires or the Authority becomes aware of this.

CHAPTER 3

ACCESSING DATA OF PUBLIC INTEREST

20. General Rules Concerning Accessing Data of Public Interest

Section 26

(1) Bodies or individuals undertaking state or local government duties, as well as other duties defined in the relevant legislation (hereinafter jointly referred to as body undertaking public duties) must be ensured the opportunity to provide access to data of public interest and data public on grounds of public interest to anyone requesting such data under their control, with the exception of cases defined within the scope of the present 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 of public interest.

(3) Should it not otherwise be regulated by law, data of public interest implies data under the control of bodies or individuals providing services which must, as a mandatory requirement, be used on the grounds of the relevant legislation or the contract concluded with the state or the local government, cannot be provided through other means, is relevant to their activities and which do not qualify as personal data.

Section 27

(1) Access to data of public interest and data public on grounds of public interest cannot be ensured should this data qualify as classified information on the grounds of the act on the protection of classified information.

(2) Right to access data of public interest and data public on grounds of public interest may – by specifying the type of data – be restricted by law

a. in the interest of national defence;
b. in the interest of national security;
c. to prosecute or prevent offences;
d. in the interest of environmental protection or nature preservation;
e. in the interest of central financial and exchange rate policy;
f. in regard to foreign relations and relations with international organisations;
g. in regard to legal or administrative proceedings;
h. in regard to intellectual property rights.

(3) The relevant provisions set out in the Civil Code regulate access to business secrets.

(4) Access to data of public interest may be restricted on the grounds of EU contractual clauses in regard to major financial or economic policy interests of the European Union, equally including interests pertaining to monetary, budgetary and tax policies.

(5) Data generated or registered during the course of a procedure aimed at the body undertaking public duties making a decision within its respective scope of responsibilities and authority and serving as a basis for making this decision cannot be disclosed for a period of 10 years following the date this data was generated or registered. The competent executive of the body controlling this data is entitled to authorise access to this data by considering the gravity of the given public interest relating to ensuring or denying access to this data.

(6) Requests for access to data serving as a basis for decision-making may be rejected – within the period defined in subsection (5) – should accessing this data potentially interfere with the legal operational procedure of the body undertaking public duties or the delivery of its scope of responsibilities and authority devoid of unauthorised outside influence, and therefore, in particular, free expression of the position of the body which generated the data during decision preparation.

(7) Legislation regulating restrictions to accessing certain data serving as a basis for decision-making may specify a shorter period than specified in subsection (5).

(8) Provisions set out in the present chapter cannot be applied to the provision of data from registers regulated under separate legislation.

21. Demand for Accessing Data of Public Interest

Section 28

(1) Requests for accessing data of public interest may be made verbally, submitted in writing or electronically by anyone. Provisions governing accessing data of public interest must be applied to access public data of public interest.

(2) Should it not be otherwise regulated by law, the personal data of the applicant submitting the request may only be controlled should this be necessary for processing the request and paying the fee charged for making copies. The personal data of the applicant must be immediately deleted after the request is processed and the fee is paid.

(3) should the data request be incomplete or unclear, the controller requests further specification from the applicant.

Section 29

(1) The body undertaking public duties controlling the data shall satisfy the requirements relating to accessing data of public interest within the shortest possible space of time, but within a maximum period of 15 days.

(2) The deadline set in subsection (1) may be extended once by 15 days should the request for data concern an extensive and large volume of data. The applicant must be notified of this within a period of eight days following the receipt of the request.

(3) The applicant is entitled to receive a copy of the documents or document section containing the

data regardless of its mode of storage. The body undertaking public duties controlling the data is entitled to charge a fee for making the copies – which fee shall be aligned to costs arising in connection with copying – of which the applicant must be notified before the request is processed.

(4) Should the document or document section of which a copy has been requested be large, copying requests shall be fulfilled within a period of 15 days after the payment of the fee charged. The applicant must be notified of the large size of the document or document section of which a copy was requested, the fee charged, as well as options in which case copying is not needed to satisfy data requirements within a period of eight days following the receipt of the request.

(5) The relevant legislation regulates cost items and the highest value of these taken into account when setting fee rates, as well as criteria to be applied to determine the large volume of the document of which a copy was requested.

Section 30

(1) Should the document containing data of public interest also contain data that cannot be disclosed to the individual requesting the document, such data which cannot be disclosed must be made unrecognisable in the copy.

(2) Data requests must be satisfied in a clear manner and in a mode and through the use of the technical instrument specified by the applicant, should the body controlling the data of public interest be easily able to do this. If the data requested was electronically disclosed at an earlier date, the request can be also satisfied by indicating the public source containing the given data. Requests for data cannot be rejected by claiming that they cannot be properly satisfied.

(3) The applicant must be notified of the rejection, the reasons for the rejection, as well as information on legal redress options the individual is entitled to pursuant to the present Act in writing, or electronically should the request have been submitted via email, within a period of eight days. The controller shall register requests rejected and reasons for their rejection and shall inform the Authority of the contents of this file each year prior to 31 January.

(4) Requests for access to data of public interest cannot be rejected because the non-native Hungarian speaking individual requesting the data submitted the request in their native language or other language they may speak.

(5) Should the relevant legislation facilitate the opportunity for the controller to consider rejecting the fulfilment of the request to access data of public interest, a narrow interpretation must be applied to such a rejection and the fulfilment of the request aimed at accessing data of public interest may be rejected should the gravity of the public interest serving as a basis for rejection supersede the public interest relating to the fulfilment of the request to access data of public interest.

(6) The body undertaking public duties shall compile regulations setting out the rules of procedure for fulfilling requests aimed at accessing data of public interest.

Section 31

(1) The applicant is entitled to turn to the courts should the deadline period open for the rejection or fulfilment of the request for access to data of public interest, or the deadline extended by the controller in accordance with Section 29 (2) expire and become inconclusive, and in addition is entitled to review the fee charged for making a copy, should this fee not yet have been paid.

(2) The controller is required to prove the legal grounds of rejection and its underlying reasons and the substantiation of the sum of the fee charged for making a copy.

(3) Litigation must be launched against the body undertaking public duties within a period of 30 days following the announcement of the rejection of the request, the expiry of the deadline which was inconclusive and the expiry of the deadline set for paying the fee charged. Should it be in the interests of the applicant to request an investigation of the Authority due to the rejection of the

request, its non-fulfilment or the fee charged for making a copy and the applicant declares this to the Authority, litigation concerning the refusal to effectively assess this submission, termination of the assessment procedure may be launched within a period of 30 days following the receipt of the notification on termination specified in Section 55 (1)(b) or notification specified in Section 58 (3). Justification must be provided should the deadline period available for launching litigation expire.

(4) Persons normally not having the capacity to be a party to legal proceedings may also be parties to the litigation. The Authority is entitled to intervene in the proceedings in favour of the applicant.

(5) Litigation launched against bodies undertaking public duties with a national scope of competence fall under the scope of jurisdiction of county courts. Matters within the scope of jurisdiction of the local court shall be processed at the local court at the seat of the county court, in Budapest or in the Pest Central District Court. The seat of the body undertaking the public duties of the defendant shall nominate the competent court.

(6) The court shall take immediate action.

(7) Should the court accept the submission to request data of public interest, the court shall oblige the controller to disclose the data of public interest requested in the court decision. The court is entitled to modify the sum of the fee charged for making a copy, or order the body undertaking public duties to launch a new procedure to determine the sum of the fee charged.

CHAPTER 4

DISCLOSING DATA OF PUBLIC INTEREST

22. Information Obligation Concerning Data of Public Interest

Section 32

In regard to matters within their scope of responsibilities – therefore, with special regard to the state and local budget and the implementation of these, managing state or local government assets, use of public finances and contracts concluded in this regard, in respect of ensuring special or exclusive rights for market players, private organisations and individuals - the body undertaking public duties is obliged to facilitate and ensure that the public receives accurate and expedient information.

23. Electronic Disclosure Obligation

Section 33

(1) Access to data defined as data of public interest pursuant to the present Act must be ensured free of charge in digital format on internet websites for anyone interested, without disclosing any personal ID data or applying restrictions, in printable format ensuring the opportunity to copy parts of the text without data loss or distortion, enabling the document to be viewed, copies to be downloaded and printed, as well as network data transfer (hereinafter electronic disclosure). Access to the data disclosed cannot be subject to the disclosure of personal data.

(2) Should it not otherwise be regulated by law, the following organisations shall publish the data defined in disclosure lists specified under Section 37 on their respective websites:

a. Office of the President of the Republic of Hungary, Office of the National Assembly, Office of the Constitutional Court, Office of the Commissioner for Basic Rights, State Audit Office of Hungary, Hungarian Academy of Sciences, Hungarian Academy of Arts, National Council of Justice of Hungary, Office of the Prosecutor General;
b. state public administration body with the exception of the Government Committee, as well as the national chamber and
c. regional public administration body of the Government with general scope of authority.

(3) Bodies undertaking public duties not listed in subsection (2) may also fulfil electronic disclosure obligations set out in Section 37 by disclosing data on a central website either operated alone or in conjunction with associated bodies – as they so choose – maintained by bodies undertaking their

supervision, professional management or coordination in connection with their operation and set up for this specific purpose.

(4) Should the public education institution not undertake national or regional responsibilities, electronic disclosure obligations set put in the present Act are fulfilled by supplying data to information systems defined under sectoral legislation.

Section 34

(1) The data officer not publishing the data on their own website - by applying Section 35 – transfers the data to be disclosed to the body providing the data, which individual shall ensure that the data is published on their website, and in addition ensure that the body supplying the specific data of public interest published is explicitly recognisable and which body the given data concerns.

(2) The body publishing the data shall design the website used to publish the data in such a way that the data is suitable for publication; ensures its ongoing operation, repairs potential malfunctions and updates the data.

(3) Information on the detailed rules concerning an individual's request for public data must be clearly provided on the website used to publish the data. This information must equally include information on options for legal redress.

(4) Beyond data of public interest defined in the disclosure lists, other data of public interest and data public on grounds of public interest may also be disclosed on the publication website.

Section 35

(1) The body responsible for the data and obliged to electronically disclose this data shall ensure the accurate, updated and ongoing publication of the data specified in disclosure lists defined under Section 37 and that this data is transferred to the body supplying the data.

(2) The body supplying the data is responsible for their electronic disclosure, and for ensuring continuous access, authenticity and updating of the data.

(3) To fulfil the obligations set out in subsection (1), the data officer shall set out detailed rules in an internal regulation, whilst the body supplying the data shall act likewise to fulfil obligations set out in subsection (2).

(4) Unless otherwise regulated within the scope of the present Act or other legislation, electronically published data cannot be removed from the website. Should the body cease to exist, their legal successor shall be responsible for meeting disclosure obligations.

Section 36

Disclosure of data detailed in the disclosure lists defined under Section 37 does not affect obligations of the given body in connection with the publication of data of public interest or data public on grounds of public interest or other obligations set out under the relevant legislation.

24. Disclosure Lists

Section 37

(1) Bodies defined in Section 33 (2)-(4) (hereinafter jointly referred to as bodies obliged to disclose data) shall publish data detailed in the general disclosure list compiled in Annex 1 in accordance with the requirements specified in Annex 1, with the exception of cases defined in subsection (4).

(2) Other data which must be disclosed (hereinafter special disclosure list) may be specified in connection with specific sectors and types of bodies undertaking public duties by legislation.

(3) The head of the body obliged to disclose data – after requesting the opinion of the Authority – as well as legal regulations may define additional scopes of data which must be disclosed as a mandatory requirement applicable to bodies undertaking public duties, the management of these,

bodies under their supervision or some of these (hereinafter individual disclosure list).

(4) The Minister in charge of the direction of civil national security services and the Minister competent for the direction of civil intelligence activities define the scope of data to be disclosed by civil national security agencies, whilst the Minister for Defence defines the scope of data to be disclosed by national defence agencies - after requesting the opinion of the Authority – within the scope of a decree.

(5) Compiling and modifying the individual disclosure list – having requested the opinion of the Authority - is designated to the scope of authority of the body in the case of bodies obliged to disclose information operating as corporate bodies.

(6) The head of the organisation obliged to disclose information annually reviews the disclosure list they issued in accordance with subsection (3) on the basis the data of data requests made in connection with data of public interest not included in the disclosure list and adds items to this list based on the high rate or volume of data requests made.

(7) Depending on the type of data to be disclosed, it is also possible to determine the frequency of disclosure in these disclosure lists.

(8) The Authority is also entitled to make recommendations for compiling and contributing to special and individual disclosure lists.

CHAPTER 5

NATIONAL AUTHORITY FOR DATA PROTECTION AND FREEDOM OF INFORMATION

25. Legal Status of the Authority

Section 38

(1) The Authority shall be an autonomous state administration organ.

(2) The task of the Authority shall be to supervise and promote the enforcement of the right to the protection of personal data, and of the right to access to data of public interest or to data public on grounds of public interest.

(3) In the performance of its tasks pursuant to subsection (2) and to the provisions laid down in this Act, the Authority

a) shall conduct investigations on the basis of reports;

b) may conduct ex officio data protection procedures;

c) may conduct ex officio procedures for the supervision of classified data;

d) may institute legal proceedings for infringements relating to access to data of public interest or to data public on grounds of public interest;

e) may intervene in legal proceedings initiated by others;

f) shall keep a data protection register.

(4) In the performance of its tasks pursuant to subsection (2), the Authority

a) may put forward proposals for the making or amendment of rules of law affecting the processing of personal data or affecting access to data of public interest or to data public on grounds of public interest, and shall give an opinion on the draft rules of law affecting its tasks;

b) shall publish an annual report on its activities by 31 March of the calendar year and submit the report to Parliament;

c) shall issue general recommendations and recommendations for specific controllers;

d) shall provide recommendations relating to special and/or individual publication lists to be published pursuant to this Act in connection with the activities of organs performing public tasks;

e) shall represent Hungary, in cooperation with the organs or persons specified in an Act, in the joint data protection supervisory bodies of the European Union;

f) shall organise the conferences of internal data protection officers;

g) shall define the professional criteria for data protection auditing;

h) may conduct data protection audits at the request of controllers.

(5) The Authority shall be independent, subordinated only to Acts; it may not be given instructions as to the performance of its tasks, and shall perform its tasks separately from other organs, free of any outside influence. Tasks for the Authority may only be established by an Act.

26. Budget and 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 Authority shall be headed by a President. The President of the Authority shall be appointed by the President of the Republic at the proposal of the Prime Minister from among those Hungarian nationals who have a law degree, the right to stand as a candidate in elections of Members of Parliament, and at least ten years of professional experience in supervising proceedings related to data protection or freedom of information or a Ph.D. degree in either of these fields.

(2) No one may be appointed President of the Authority who – in the four years preceding the proposal for his or her appointment – had been a Member of Parliament, Member of the European Parliament, President of the Republic, Member of the Government, state secretary, member of a local government body, mayor, deputy mayor, Lord Mayor, Deputy Lord Mayor, president or vice president of a county representative body, or member of a local, regional or national nationality self-government, or officer or employee of a political party.

(3) The President of the Republic shall appoint the President of the Authority for nine years.

(4) After his or her appointment the President of the Authority shall take an oath before the President of the Republic; the content of the oath shall be governed by the Act on the oath and pledge of certain officers of public law.

Section 41

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

(2) The President of the Authority may not pursue any other gainful occupation, nor accept

remuneration for his or her other activities, with the exception of academic, educational or artistic activities, activities falling under copyright protection, proof-reading or editing activities.

(3) The President of the Authority may not be executive officer of a business organisation, member of its supervisory board or such member of a business organisation that has an obligation of personal involvement.

Section 42

(1) The President of the Authority shall make a declaration of assets, identical in contents to those of Members of Parliament, within thirty days of his or her appointment, then by 31 January of each year, and within thirty days of the termination of his or her mandate.

(2) Should the President of the Authority fail to make a declaration of assets, he or she may not perform the tasks deriving from his or her office, and may not receive remuneration until he or she submits the declaration of assets.

(3) The declaration of assets shall be public and an authentic copy thereof shall be published without delay on the website of the Authority. The declaration of assets may not be removed from the website of the Authority for one year following the termination of the mandate of the President of the Authority.

(4) Anyone may initiate proceedings related to the declaration of assets of the President of the Authority by the Prime Minister with a statement of facts specifically indicating the contested part and content of the declaration of assets. The Prime Minister shall reject the initiative without conducting proceedings if it does not meet the requirements contained in this subsection, if it is manifestly unfounded or if a repeatedly submitted initiative does not contain new facts or data. The veracity of those contained in the declaration of assets shall be checked by the Prime Minister.

(5) In the course of declaration of assets proceedings, at the invitation of the Prime Minister the President of the Authority shall notify the Prime Minister without delay and in writing of the supporting data on the property, income and interest relations indicated in his or her declaration of assets. The Prime Minister shall inform the President of the Republic of the outcome of the check by transmitting the given data. The data may be accessed only by the Prime Minister and the President of the Republic.

(6) The supporting data submitted by the President of the Authority shall be deleted on the thirtieth day following the termination of the declaration of assets proceedings.

Section 43

(1) The President of the Authority shall be entitled to a salary and allowances identical to those of a Minister; the salary supplement for management duties, however, shall be one and a half times that of a Minister.

(2) The President of the Authority shall be entitled to forty working days of leave per calendar year.

Section 44

(1) From the point of view of entitlement to social security provisions, the President of the Authority shall be considered an insured person employed in a public service legal relationship.

(2) The time period of the mandate of the President shall be considered as time served in a public service legal relationship with an organ of public administration.

Section 45

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

a) upon expiry of the term of his or her mandate;

b) upon his or her resignation;

c) upon his or her death;

d) upon establishment of the absence of the conditions necessary for his or her appointment or upon violation of the rules regarding the declaration of assets.

e) upon establishment of a conflict of interest.

(2) The President of the Authority may at any time resign from his or her mandate in a written declaration addressed to the President of the Republic through the Prime Minister. The mandate of the President of the Authority shall terminate on the date indicated in the resignation, which date shall be posterior to the communication of the resignation or, in the absence thereof, on the day of communication of the resignation. No statement of acceptance shall be necessary for the validity of the resignation.

(3) If the President of the Authority fails to terminate a conflict of interest within thirty days of his or her appointment or if, in the course of the exercise of his or her office, a conflict of interest arises, the President of the Republic shall, at the written motion of the Prime Minister, decide on the question of the establishment of a conflict of interest.

(4)

(5)

(6) The absence of conditions necessary for the appointment of the President of the Authority shall be established by the President of the Republic upon the motion of the Prime Minister. The President of the Republic, upon the motion of the Prime Minister, shall establish that a violation of the rules regarding the declaration of assets has occurred should the President of the Authority deliberately make a false declaration regarding important data or facts in his or her declaration of assets.

(6a) The Prime Minister shall notify The President of the Republic and the President of the Authority simultaneously regarding his or her motions based on Subsections (3) and (6).

(6b) The President of the Authority, upon receiving the motion, may appeal to the court within 30 days on the basis that the motion has not been established. If the deadline has been missed, no justification shall be accepted. The President of the Authority must instigate the proceedings against the Prime Minister. Regulations of the Actions Relating to Contracts of Employment and Other Similar Legal Relationships of the Act III of 1952 on the Code of Civil Procedure shall apply in regard to the jurisdiction of the court, with the exceptions that the Fővárosi Munkaügyi Bíróság (Budapest Labor Court) shall have exclusive jurisdiction, the court shall hear such cases in priority proceedings, and that the statement of the claim and the final judgment on the merits of the case must be communicated to the President of the Republic.

(6c) If the final judgment on the merits of the case, based on the Action of The President of the Authority, set forth in Subsection (6b), finds that the motion of the Prime Minister based on Subsections (3) and (6), has not been established, The President of the Republic shall not terminate the mandate of the President of the Authority.

(6d) The President of the Republic, on the motion of the Prime Minister based on subsections (3) and (6), shall make his or her decision

a) within 15 days if the President of the Authority missed the deadline set forth in subsection (6b)

b) within 15 days of receipt of the final judgment on the merits of the case if the President of the Authority meets the deadline set forth in subsection (6b)

(7) In the event of termination of the mandate pursuant to subsection (1)(a) or (b), the President of the Authority shall be entitled to an additional payment three times the amount of his or her monthly salary at the time of termination.

(8) Decisions assigned to the competence of the President of the Republic by subsections (3) and (6)

or by Section 40 need not be countersigned.

Section 45/A

The President of the Authority may participate and address the session of the Parliamentary Committees.

28. Deputy of the President of the Authority

Section 46

(1) The President of the Authority shall be assisted in his or her work by a Deputy appointed by himself or herself for an indefinite period of time. The President shall exercise the employer's rights over the Vice President of the Authority.

The Vice President shall meet the requirements necessary for the appointment of the President of the Authority as laid down in Section 40 (1) and (2) with the exception that Vice President shall have at least five years of professional experience in supervising proceedings related to data protection or freedom of information.

(3) In regard to conflicts of interest regarding the Vice President the provisions laid down in Section 41 shall apply as appropriate.

(4) The Vice President shall exercise the powers and perform the tasks of the President if the President is prevented from acting or the office of President is vacant.

Section 47

The provisions of Section 42 shall apply, as appropriate, to the obligation of the Vice President to make a declaration of assets and to the proceedings related to his or her declaration of assets with the proviso that in the course of the declaration of assets proceedings, the President of the Authority shall proceed instead of the Prime Minister, and the President of the Republic does not need to be informed of the outcome of the check.

Section 48

(1) The Vice President shall be entitled to a salary and allowances identical to those of a state secretary.

(2) The Vice President shall be entitled to forty working days of leave per calendar year.

(3) From the point of view of entitlement to social security provisions, the Vice President shall be considered an insured person employed in a public service legal relationship.

(4) The time period of the mandate of the Vice President shall be considered as time served in a public service legal relationship with an organ of public administration.

49. § (1) The mandate of the Vice President of the Authority shall terminate

a) upon his or her resignation;

b) upon his or her death;

c) upon establishment of the absence of conditions necessary for his or her appointment;

d) upon establishment of a conflict of interest;

e) upon his or her dismissal; or

f) upon removal from office.

(2) The Vice President of the Authority may at any time resign from his or her mandate in a written declaration addressed to the President of the Authority. The mandate of the Vice President of the Authority shall terminate on the date indicated in the resignation, which date shall be posterior to the communication of the resignation or, in the absence thereof, on the day of communication of the

resignation. No statement of acceptance shall be necessary for the validity of the resignation.

(3) If the Vice President of the Authority fails to terminate a conflict of interest pursuant to Section 41 within thirty days of his or her appointment or if, in the course of the exercise of his or her office, a conflict of interest arises, the President of the Authority shall decide on the establishment of a conflict of interest.

(4) The President of the Authority shall dismiss the Vice President of the Authority if, for reasons not imputable to him or her, the Vice President of the Authority is not able to perform the duties deriving from his or her mandate for more than ninety days.

(5) The President of the Authority may dismiss the Vice President of the Authority; at the same time the Vice President of the Authority shall be offered a position as a public servant at the Authority, and – even in the absence of the conditions laid down in subsection (1) of Section 51 – the position of an inquirer.

(6) The President of the Authority shall remove the Vice President of the Authority from office if, for reasons imputable to him or her, the Vice President of the Authority fails to perform the duties deriving from his or her mandate for more than ninety days or if he or she deliberately makes a false declaration on important data or facts in his or her declaration of assets.

(7) The absence of conditions necessary for the appointment of the Vice President of the Authority shall be established by the President of the Authority.

(8) In the event of termination of the mandate pursuant to subsection (1)(a) or (f), the Vice President of the Authority shall be entitled to an additional payment three times the amount of his or her monthly salary at the time of termination.

29. Staff of the Authority

Section 50

The employer's rights over the public servants and employees of the Authority shall be exercised by the President of the Authority.

Section 51

(1) The President of the Authority may appoint inquirers, up to twenty per cent of the number of public servants of the Authority, from among those public servants of the Authority who have a higher education degree in informatics or law and have held for at least three years the post of data protection expert or data protection officer, and who have passed a Hungarian professional examination in public administration or a Hungarian professional examination in law.

(2) The mandate of an inquirer shall be given for an indefinite period of time, and it shall be revocable by the President of the Authority at any time without justification. If the President of the Authority revokes the mandate of an inquirer, the public servant in question shall be reinstated in the position he or she last held before being given the mandate of an inquirer.

(3) Inquirers shall be entitled to the salary of a head of unit without managerial allowance.

CHAPTER 6

PROCEDURES OF THE AUTHORITY

30. Investigation of the Authority

Section 52

(1) Anyone is entitled to request an investigation from the Authority, on the grounds of infringement of law, in connection with the control of personal data, as well as exercising rights relating to access to data of public interest or data public on grounds of public interest, or in the event of such immediate threat to the above.

(2) The investigation launched by the Authority does not qualify as administrative proceedings, which is why it is not necessary to apply the provisions governing the act on the general rules of administrative proceedings.

(3) No one may be placed at a disadvantage because of the report made to the Authority. The Authority is only allowed to disclose the identity of the person making a report to the Authority if it is otherwise not possible to conduct the investigation. Upon request of the person making a report to the Authority, the Authority is not allowed to disclose the identity of this person even if it is otherwise not possible to conduct the investigation. Of this consequence the Authority shall notify the person

(4) The Authority shall conduct the investigation free of charge; the Authority shall advance and bear the costs of the procedure.

Section 53

(1) With the exception of the cases specified above in subsection (2) and (3), the Authority is obliged to effectively assess the report made.

(2) The Authority is entitled to reject the submission without investigating it, in the event that

a. the legal abuse claimed is minor, or
b. it was reported anonymously.

(3) The Authority is entitled to reject the submission without investigating it, should

a. legal proceedings be in progress in connection with the given issue, or a legally binding decision was made earlier in connection with the issue;
b. the person reporting the case have requested that their anonymity be maintained in accordance with subsection of Section 52 (3);
c. the claim be unfounded;
d. the report submitted repeatedly not contain any new facts or data.

(4) Should the report have been made by the Commissioner for Fundamental Rights, the Authority is only allowed to refuse to make an investigation, should legal proceedings be in progress in connection with the given issue, or if a legally binding decision was made earlier in connection with the issue.

(5) The Authority shall terminate the investigation in the event of

a. the submission should have been rejected without investigation on the grounds of the subsections (3) and (4); however, the Authority only acquired information on the reasons for rejection after the investigation was launched;
b. the circumstances giving rise to the investigation no longer prevail.

(6) The Authority shall notify the person reporting to the Authority of the dismissal of the claim made without conducting an investigation, termination of the procedure and justification for the dismissal or termination.

(7) The Authority shall refer the report submitted in connection with issues not within the Authority's respective scope of authority – by concurrently notifying the person submitting the report – to the body authorised to act in respect of the claims made, should it, on the basis of the data available to it, be possible to identify the competent body. Should, on the basis of the report submitted in connection with issues outside the scope of authority of the Authority, the Authority deem that legal proceedings may be initiated in connection with the issue, the Authority shall notify the reporting individual.

Section 54

(1) During the investigation, the Authority is entitled to

a. inspect all documents controlled by the controller under review and associated with the given case, or request copies of these;
b. acquire knowledge of data control activities associated with the case under review and enter the premises where control activities are undertaken;
c. request verbal or written information from the controller under review, as well as from any employee of the controller,
d. request information in writing from any organisation or individual associated with the case under review, and
e. request that the head of the supervisory body of the data control authority carry out an investigation.

(2) Pursuant to the request made by the Authority in accordance with subsection (1), the controller under review, or other concerned organisation or individual shall be obliged to fulfil requests made by the Authority within the deadline period set by the Authority. The deadline period defined by the Authority may not be less than 15 days in cases defined in subsections (1) (d) and (e).

(3) The individual competent for providing information may refuse to provide information specified under subsections (1) (c) and (d), should

a. the individual constituting the object of the investigation of the Authority concerned by the report submitted be an immediate relative or former spouse, in accordance with the act on the general rules of administrative proceedings;
b. the given individual or their immediate relative or former spouse as specified within the scope of the act on the general rules of administrative proceedings have been charged with committing a crime in connection with the given case during the course of the provision of information.

Section 55

(1) Within two days of the receipt of the submission, the Authority shall undertake the following:

a. should the Authority deem the submission to be well-founded, the Authority shall
a. take measures defined under Section 56 and Section 57;
b. close the investigation and launch a data protection procedure in accordance with Section 60, or
c. close the investigation and launch a procedure for the supervision of classified data in accordance with Section 62;
b. close the investigation should it deem that the content of the submission is unfounded.

(2) The Authority shall notify the individual making the report of the results of the investigation, and of the reasons for closing the investigation and launching administrative proceedings.

Section 56

(1) Should the Authority deem that the exercising of rights in connection with the control of the personal data, or relating to access to data of public interest or data made public on the grounds that the public interest was abused, or in the event of immediate threat to the above, the Authority shall instruct the controller to address this and terminate any immediate relating threat.

(2) The controller – in the event of a consensus – shall immediately initiate the necessary measures in the notification specified above in subsection (1) and shall notify the Authority on measures taken, or – in the event of disagreement – send their position to the Authority within 30 days of the receipt of the given notification.

(3) In the case of data control authorities with supervisory bodies, the Authority shall make recommendations to the supervisory body of the data control organisation, concurrently to notifying the data control body, should the notification issued in accordance with subsection (1) have proved ineffective. Should the supervisory body of the data control organisation have not been notified in accordance with subsection (1), the Authority may also directly make recommendations, if, in their

view, these recommendations would effectively address the legal anomaly or terminate the immediate threat of legal infringement.

(4) The supervisory body shall notify the Authority of the position they established in respect of the recommendation, as well as measures initiated within a period of 30 days following the receipt of the recommendation.

Section 57

Should, pursuant to the investigation, the Authority deem that the legal anomaly or its immediate threat ensues from any kind of unnecessary, ambiguous or inappropriate provision governing legislation or regulatory instrument of public law, or the lack of or deficient nature of the legal regulation of issues associated with data control, the Authority may make recommendations to elaborate legislation or to the body authorised to issue the regulatory instrument of public law, as well as individuals responsible for drafting legislation to prevent the future occurrence of this anomaly and its immediate threat. The Authority may recommend the amendment, repeal or drafting of legislation or the regulatory instrument of public law in this recommendation. The body contacted may notify the Authority of their position, as well as measures taken in accordance with recommendations made within a period of 60 days.

Section 58

(1) Should, pursuant to the notification issued in accordance with Section 56 or the recommendation, 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 Section 56 (2), or Section 56 (4) if a recommendation was not issued.

(2) In regard to further measures required in the case of subsection (1), the Authority

a. may launch a data protection procedure in accordance with Section 60;
b. may launch a procedure for the supervision of classified data in accordance with Section 62;
c. may launch legal proceedings in accordance with Section 64, or
d. may compile a report in accordance with Section 59.

(3) The Authority shall notify the individual making the report of the outcomes of measures initiated in accordance with Section 56 and Section 57, as well as further measures initiated in accordance with subsection (2).

31. Report Issued by the Authority

Section 59

(1) The Authority shall compile a report on the investigation carried out on the grounds of the claim made, if the Authority did not launch administrative or legal proceedings.

(2) This report shall include facts exposed during the course of the investigation, as well as findings made and conclusions drawn on the basis of these.

(3) The report compiled by the Authority is public. The president of the Authority is entitled to classify reports containing classified information, or repeatedly classify this information as classified. The report containing classified information or confidential information protected by law must be disclosed in such a way that the classified information or other confidential information protected by law cannot be recognised.

(4) Reports compiled for the Authority about investigations carried out in connection with these activities by bodies authorised to use intelligence instruments and methods may not contain data on which grounds it would be possible to deduce the confidential information collection activity of the body carried out in respect of the case.

(5) The report issued by the Authority cannot be contested in court or with any other authorities.

32. Data Protection Procedures of the Authority

Section 60

(1) The Authority is entitled to launch data protection procedures to enforce the right to the protection of personal data.

(2) Unless otherwise provided in this act, the Act on the general rules of administrative proceedings applies for data protection procedures.

(3) Data protection procedures can only be launched ex officio, and shall not qualify as a procedure launched on request even if an investigation based on a report and made by the Authority preceded the data protection procedure. Should, however, an investigation based on a report and made by the Authority have preceded the data protection procedure, the reporting individual must be notified of the launch and the closing of the data protection procedure.

(4) The Authority shall launch a data protection procedure, if, on the basis of the investigation based on a report or otherwise, unlawful control of the personal data is presumed and the unlawful control

a. concerns a wide scope of persons;
b. concerns special data, or
c. significantly harms interests or engenders the risk of damages.

(5) The deadline date for administration within the scope of the data protection procedure is two months.

Section 61

(1) In the decision made within the scope of the data protection procedure, the Authority may

a. order the correction of unauthentic personal data;
b. order the blocking, deletion or destruction of illegally controlled personal data;
c. prohibit the illegal control or processing of the personal data;
d. prohibit the transfer of the personal data to other countries;
e. order notification of the data subject, should the controller have unlawfully refused to, and
f. impose a fine.

(2) The Authority is entitled to instruct the disclosure of their decision – by disclosing the ID data of the controller – should this be required in the interest of data protection or to protect the rights of a greater number of data subjects ensured within the scope of the present Act.

(3) The fine imposed in accordance with subsection (1)(f) may range from 100,000 HUF to 10,000,000 HUF.

(4) To decide whether a fine should be imposed and to determine its amount, the Authority shall consider all circumstances of the case, with special regard to the size of the scope of individuals affected by the legal offense, its weight and repetition.

(5) The disputed data cannot be deleted or destroyed until the deadline for launching the procedure relevant to initiating a review by the court expires, or until the court issues its final verdict in the case of the initiation of review.

33. Procedure for the Supervision of Classified Data

Section 62

(1) The Authority is authorised to launch a procedure for the supervision of classified data, should, pursuant to the investigation conducted based on the report made, it may otherwise be presumed that national classified information has been illegally classified. The procedure for the supervision of classified data of the Authority does not encompass tasks undertaken by the National Security Authority defined within the scope of the act on the protection of classified information.

(2) Unless otherwise provided in this act, the Act on the general rules for administrative proceedings applies for procedures for the supervision of classified data.

(3) Procedure for the supervision of classified data may only be launched ex officio. Should the investigation carried out by the Authority based on a report made have preceded the procedure for the supervision of classified data, it therefore does not qualify as a procedure launched to assess the report made. However, should the investigation carried out by the Authority have been based on a report that preceded the procedure for the supervision of classified data, the reporting individual must be notified of its launch and completion.

Section 63

(1) Should the Authority assess that legislation applicable in connection with the classification of national classified information has been infringed in the decision made within the framework of the procedure for the supervision of classified data, the Authority instructs the classifier to modify the classification level and its period of validity in compliance with relevant legislation, or to terminate classification.

(2) Should the classifier deem that the decision made by the Authority in accordance with subsection (1) is unfounded, the classifier may request that it be reviewed by a court within a period of 60 days of the announcement of the decision. The execution of the decision can be delayed by submitting the statement of claim. Should the classifier not turn to the courts within a 60-day period beginning on the date the decision was announced, the classification of the national classified information becomes null and void in accordance with the decision on the 64th day following the announcement of the decision and its classification level or period of validity changes in accordance with the decision.

(3) Provisions governing the civil court procedure of public administration litigation shall be applied to the legal proceedings, together with the specification that the court shall immediately proceed with the case in a closed session.

(4) The court confirms, amends or reverses the Authority’s decision, or instructs the Authority to launch a new procedure, should it be required.

(5) The decision issued by the court and the Authority does not affect the obligations of the classifier concerning the review of national classified information specified in the act on the protection of classified information.

(6) Only judges that have undergone the highest level national security screening specified in the act on national security services may be appointed.

(7) Besides the judge, the plaintiff and the defendant, any other person may only gain access to the classified information should they have undergone the highest level national security screening specified in the act on national security services.

34. Litigation Options for the Authority

Section 64

(1) Should the controller fail to respond to the warning issued in accordance with Section 56 (1), the Authority may, due to the infringement of law regarding data of public interest and data public on grounds of public interest, request the court to oblige the controller to act in accordance with the warning notification issued within a period of 30 days following the expiry of the deadline period for providing information specified in subsection of Section 56 (2).

(2) Litigation falls under the scope of authority and jurisdiction of the court specified in Section 31 (5).

(3) The controller is obliged to prove that the data control corresponds to provisions governing relevant legislation.

(4) Persons normally not having the capacity to be a party to legal proceedings may also be parties to the litigation.

(5) Should it be requested, the court is entitled to make its verdict public – by disclosing the ID data of the controller – should it be deemed necessary in the interests of data protection and freedom of information, as well as to protect the rights of a greater number of data subjects protected within the scope of the present Act.

35. Data Protection File

Section 65

(1) The Authority registers data control undertaken in respect of personal data in a file (hereinafter data protection file) to facilitate access to information for the data subject, which file – with exceptions defined in subsection (2) - contains the following:

a. the objective of the data control;
b. legal grounds of control;
c. scope of data subjects;
d. description of data concerning the data subjects;
e. source of the data;
f. duration of the control of the data;
g. type of data transferred, its recipients and the legal grounds of transfer, equally including data transfers to third countries;
h. name and address of the controller, as well as the data processor, actual data control, place of data processing and the activity undertaken by the data processor in connection with data control;
i. type of data processing technology applied;
j. name and contact details of the internal data protection officer, in the event of taking part in the process.

(2) The data protection file shall contain the name and address of the national security agency, the objective of the control and its legal grounds in respect of data control undertaken by national security agencies.

(3) The Authority shall not register data controls in the data protection file which

a. relate to the personal data of individuals associated with the controller through employment, organisational membership, enrolment in kindergarten, educational institutions, college membership – with the exception of financial organisations, public utility services, electronic telecommunications service providers - or who are clients of the controller;
b. are carried out in accordance with the internal regulations of the Church, a religious denomination or religious community;
c. relate to personal data regarding the illness or state of health of an individual undergoing healthcare treatment with the aim of receiving medical therapy or health preservation, validating social security claims;
d. relate to personal data registered with the aim of providing financial and social assistance to the data subject;
e. relate to the personal data of individuals involved in administrative, prosecution and legal proceedings and conducting the proceedings, or personal data controlled in connection with the execution of the sentence during the course of the sentence;
f. contain personal data for official statistical purposes on condition that the verification of the link between the data and the data subject is definitively severed in accordance with conditions set out under the relevant legislation;
g. contain the data of media service providers, as specified within the scope of the act on media services and mass telecommunication, which exclusively serve their own information activities;

h. facilitate the objectives of scientific research should the data not be disclosed;
i. were conducted in respect of documents placed in archives.

(4) The data protection file is public, which the Authority shall publish on its website and guarantee free access to.

Section 66

(1) The controller requests that the Authority registers the control of the personal data in a file, with the exception of mandatory data control prior to launching the control process. The control process cannot be launched prior to registration in the file, with the exception of mandatory data control and the case specified in Section 68 (2).

(2) The controller may request the registration of mandatory data control in the file from the Authority within a period of 20 days following the coming into force of the legislation regulating mandating data control.

(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 request for registration in the file must include the data specified in Section 65 (1) and (2).

Section 67

The administration service fee defined in the ministry decree must be paid to register the data control in the data protection file, which does not apply to mandatory data control.

Section 68

(1) With the exception of the case defined in subsection (3), the Authority shall file the data control within a period of eight days following the receipt of the request, should this request contain the data specified in Section 65 (1) and (2).

(2) With the exception of the case defined in subsection (3), should the Authority fail to assess the request for registration prior to the expiry of the deadline set, the controller is authorised to launch data control in accordance with the content of the request submitted.

(3) The Authority shall register data control specified in subsection (4) and (5) within a period of 40 days following the receipt of the request, should the request contain the data specified in Section 65 (1) and (2) and the conditions for legitimate data control are ensured by the controller.

(4) Should the request concern data control registration - defined in subsection (5) – relating to data files in which case data control by the controller registered previously has not been undertaken, or not applied in the case of data control registered previously by the controller, this necessitates the use of new data processing technology and ensuring the conditions for legitimate control by the controller is a precondition for registration.

(5) In accordance with the conditions defined, the precondition for registration defined in subsection (4) relate to

a. controlling national official, occupational and criminal data files;
b. data control concerning financial organisations and public utility service providers;
c. data control concerning clients using the services of electronic telecommunications service providers.

(6) The decision issued by the Authority in respect of the authorisation of registration in the data protection file must contain the data control registration number which the controller must indicate in the case of each individual data transfer, disclosure and data made available to the data subject. This registration number allows the data control to be identified and does not certify the legitimacy of the control activity registered.

(7) In the event of changes to data specified under Section 65 Subsection (1)(b) - (j), the controller

shall submit a change registration request to the Authority within a period of eight days of the occurrence of changes. Rules defined in subsections (1), (3) and (5) must be applied in the case of the change registration procedure on condition that the request must contain the data which changed.

36. Data Protection Audit

Section 69

(1) The data protection audit is a service provided by the Authority designed to provide high standard data protection and data security on control operations carried out or planned through the evaluation of professional standards defined and published by the Authority. Planned control operations may be audited should the concept regarding data control enable this.

(2) The Authority shall conduct a data protection audit pursuant to the request of the controller. The fee defined in the ministry decree must be paid to conduct the data protection audit.

(3) The Authority shall register the outcomes of the data protection audit in an evaluation report compiled in connection with the audit. This evaluation report may put forth recommendations for the controller. The evaluation report is public, unless otherwise requested by the controller.

(4) The data protection audit does not restrict the Authority from exercising the scopes of authority defined within the scope of the present Act.

37. Initiating Criminal, Infringement and Disciplinary Proceedings

Section 70

(1) The Authority shall initiate criminal proceedings with the body authorised to launch such proceedings if the Authority suspects that an offence has been committed during the course of the procedure. The Authority shall initiate infringement or disciplinary proceedings with the body authorised to launch such proceedings if the Authority suspects that an infringement or disciplinary violation has been committed during the course of the procedure.

(2) The body defined in subsection (1) shall notify the Authority of their position in connection with the launch of the procedure – unless otherwise regulated by law – within a period of 30 days and shall notify the Authority of its outcomes within a period of 30 days following its completion.

38. Data Control and Confidentiality

Section 71

(1) The Authority is authorised to control - to the extent and duration required for conducting the procedure - any personal data during the procedure, as well as data classified by law as confidential information and linked to exercising their profession, which relate to the procedure and the control of which is required to efficiently conduct the procedure.

(2) The Authority is entitled to use data acquired during the course of the investigation within the scope of its administrative proceedings.

(3) The Authority may have access to data defined in Article 23 (2) of Act CXI of 2011 on the Commissioner of Fundamental Rights in accordance with the conditions set out in Article 23 (7) of Act CXI of 2011 on the Commissioner of Fundamental Rights.

(4) Within the scope of the procedure conducted in connection with the control of classified information, the vice president, executive public officer and inspector of the Authority may also gain access to classified information without holding any user authorisation defined in the act on the protection of classified information, if they hold an appropriate level personal attestation of security clearance.

(5) The president and vice president of the Authority, as well as individuals employed or contracted, or previously employed or contracted by the Authority - with the exception of providing data

defined in relevant legislation for other organisations – are obliged to safeguard personal data, classified information, data classified by law as confidential information and confidential information associated with their professional practice they acquired knowledge of in connection with the responsibilities of the Authority and the provision of these during the course of their period of employment, as well as after, in addition to all data, facts and circumstances the Authority is not obliged to ensure public access to in accordance with provisions governing the relevant legislation.

(6) The obligation to provide safeguards in the case of individuals listed in subsection (5) extends to their not being permitted to disclose any data, facts or circumstances they acquired knowledge of during the course of performing their responsibilities in an unauthorised manner; nor are they allowed to use these or ensure access to these for third parties.

CHAPTER 7

FINAL PROVISIONS

Section 72

(1) The Government shall be authorised to issue decrees in respect of

a. defining the detailed set of regulations adopted in connection with the electronic disclosure of data of public interest;
b. defining the cost items and the highest value of these taken into account in connection with determining the fee to be paid for making copies to satisfy requests for data of public interest, as well as criteria to be applied to determine the large size of the document of which a copy is requested;
c. determining the special disclosure list.

(2) Authorisation shall be provided to

a. the minister competent for the scope of responsibilities, in order for the minister to determine a special disclosure list for bodies under their respective scope of management or supervision within the scope of a decree;
b. the minister responsible for e-administration, in order for the minster to define disclosure templates required for publishing data listed in special disclosure lists within the scope of a decree;
c. the minister responsible for the direction of civil national security services, the minister responsible for the direction of civil intelligence services, as well as the minister for defence to define – by requesting the position of the Authority – the scope of data to be disclosed by national security agencies under their supervision within the scope of a decree.

(3) The minister for justice shall - by requesting the position of the Authority and in agreement with the minster responsible for tax policies - be authorised to define the detailed set of regulations to be adopted in connection with the rate of the administrative fee to be paid for registration in the data protection file and the data protection audit, as well as the collection, administration, registration and reimbursement of this fee.

Section 73

(1) The present Act - with the exception of specifications defined in subsections (2) and (3) - shall enter into force following the day of its proclamation.

(2) Sections 1-37, Section 38 Subsection (1)–(3), Section 38 Subsection (4) (a)-(f), Section 38 Subsection (5), Section 39, Sections 41–68, 70–72, 75–77 and 79–88, as well as Annex 1 shall enter into force on 1 January 2012.

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

Section 74

The Prime Minster shall put forth their recommendation for the president of the Authority to the President of the Republic of Hungary by 15 November 2011. The President shall appoint the first president of the Authority, to take effect as of 1 January 2012.

Section 75

(1) The Authority shall proceed in accordance with regulations governing the present Act in cases in progress on the grounds of submissions received by the data protection commission prior to 1 January.

(2) Data controlled within the scope of responsibilities of the data protection commissioner prior to 1 January 2012 shall be controlled by the Authority from 1 January 2012.

(3) Requests for data control registration under the scope of data protection registration of the present Act initiated prior to 1 January 2012; however, not registered in the data protection file up to 1 January 2012 must be requested from the Authority after 30 June 2012 in accordance with regulations governing the present Act, which, should it be omitted, implies that data control will be interrupted following 30 June 2012. Data control activities defined under the present section cannot be carried out either should, on the grounds of the request for registration submitted after 31 December 2011, the Authority have rejected registration.

Section 76

Chapter 5 of the present Act qualifies as a cardinal provision pursuant to Article 6 (3) of the Fundamental Law.

Section 77

The present 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 2008/98/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

Section 79

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 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

Section 83

Section 84

Section 85

Section 86

Section 87

Section 88

Section 89

Annex 1 to Act CXII of 2011

GENERAL LIST OF DATA PUBLISHED

I. Organisational, Personal Data

	Data	Updating	Safeguarding
1.	Official name, seat, postal address, telephone and fax number, email address, website and customer service contact details of the body undertaking public duties	Immediately following modification	Previous state to be deleted
1.	Organisational structure of the body undertaking public duties by indicating organisational units and the responsibilities of specific organisational units	Immediately following modification	Previous state to be deleted
1.	Name of the executives of the body undertaking public duties; name of the executives of specific organisational units, their positions and contact details (telephone and fax number, email address)	Immediately following modification	Previous state to be deleted
1.	Name and contact details of the customer service manager competent within the organisation (postal address, telephone and fax number, email address) and customer service business hours	Immediately following modification	Previous state to be deleted
1.	Staff size, composition, name of members, their positions and contact details in the case of official bodies	Immediately following modification	Previous state to be deleted
1.	Name of other bodies under the management, supervision or control of the body undertaking public duties, or subordinates to the latter, as well as their data as defined under Point 1	Immediately following modification	By preserving the previous state in the archives for one year
1.	Name, seat and contact details (postal address, telephone and fax number, email address) of the business organisation under the majority ownership of the body undertaking public duties, or operating in association with this body; their scope of activities, ratio of shares held by the body undertaking public duties	Immediately following modification	By preserving the previous state in the archives for one year
1.	Name, seat and contact details (postal address, telephone and fax number, email address) of foundation founded by the body undertaking public duties; the statutes of this organisation and members of its executive body.	Immediately following modification	By preserving the previous state in the archives for one year
1.	Name, seat and reference number of the founding regulation of the budgetary organisation founded by the body undertaking public duties, as well as the decision of the foundation, the statues of the budgetary organisation, its executive, website details and operating license	Immediately following modification	By preserving the previous state in the archives for one year
1.	Name of newspapers founded by the body undertaking public duties; their address and the name of the editor-in-chief	Immediately following modification	By preserving the previous state in the archives for

			one year
1.	Date defined under Point 1 of the supervisory body of the body undertaking public duties authorised to appeal against official decisions, or the body exercising legitimate supervision over the body undertaking public duties	Immediately following modification	By preserving the previous state in the archives for one year

II. Data concerning activities, operations

	Data	Updated	Safeguarding
1.	Key legislation, instruments of public law, as well as the organisation and operational manual, regulations or rules of procedure relevant to defining the responsibilities, scope of authority and basic activities of the body undertaking public duties and the full text of the data protection and data security regulation in effect	Immediately following modification	By preserving the previous state in the archives for one year
1.	English and Hungarian versions of the document on the responsibilities and activities of the body undertaking public duties in the case of bodies with a national scope of competence, as well as the regional state administration body of the Government with a general scope of competency.	Immediately following modification	Previous state to be deleted
1.	Responsibilities assumed on a voluntary basis by the local government	Quarterly	By preserving the previous state in the archives for one year
1.	Name of the body, by type of case and procedure, competent in state administration and other official matters; name of the body competent to act in the case of the assignment of scope of authority, its scope of regional competence; defining the scope of documents and duty charged (administration service fees); fundamental rules of procedure, mode of submission of the document launching the procedure (time and place); customer service business hours, deadline for administration (deadline for processing and lodging objections); information regarding procedures and downloadable forms used for processing matters; access to available electronic programmes; making appointments, list of legislation in connection with the type of procedure, information on rights the customer is entitled to and the obligations of the client	Immediately following modification	Previous state to be deleted
1.	Name and content of public services provided by the body undertaking public duties or financed from its budget; rules of procedure for using public services; the fee charged for using public services and discounts offered	Immediately following modification	By preserving the previous state in the archives for one year
1.	Databases maintained by the body undertaking public duties, as well as the data parameters of files	Immediately following	By preserving the previous

	(name, format, objective of the data control, its legal grounds, scope of data subjects, source of the data and the questionnaire to be completed in the case of data recorded by questionnaire surveys); identification data as specified within the scope of the present Act for files to be entered into the data protection file; type of data collected and processed by the body undertaking public duties within its scope of basic activities, their mode of access and fee charged for making copies	modification	state in the archives for one year
1.	Title, theme, mode of access, free or paid access to the public publications of the body undertaking public duties, as well as the fee charged to access these.	Quarterly	By preserving the previous state in the archives for one year
1.	Rules of procedure for preparing the decisions of official bodies; mode of participation by nationals (issuing opinions); rules of procedure; the place and time the session was convened, as well as its public character, decisions made, minutes and summaries; data concerning voting if this is not restricted by relevant legislation.	Immediately following modification	By preserving the previous state in the archives for one year
1.	Bills and related documents to be published by law; submissions to the open session of local government representative bodies from their date of submission.	Immediately following the date of submission if otherwise not regulated by law	By preserving the previous state in the archives for one year
1.	Bulletins, communiqués published by the body undertaking public duties	Continuously	By preserving it in the archives for at least one year
1.	Technical description and reasons for calls for applications announced by the body undertaking public duties	Continuously	By preserving the previous state in the archives for one year
1.	Investigations, reviews carried out in connection with basic activities at the body undertaking public duties and their public findings	Immediately after gaining access to the investigation report	By preserving it in the archives for at least one year
1.	Rules of procedure of request made to access data of public interest; the name of the competent organisational unit, its contact details, name of the data protection officer or individual competent for information right in units where such appointments are made.	Quarterly	Previous state to be deleted

1.	Results and changes to statistical data collected in relation to the activities of the body undertaking public duties	Quarterly	By preserving it in the archives for at least one year
1.	Data of mandatory provision of statistical data in relation to data of public interest concerning the given body	Quarterly	By preserving it in the archives for at least one year
1.	List of contracts aimed at using data of public interest of which the body undertaking public duties is one of the signatories.	Quarterly	By preserving it in the archives for at least 1 year
1.	General terms of contract concerning the use of data in the public interest under the management of the body undertaking public duties	Immediately following modification	By preserving it in the archives for at least one year
1.	Special disclosure list concerning the body undertaking public duties	Immediately following modification	Previous state to be deleted

III. Financial Data

	Data	Updating	Safeguarding
1.	Annual budget of the body undertaking public duties, report compiled in compliance with the Accountancy Act; reports compiled in connection with the implementation of the budget, according to the mode and frequency defined under separate legislation.	Immediately following modification	For the period specified under separate legislation; however, by keeping it in the archives for at least five years
1.	Aggregated data regarding the staff size and remuneration of employees at the body undertaking public duties; total amount of remuneration paid to executive staff members and executive officers, their salaries, regular benefits and reimbursements made; total type and rate of benefits offered to other employees.	Quarterly	For the period specified under separate legislation; however, by keeping it in the archives for at least one year
1.	The name of the beneficiary, the objective of the funding, its amount and data concerning the place of implementation of the funded programme regarding non-normative, specific, operational and development funding granted from the budget of the body undertaking public duties	On the 60th day following the decision	For the period specified under separate legislation; however, by keeping it in the archives for at least one year
1.	List (type) of contracts concerning the procurement of goods, building investments, services ordered, sale of property, use of property, assignment of property or property rights, as well as the assignment of concessions executed by using public finances and associated with financial management relating to the state budget, the value	On the 60th day following the decision	For the period specified under separate legislation; however, by keeping it in the archives for at least one year

	of which is defined under separate legislation; the object of the contract, the name of the contracting parties, the value of the contract, the duration of the contract in the case of contracts concluded for a definite period.		
1.	Public data defined in the Act on concessions (calls for applications, data of applicants, reminders compiled in connection with assessment, the result of the application procedure)	Quarterly	For the period specified under separate legislation; however, by keeping it in the archives for at least one year
1.	Payments made by the body undertaking public duties exceeding five million HUF in connection with the provision of non-statutory responsibilities (therefore, with special regard to payments made for funding civil society organisations, responsibilities of professional and interest representation bodies, their employees and associates; funding organisations engaging in educational, cultural, social and sports activities, responsibilities undertaken by foundations)	Quarterly	For the period specified under separate legislation; however, by keeping it in the archives for at least one year
1.	Description of developments implemented from EU funding and their relevant contracts	Quarterly	By keeping it in the archives for at least one year
1.	Public procurement information (annual plan, summary of the assessment of offers submitted and contracts concluded)	Quarterly	By keeping it in the archives for at least one year