Strasbourg, 24 September 2012

CDL-REF(2012)021

Opinion No. 672 / 2012

Engl. only

EUROPEAN COMMISSION FOR DEMOCRACY THROUGH LAW
(VENICE COMMISSION)

ACT CXII
of 2011

ON INFORMATIONAL SELF-DETERMINATION AND FREEDOM OF INFORMATION

OF HUNGARY

This document will not be distributed at the meeting. Please bring this copy.
www.venice.coe.int

Act CXII of 2011

On Informational Self-determination and Freedom of Information

To ensure the right to informational self-determination and freedom of information, and to implement the Fundamental Law, the Parliament hereby adopts the following Act on the fundamental rules for the protection of personal data and the enforcement of the right to access and disseminate data of public interest and data public on grounds of public interest, and on the authority competent to monitor these rules, pursuant to Article VI of the Fundamental Law:

CHAPTER I

GENERAL PROVISIONS

1. Object of the Act

Article 1

The object of this Act is to define the fundamental rules for controlling data to ensure that the data controllers respect the private sphere of natural persons and to achieve transparency in public affairs through the enforcement of rights to access and disseminate data of public interest and data public on grounds of public interest.

2. Scope of the Act

Article 2

(1) The scope of this Act covers all data control and data processing activities performed 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) This Act shall apply to fully or partially automated or manual data control and data processing.

(3) The provisions of this Act shall apply if the data controller controlling personal data outside the territory of the European Union contracts a data processor with a seat, site, branch or domicile or place of residence within the territory of Hungary or uses a device here 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) The provisions of this Act shall not apply to natural persons controlling data exclusively for their own personal purposes.

(5) Concerning further use of public sector information, rules other than those of this Act can be laid down by law for the mode and conditions of data provision the consideration to be paid, as well as in respect of legal remedy,.

3. Definitions

Article 3

For the purposes of this Act:

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

Personal data: data relating to the data subject, in particular, their name and identification number, as well as one or more factors specific to their physical, physiological, mental, economic, cultural or social identity as well as conclusions drawn from the data concerning the data subject.

Special data:

a) personal data concerning racial origin, nationality, 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.

Criminal personal data: personal data relating to the data subject or criminal conviction, generated in the course of or prior to the criminal proceedings, in connection with a criminal act or criminal proceedings at the bodies authorised to conduct criminal proceedings or to detect a criminal act, as well as at penal institutions.

Data of public interest: information or data other than personal data, registered in any mode or form, controlled by the body or individual performing state or local government responsibilities, as well as other public tasks defined by legislation, concerning their activities or generated in the course of performing their public tasks, regardless of the mode of control, its independent or collective nature; in particular, data concerning the scope of authority, competence, organisational structure, professional activity and its evaluation including efficiency, the type of data held and the legislation regulating operation, as well as data concerning financial management and concluded contracts.

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

Consent: any freely given specific and informed indication of the data subject's will, by which they unambiguously agree to the full control of their personal data or to the extent of specific operations.

Objection: declaration made by the data subject objecting to the control of their personal data and requesting the termination of data control, as well as the deletion of the data controlled.

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

Data control: any operation or the totality of operations performed on the data, regardless of the procedure applied; in particular, collecting, recording, registering, classifying, storing, modifying, using, querying, transferring, disclosing, synchronising or connecting, blocking, deleting and destructing the data, as well as preventing their further use, taking photos, making audio or visual recordings, as well as registering physical

characteristics suitable for personal identification (such as fingerprints or palm prints, DNA samples, iris scans).

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

Disclosure: ensuring open access to the data.

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

Tagging data: marking data with a special ID tag to differentiate it.

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

Data destruction: complete physical destruction of the storage medium containing the data.

Data processing: performing 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 execution, provided that the technical task is performed on the data.

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 concluded pursuant to legislative provisions.

Data officer: the body performing public tasks which generated the data of public interest to be published mandatorily by electronic means, or during the operation of which this data was generated.

Data publisher: the body performing public tasks which publishes the data transferred by the data officer on its website, if the officer does not published them.

Data set: the totality of data controlled in a single file.

Third party: any natural or legal person, or organisation without legal personality other than the data subject, the data controller or the data processor.

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 and the State which is not party to the Agreement on the European Economic Area

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

CHAPTER II

PROTECTION OF PERSONAL DATA

4. Principles of Data Control

Article 4

(1) Personal data may exclusively be controlled for a specific purpose to exercise rights and fulfil 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 essential and suitable to achieve the purpose of the control may be controlled. Personal data may only be controlled to the extent and for the time required to achieve the purpose.

(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 disposal.

(4) The accuracy, integrity and – if required for the purpose of the data control – actuality of the data has to be ensured during the course of the data control, the data subject should only be identifiable for the time required for the purpose of the data control.

5. Legal Basis of Data Control

Article 5

(1) Personal data may be controlled if

a) the data subject agrees to it, or

b) it is provided for by law or – by authorisation of law, within the scope defined in that law – a local government decree for purposes in the public interest (hereinafter: mandatory data control).

(2) Special data may be controlled in cases specified in Article 6 or if

a) the data subject agrees to it in writing;

b) it is necessary for the implementation of an international treaty adopted within the framework of a law in the case of data specified in Article 3, point 3. a), or if provided for by law to enforce fundamental rights ensured in the Fundamental Law, in the interest of national security, to prevent or prosecute criminal acts, or serves national defence interests, or

c) it is provided for by law for purposes in the public interest in the case of data listed in Article 3, point 3. b).

(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 data controller.

(4) Only state or local government bodies are entitled to control criminal personal data related to the prevention and prosecution of criminal acts and controlled to perform public

administrative and judicial tasks, as well as files containing data in connection with offences, civil litigation and non-litigation matters.

Article 6

(1) Personal data may also be controlled if it is impossible or would entail disproportionate cost to obtain the consent of the data subject and the personal data

a) must be controlled to fulfil legal obligations of the data controller, or

b) must be controlled to enforce the rightful interests of the data controller or a third party and the enforcement of such interests is proportionate to the restrictions of the right to the protection of personal data.

(2) Should the data subject be unable to give their consent due to incapacity to act or other unavoidable reason, the personal data of the data subject may be controlled to protect their own or other persons' vital interests to the extent required, during the period in which consent is unavailable, as well as to avert or prevent imminent danger to the lives, physical integrity or possessions of persons.

(3) The consent or subsequent approval of the legal representative is not required for legal declarations containing the consent of minors aged over 16.

(4) If the aim of the data control based on consent is to execute the contract concluded in writing with the data controller, such contract must include all information the data subject must be aware of – under this Act – relating to the control of personal data, in particular, the determination of the data to be controlled, the duration of control, the purpose of use, the fact of the transfer of data, its recipients and the fact 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 their 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 data controller may, unless otherwise regulated by law, also control the data recorded

a) to fulfil their relevant legal obligations, or

b) to enforce the rightful interest of the data controller or third party if the enforcement of these interests is proportionate to the restriction of the protection of personal data

without further specific consent, even after the data subject withdrew their consent.

(6) The consent of the data subject shall be presumed in respect of personal data necessary to conduct the legal or administrative proceedings launched upon his request or initiative, and in respect of personal data provided by him in other proceedings launched upon his request.

(7) The consent of the data subject shall be considered as granted in respect of personal data communicated or provided for disclosure by them during their public appearance.

(8) In case of doubt, it shall be presumed that the data subject did not provide their consent.

6. The Requirement of Data Security

Article 7

(1) The data controller must plan and execute data control operations to ensure the protection of the private sphere of data subjects throughout the application of this Act and other regulations applicable to data control.

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

(3) The data must be protected by appropriate measures, particularly from unauthorised access, modification, transfer, disclosure, deletion or destruction, accidental destruction and damage as well as inaccessibility 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 by appropriate technological solutions that – unless permitted by law – data stored in the files cannot be directly connected and linked to the data subject.

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

a) the prevention of unauthorised data entry;

b) the prevention of the use of automatic data processing systems by unauthorised persons by using data transfer devices;

c) the possibility to verify and establish which bodies the personal data have been or can be transmitted to using a data transfer device;

d) the possibility to verify and establish which personal data have been registered in the automatic data processing systems, when and by whom;

e) the possibility to restore the systems installed in the event of malfunctions and;

f) reporting on errors occurring during the course of automated processing.

(6) The data controller and data processor must take account of the current level of development of the relevant technology when determining and applying measures to protect the data. From among several possible data control solutions the one which ensures a higher level of protection of the personal data shall be chosen, unless this causes disproportionate difficulties for the data controller.

7. Data Transfer to Other Countries

Article 8

(1) Data controllers under the scope of this Act are allowed to transfer personal data to controllers controlling data in third countries or to deliver such data to data processors processing data in third countries, if

a) the data subject has provided their explicit consent, or

b) the conditions set out under Article 5 and Article 6 have been fulfilled and − except for the case under Article 6 (2) − an appropriate level of protection of the personal data is ensured in the third country during the course of the control and processing of the data transferred.

(2) Appropriate level of protection of the personal data is ensured if

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

b) an international treaty, concluded between the third country and Hungary, guaranteeing the enforcement of rights under Article 14 and the assurance of legal redress for the data subject, as well as the independent supervision of data control and data processing procedure be in effect.

(3) Personal data may be transferred to third countries − even in the absence of conditions set out in paragraph (2) − to execute the international agreement on the exchange of information relating to taxation and avoiding double taxation, for the purpose defined in the international agreement, in accordance with the conditions and scope of data set out in it.

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

8. Restrictions to Data Control

Article 9

(1) Should the data controller − pursuant to provisions of law, international treaty or a binding legal act of the European Union − receive personal data in a manner that the data transferring data controller indicates at the time of the transfer of the personal data

a) the possible objective of the data control,

b) possible duration of the data control,

c) possible recipients of the data transferred,

d) restriction of rights of the data subject ensured in this Act, or

e) other restrictions regarding control

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

(2) The data recipient is also entitled to control the personal data irrespective of the data control restrictions and to guarantee the rights of the data subject if the data transferring data controller have provided their preliminary consent.

(3) Pursuant to provisions of law, international treaty or a binding legal act of the European Union, the data controller shall notify the recipient at the time of transferring the personal data of the data control restrictions to be applied..

(4) The data controller is entitled to provide the consent specified in paragraph (2), if it does not conflict with legal provisions to be applied to legal subjects under the jurisdiction of Hungary.

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

9. Data Processing

Article 10

(1) The data controller defines the rights and obligations of the data processor in relation to the processing of personal data within the framework of this Act and separate laws on data control. The data controller is responsible for the legality of their instructions.

(2) The data processor is not permitted to use other data processors during the course of their activities.

(3) The data processor is not authorised to make any substantive decision affecting the data control; may only process the personal data received in accordance with the instructions of the data controller; is not authorised to process data for their own purposes and shall store and preserve the personal data in compliance with the instructions of the controller.

(4) The contract on data processing must be concluded in writing. Organisations with commercial interests in the use of the personal data to be processed cannot be contracted for data processing.

10. Decision by Automated Data Processing

Article 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, if the decision

a) was made when concluding or executing a contract, provided that it has been initiated by the data subject or

b) is permitted by law which also specifies measures protecting the rightful interests of the data subject.

(2) At 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. Control of Personal Data in Scientific Research

Article 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 definitively be made impossible. In the meantime, data suitable for the

identification of individuals must be stored separately. This data can only be linked to other data if this is required for the purpose of the research.

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

a) the data subject consents to this, or

b) this be required to present the results of research on historical events.

12. Use of Personal Data for Statistical Purposes

Article 13

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

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

13. Rights of Data Subjects and their Enforcement

Article 14

The data subject may request from the data controller:

a) information on the control of their personal data,

b) correction of their personal data, and

c) deletion or blocking of their personal data, except in the case of mandatory data control.

Article 15

(1) At the request of the data subject, the data controller shall provide information on the data subject's data controlled, as well as the data processed by the data processor contracted, its sources, the objective of the control, its legal grounds and duration, the name and address of the data processor and their activities related to the data control, and − in case of transfer of the data subject's personal data − the legal grounds and recipients of the data transfer.

(2) The data controller keeps a record of the data transferred to verify the legality of the data transfer and to inform the data subject, which contains the time of transfer of the personal data controlled, the legal grounds and recipients of the transfer, the scope of the personal data transferred, as well as other data specified in legislation requiring data control.

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

(4) The data controller shall provide comprehensible information at the data subject's request in writing within the shortest possible time but no later than thirty days following the submission of the request.

(5) Information specified in paragraph (4) is free of charge, if the applicant has not yet submitted a request for information in the same year to the data controller covering the same data. In other cases, a fee may be charged. The parties can record the rate of the fee in contract. The fee paid must be reimbursed if the data were controlled unlawfully, or if the request for information has lead to correction of the data.

Article 16

(1) The data controller can only deny a request for information in cases specified in Article 9 (1) and Article 19.

(2) If the request for information is denied, the data controller shall notify the data subject in writing of the relevant article of this Act, based on which the request for information was denied. If the request for information is denied, the data controller shall inform the data subject of the possibility of legal redress and turning to the National Authority for Data Protection and Freedom of Information (hereinafter Authority).

(3) The data controller notifies the Authority of rejected requests until 31 January of the following year.

Article 17

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

(2) Personal data must be deleted if

a) its control is unlawful;

b) it has been requested by the data subject pursuant to point c) of Article 14;

c) it is incomplete or incorrect – and this cannot be remedied – provided that deletion is not ruled out by law;

d) the objective of the data control has ceased to exist or the period for storing the data set out by law has expired;

e) it has been ordered by the court or the Authority.

(3) The deletion obligation in point d) of paragraph (2) does not apply to personal data recorded on a data storage medium to be placed in the archives in accordance with legislation governing the preservation of archival materials.

(4) Instead of deletion, the data controller blocks the personal data if the data subject so requests, or if, based on information available, deletion would presumably violate the rightful interests of the data subject. Personal data so blocked may only be controlled until the objective of the data control which excluded the deletion of the personal data, persists.

(5) The data controller tags the personal data controlled if the data subject disputes its correctness or accuracy, but the incorrectness or inaccuracy of the disputed personal data cannot be explicitly established.

Article 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, tagging and deletion. The notification can be omitted if this does not violate the rightful interest of the data subject with regard to the objective of data 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 thirty 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 possibility of legal redress or turning to the Authority.

Article 19

The rights of the data subject under Articles 14–18 may be restricted by law for reasons of external and internal state security, in particular, for reasons of national defence, national security, prevention or prosecution of criminal acts, the security of penal institutions, as well as in the economic and financial interests of the state or local governments; in the major economic and financial interest of the European Union, and to prevent and expose disciplinary and ethical offences, labour law related and occupational safety infringements – including in each case the control and supervision – and to protect the rights of the data subject or others.

14. The Requirement of Prior Notification of the Data Subject

Article 20

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

(2) Prior to the data control the data subject must be explicitly informed in detail of every fact relating to the control of their data, in particular, of the objective of the data control and its legal grounds, the individual authorised to control and process the data, the duration of the data control, whether the personal data are controlled pursuant to Article 6 (5) as well as of who have access to the data. This information must include the rights and legal redress opportunities of the data subject in connection with the data control.

(3) In the case of mandatory data control, information may also be provided by publishing a reference to legislative provisions specifying information set out in paragraph (2).

(4) If it is not possible to personally inform the data subject or it would entail disproportionate cost,, information may also be provided by disclosing the following information:

a) the fact of the data collection,

b) the data subjects concerned,

c) purpose of the data collection,

d) duration of the data control,

e) potential data controllers having access to the data,

f) information on the rights and legal redress opportunities in connection with the data control, and

g) the data control registration number, if the data control is subject to data protection registration, except in the case specified in Article 68 (2).

15. Objection to the Control of Personal Data

Article 21

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

a) if the personal data are controlled or transferred to fulfil the legal obligations of the data controller, or enforce the rightful interests of the data controller, data recipient or third party except in the case of mandatory data control;

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

c) in other cases defined by law.

(2) The data controller shall assess the objection within the shortest possible time but no later than fifteen days following the submission of the request, decides on its merits and notifies the applicant of the decision in writing.

(3) If the data controller establishes that the objection is justifiable, it terminates the data control – including any further data entry and data transfer –, blocks the data and notifies of the objection and of the measures taken to whom the personal data concerned was previously transferred and who are obliged to take measures to enforce the right to object.

(4) If the data subject disagrees with the data controller's decision based on paragraph (2), or if the data controller fails to observe the deadline set in paragraph (2), the data subject can initiate legal proceedings – as set out in Article 22 – within a period of thirty days following the announcement of the decision or the deadline.

(5) If the data recipient does not receive the data required to enforce their rights due to the objection of the data subject, they can initiate legal proceedings against the data controller – as set out in Article 22 – to gain access to the data, within a period of fifteen days following the announcement of the decision pursuant to paragraph (3). The data controller can summon the data subject to court.

(6) If the controller fails to send the notification under paragraph (3), the data recipient can request information from the data controller on the failure of the data transfer, which the data controller is obliged to provide within a period of eight days following the receipt of the request. In the case of request for information, the data recipient can initiate legal

proceedings against the data controller within a period of fifteen days following the information is provided, but no later than fifteen days following the deadline set for the provision of the information. The data controller can summon the data subject to court.

(7) The data controller cannot delete the data subject's data if the data control was ordered by law. However, the data cannot be transferred to the data recipient if the data controller agreed with the objection, or if the court established that the objection was justified.

16.

17. Enforcement of Rights in Court

Article 22

(1) The data subject, as well as the data controller against the data recipient in cases listed under Article 21, are entitled to initiate legal proceedings in case of infringement of their rights. The courts shall take immediate action in such cases.

(2) The data 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 legality of the data transfer in cases listed in Article 21 (5) and (6).

(3) The tribunal shall be competent to assess the case. The legal procedure may be launched at the tribunal for the place where the data subject is domiciled or resident, at the choice of the data subject.

(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 favour of the data subject.

(5) Should the court entertain the motion, the data controller shall be obliged to provide information, correct, block and delete the data, reverse the decision made by automated data processing, take account of data subject's right to object and issue the data requested by the data recipient defined under Article 21.

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

(7) The court can order the public disclosure of the judgment – by disclosing the data controller's identification data – should this be in the interest of data protection and the rights of a higher number of data subjects protected by this Act.

18. Compensation

Article 23

(1) The data controller shall be obliged to compensate for damages caused by the unlawful control of the data subject's data or the breach of data security requirements. The data controller is responsible to the data subject for damage caused by the data processor. The data

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.

19. Internal Data Protection Officer and Data Protection Regulation

Article 24

(1) An internal data protection officer – with a 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 data controller or data processor

a) at the data 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) contribute to and assist in making decisions in connection with data control and in guaranteeing the rights of the data subjects;

b) control compliance with provisions of this 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 calls on the data controller or data processor to terminate unauthorised data control;

d) compile the internal data protection and data security regulation;

e) manage the internal data protection file;

f) organise data protection training.

(3) Data controllers defined in paragraph (1), as well as other state and local government data controllers – with the exception of data controllers not obliged to submit reports in the data protection file - are required to compile an internal data protection and data security regulation to implement this Act.

20. Conference of Internal Data Protection Officers

Article 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 uniform application of legislation on the protection of personal data and access to data of public interest.

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

(3) The internal data protection officers of every organisation where the appointment is required by law, are members of the conference.

(4) The internal data protection officers who do not have to be appointed by law may also be members of this conference. They can register to 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 database contains the internal data protection officer's name, their postal and email address, as well as the organisation they represent.

(6) The Authority maintains the data defined in paragraph (5) until it becomes aware of the expiry of the data protection officer's the mandate.

CHAPTER III

ACCESS TO DATA OF PUBLIC INTEREST

21. General Rules Concerning Access to Data of Public Interest

Article 26

(1) Bodies or individuals performing state or local government tasks, as well as other public tasks defined in legislation (hereinafter jointly referred to as body performing public tasks) must ensure access to data of public interest and data public on grounds of public interest in their control to anyone requesting such data, with the exception of cases defined in this Act.

(2) The name of the person acting on behalf of the body performing public tasks, as well as their scope of responsibilities, scope of work, executive mandate and other personal data relevant to the performance of public tasks, and their personal data to which access must be ensured by law qualify as data public on grounds of public interest.

(3) Unless otherwise regulated by law, data public on grounds of public interest are data controlled by bodies or individuals providing mandatory services or services which cannot be provided through other means, based on legislation or contract concluded with a state or the local government body, which are relevant to their activities and do not qualify as personal data.

Article 27

(1) Data of public interest and data public on grounds of public interest cannot be accessed if it qualifies as classified information pursuant to 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 criminal acts;

d) in the interest of environmental protection or nature preservation;

e) in the interest of central financial and foreign exchange 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 of the Civil Code apply to access to business secret.

(4) Access to data of public interest may be restricted pursuant to a legal act of the European Union with regard to major financial or economic policy interests of the European Union, including monetary, budgetary and tax policy interests.

(5) Data generated or registered during the course of the decision-making process of the body performing public tasks, which serve as a basis for decision-making shall not be disclosed for a period of ten years following its generation. The head of the body controlling this data is entitled to authorise access to it by weighing the public interest in ensuring or denying access to this data.

(6) Requests for access to data serving as a basis for decision-making may be rejected after the decision-making– within the period defined in paragraph (5) – if access to this data jeopardizes the legal operation of the body performing public tasks or the unbiased performance of its responsibilities, in particular, the free expression of its position generating the data during the decision-making process.

(7) Legislation may specify a shorter period than set out in paragraph (5) to restrict access to certain data serving as a basis for decision-making

(8) Provisions of this chapter cannot be applied to the provision of data from authentic registers, regulated by separate law.

22. Demand for Access to Data of Public Interest

Article 28

(1) Anyone can request access to data of public interest orally, in writing or electronically. Provisions on access to data of public interest shall be applied to access of data public on grounds of public interest.

(2) Unless 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 data controller requests further specification from the applicant.

Article 29

(1) The body performing public tasks controlling the data shall ensure access to data of public interest within the shortest possible time, but within a maximum period of fifteen days.

(2) The deadline set in paragraph (1) may be extended once by fifteen 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 performing public tasks controlling the data is entitled to charge a fee for making copies – to the extent of costs incurred – 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, the request for copy shall be satisfied within a period of fifteen 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 where copying is not needed to satisfy data access requirements within a period of eight days following the receipt of the request.

(5) The relevant legislation regulates cost items and their highest level to be 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.

Article 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 must be made unrecognisable in the copy.

(2) Data requests must be satisfied in a comprehensible manner and in a mode and by the technical means 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 data. Requests for data cannot be rejected by claiming that they cannot be satisfied in a comprehensible manner.

(3) The applicant must be notified of the rejection, the reasons for the rejection, as well as information on legal remedies available under this Act in writing, or electronically if they provided their email address in the request, within a period of eight days. The data controller shall keep a record of requests rejected and reasons for their rejection and shall inform the Authority of it each year by 31 January.

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

(5) Should the law allow for the discretion of the controller to reject the request for access to data of public interest, a narrow interpretation must be applied to such rejection and access to data of public interest may only be rejected if the public interest serving as a basis for the rejection prevails over the public interest relating to the access to data of public interest.

(6) The body performing public tasks shall compile a regulation setting out the rules of procedure for fulfilling requests for access to data of public interest.

Article 31

(1) The applicant is entitled to turn to the courts should the deadline for the rejection or fulfilment of the request for access to data of public interest, or the deadline extended by the data controller in accordance with Article 29 (2) expire without result, and in addition is entitled to ask the review of the fee charged for making a copy, if the fee has not yet been paid.

(2) The data controller shall prove the legality of rejection and its reasons and the substantiation of the fee charged for making a copy.

(3) Litigation must be launched against the body performing public tasks within a period of thirty days following the announcement of the rejection of the request, the expiry of the deadline without result and the expiry of the deadline set for paying the fee charged. Should the applicant 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, litigation can be initiated within a period of thirty days following the receipt of the notification on the refusal of substantive assessment of the request for investigation, termination of the investigation, its closure pursuant to point b) of Article 55 (1) or notification specified in Article 58 (3). Missing the deadline to launch the proceedings can be justified.

(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 performing public tasks with country-wide competence fall under the jurisdiction of the tribunal. Matters under the jurisdiction of the local court shall be processed at the local court at the seat of the tribunal, in Budapest the Pest Central District Court. The competence of the court shall be based on the seat of the defendant body performing public tasks.

(6) The court shall take immediate action.

(7) Should the court grant the request for data of public interest, it shall oblige the data controller to disclose the data of public interest requested. The court is entitled to modify the fee charged for making a copy, or order the body performing public tasks to launch a new procedure to determine the sum of the fee charged.

CHAPTER IV

DISCLOSING DATA OF PUBLIC INTEREST

23. Information Obligation Concerning Data of Public Interest

Article 32

In matters within their scope of responsibilities the body performing public tasks is obliged to facilitate and ensure accurate and prompt information to the public, in particular, on the state and local budget and their implementation, management of the state or local government assets, use of public funds and contracts concluded in this regard, special or exclusive rights for market players, private organisations and individuals.

24. Electronic Disclosure Obligation

Article 33

(1) Access to data defined as data of public interest pursuant to this 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 possibility 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) Unless otherwise regulated by law, the following organisations shall publish the data defined in disclosure lists specified under Article 37 on their respective websites:

a) Office of the President of the Republic, Office of the Parliament, Office of the Constitutional Court, Office of the Commissioner for Fundamental Rights, State Audit Office of Hungary, Hungarian Academy of Sciences, Hungarian Academy of Arts, National Office for the Judiciary, Office of the Prosecutor General;

b)

c) central public administration body with the exception of the Government Committee, as well as the national chamber and

d) regional public administration body of the Government with general scope of authority.

(3) Bodies performing public tasks not listed in paragraph (2) may also fulfil their electronic disclosure obligations set out in Article 37 by disclosing data on their website operated alone or jointly with associated bodies, or maintained by their supervisory, governing or coordinating bodies or on the central website created for this purpose.

(4) Should the public education institution not undertake national or regional responsibilities, electronic disclosure obligations under this Act shall be fulfilled by providing data to information systems defined under sectoral legislation.

Article 34

(1) The data officer not publishing the data on their own website - by applying Article 35 – transfers the data to be published to the data publisher, which ensures the publication of the data on their website, and that the origin of the data of public interest and its connection to the body providing it is recognisable.

(2) The data publisher shall design the website used to publish the data to be suitable for publication of data; ensures its ongoing operation, repairs potential malfunctions and updates the data.

(3) The website used to publish the data shall provide comprehensible information on the detailed rules of requesting public data. This information must include information on options for legal redress.

(4) In addition to 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.

Article 35

(1) The head of the body responsible for the data and obliged to electronically disclose it shall ensure the accurate, updated and ongoing publication of the data specified in disclosure lists under Article 37 and its transfer to the data publisher.

(2) The data publisher is responsible for the electronic disclosure, continuous access, authenticity and updating of the data provided.

(3) To fulfil the obligations set out in paragraph (1) the data officer, to fulfil obligations set out in paragraph (2) the data publisher shall establish detailed rules in an internal regulation.

(4) Unless otherwise regulated by this 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 fulfilling disclosure obligations.

Article 36

Disclosure of data specified in the disclosure lists defined under Article 37 does not affect obligations of the body regarding the publication of data of public interest or data public on grounds of public interest or other obligations set out under the relevant legislation.

25. Disclosure Lists

Article 37

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

(2) Legislation may specify other data to be disclosed with respect to specific sectors and types of bodies performing public tasks (hereinafter special disclosure list).

(3) The head of the body obliged to disclose data – after requesting the opinion of the Authority – as well as legislation may define additional data to be disclosed as a mandatory requirement applicable to bodies performing public tasks, and bodies under their supervision (hereinafter individual disclosure list).

(4) The scope of data to be disclosed by civil national security services shall be defined by decree of the Minister in charge of the direction of civil national security services and the Minister competent for the direction of civil intelligence activities, the scope of data to be disclosed by the National Military Security Service shall be defined by decree of the Minister for Defence – after requesting the opinion of the Authority.

(5) Corporate bodies obliged to disclose information are competent to compile and modify the individual disclosure list, after having requested the opinion of the Authority.

(6) The head of the body obliged to disclose information annually reviews the disclosure list issued pursuant to paragraph (3) based on requests for data concerning data of public interest not included in the disclosure list and amends the list on the basis of the high rate or volume of requests submitted.

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

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

24/A Central electronic register of data of public interest and uniform public data search system

Article 37/A

(1) For the purpose of the simple and quick accessibility of electronically published data, the central electronic register published on the website established for this purpose and operated by the minister responsible for ensuring the infrastructural feasibility of public administration informatics shall contain aggregately the descriptive data on the website containing data of public interest of the bodies obliged to publish electronically data of public interest under this Act as well as on databases and registers maintained by them.

(2) The uniform public data search system operated by the minister responsible for ensuring the infrastructural feasibility of public administration informatics shall ensure the electronic access to the data of public interest of the body specified in paragraph (1) based on uniform criteria and the searchability of the data of public interest.

Article 37/B

(1) The data officer shall provide for the transfer of the descriptive data of websites, databases and registers managed containing data of public interest to the minister responsible for ensuring the infrastructural feasibility of public administration informatics and shall provide for the update of the transferred data of public interest; he/she/it shall be also responsible for the content of the data of public interest transferred to the uniform public data search system and for the regular update of such data.

(2) The maintenance of the list of databases and registers containing data of public interest and the access to the uniform public data search system shall not exempt the data officer from the obligation of electronic publishing.

CHAPTER V

NATIONAL AUTHORITY FOR DATA PROTECTION AND FREEDOM OF INFORMATION

25. Legal Status of the Authority

Article 38

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

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

(3) In the performance of its tasks pursuant to paragraph (2) and in accordance with the provisions of 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 court proceedings for infringements relating 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 file.

g)

h)

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

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

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

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

d) shall give an opinion relating to special and/or individual publication lists concerning data to be published pursuant to this Act in connection with the activities of bodies performing public tasks;

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

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

g)

h)

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

26. Budget and management of the Authority

Article 39

(1) The Authority shall be a central budgetary body 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 governing body.

(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

Article 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 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 an academic 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 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 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 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.

Article 41

(1) The President of the Authority may not be member of a political party or engage in any political activity, and his 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 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.

Article 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 appointment, and thereafter by 31 January of each year, and within thirty days of the termination of his mandate.

(2) Should the President of the Authority fail to make a declaration of assets, he may not perform the tasks deriving from his office, and may not receive remuneration until he 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 a statement of facts on the specific content of the declaration of assets, submitted to the Prime Minister, 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 paragraph, 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 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.

Article 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.

Article 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.

Article 45

(1) The mandate of the President of the Authority shall be terminated by the following:

a) expiry of the term of mandate;

b) resignation;

c) death;

d) establishment of the absence of the conditions necessary for his appointment or the infringement of the provisions on the declaration of assets;

e) establishment of a conflict of interest;

f)

g)

(2) The President of the Authority may at any time resign from his 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, following the notice of the resignation or, failing this, on the day of the notice of 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 pursuant to Article 41 within thirty days of his appointment or if a conflict of interest arises in the course of the exercise of his office the President of the Republic shall decide on the conflict of interest upon the motion of the Prime Minister.

(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 the violation of the rules concerning the declaration of assets 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 forward his/her motion based on paragraphs (3) and (6) to the President of the Republic and the President of the Authority at the same time.

(6b) The President of the Authority may turn to the court to establish that the motion is unfounded within 30 days of the receipt of the motion; if the deadline has been missed, no justification shall be accepted. The President of the Authority must instigate the proceedings against the Prime Minister. The provisions of the Code of Civil Procedure relating to actions brought on the basis of an employment relationship and other similar legal relationships shall apply to the court's procedure with the exception that the Budapest Labour Court shall proceed in the case, with exclusive jurisdiction, in out-of-turn proceedings and shall forward the statement of claim and the final judgment on the merits to the President of the Republic.

(6c) If the court finds, in its final judgment based on the action brought by the President of the Authority under paragraph (6b) that the motion of the Prime Minister based on paragraphs (3) and (6) has been unfounded, the President of the Republic shall not terminate the mandate of the President of the Authority.

(6d) The President of the Republic shall decide on the motion of the Prime Minister based on paragraphs (3) and (6)

a) within 15 days of the deadline if the President of the Authority does not turn to the court within the deadline set in paragraph (6b),

b) within 15 days of receipt of the final judgment on the merits of the case if the President of the Authority turns to the court within the deadline set in paragraph (6b).

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

(8) Decisions assigned to the competence of the President of the Republic by paragraphs (3) and (6) and by Article 40 need not be countersigned.

Article 45/A

The President of the Authority shall have the right to participate and speak at the meetings of the Parliament's committees.

28. Deputy of the President of the Authority

Article 46

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

(2) The Vice President shall meet the requirements necessary for the appointment of the President of the Authority as laid down in paragraphs (1) and (2) of Article 40; he/she shall have five years of professional experience in the control of procedures concerning data protection or freedom of information.

(3) In regard to conflicts of interest regarding the Vice President the provisions laid down in Article 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.

Article 47

The provisions of Article 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 declaration of assets with the provision 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.

Article 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 civil service legal relationship.

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

Article 49

(1) The mandate of the Vice President of the Authority shall be terminated by the following:

a) resignation;

b) death;

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

d) establishment of a conflict of interest;

e) dismissal; or

f) removal from office.

(2) The Vice President of the Authority may at any time resign from his 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, following the notice

of the resignation or, failing this, on the day of the notice of 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 Article 41 within thirty days of his appointment or if, in the course of the exercise of his office, a conflict of interest arises, the President of the Authority shall decide on the conflict of interest.

(4) The President of the Authority shall dismiss the Vice President of the Authority if, for reasons not imputable to him, the Vice President of the Authority is not able to perform the duties deriving from his 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 civil servant at the Authority, and – even in the absence of the conditions laid down in paragraph (1) of Article 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, the Vice President of the Authority fails to perform the duties deriving from his mandate for more than ninety days or if he deliberately makes a false declaration on important data or facts in his 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 points a) or e) of paragraph (1), the Vice President of the Authority shall be entitled to an additional payment three times the amount of his monthly salary at the time of termination.

29. Staff of the Authority

Article 50

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

Article 51

(1) The President of the Authority may appoint inquirers, up to twenty per cent of the number of civil servants of the Authority, from among those civil servants of the Authority who have a 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 specialist exam in public administration or 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 civil servant shall be reinstated in the position they 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 VI

PROCEDURES OF THE AUTHORITY

30. Investigation of the Authority

Article 52

(1) Anyone is entitled to request an investigation from the Authority, on the grounds of violation of rights relating to the control of personal data, access to data of public interest or data public on grounds of public interest, or in the event of immediate threat of the above.

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

(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 reporting person if otherwise the investigation cannot be conducted. Upon request of the reporting person, the Authority is not allowed to disclose their identity even if, as a consequence, the investigation cannot be conducted. The Authority shall notify the person of this consequence.

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

Article 53

(1) With the exception of the cases specified in paragraph (2) and (3), The Authority is obliged to investigate the submission.

(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) there be pending legal proceedings in the case, or a legally binding decision was made earlier in the case;

b) the reporting person have requested that their anonymity be maintained in accordance with paragraph of Article 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 conduct an investigation, should there be pending legal proceedings in the case, or if a legally binding decision was made earlier in the case.

(5) The Authority shall terminate the investigation if

a) the submission should have been rejected without investigation pursuant to paragraphs (3) and (4); but the Authority only became aware of 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 reporting person of the dismissal of the submission without substantive investigation, the termination of the procedure and the justification for the dismissal or termination.

(7) The Authority shall refer submissions outside its competence – by notifying the reporting person – to the competent body if, on the basis of the data available, the competent body can be identified. If, on the basis of the report submitted outside its competence, the Authority establishes that legal proceedings may be initiated, the Authority shall notify the reporting person.

Article 54

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

a) inspect all documents controlled by the data controller under review and associated with the given case, or request copies of these;

b) be informed about the 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 data controller under review, as well as from any employee,

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 paragraph (1), the data controller under review, or other organisation or individual concerned shall be obliged to fulfil requests made by the Authority within the deadline set by the Authority. The deadline defined by the Authority shall not be less than fifteen days in cases defined in points d) and e) of paragraph (1).

(3) The person competent for providing information may refuse to provide information specified under points c) and d) of paragraph (1), should

a) the person concerned by the report constituting the object of the investigation of the Authority be an immediate relative or former spouse pursuant to the act on the general rules of administrative proceedings;

b) they accuse themselves or their immediate relative or former spouse as specified in the act on the general rules of administrative proceedings with committing a crime, in the question relating to it.

Article 55

(1) Within two days of the receipt of the submission, the Authority shall act as follows:

a) should the Authority deem that the submission is well founded, the Authority shall

aa) take measures defined under Article 56 and Article 57;

ab) close the investigation and launch a data protection procedure in accordance with Article 60, or

ac) close the investigation and launch a procedure for the supervision of classified data in accordance with Article 62;

b) close the investigation should it deem that the submission is unfounded.

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

Article 56

(1) Should the Authority establish the violation of rights relating to the control of personal data, access to data of public interest or data public on grounds of public interest, or the immediate threat of it, it shall call on the data controller to remedy it or eliminate the immediate threat.

(2) The data controller – in case of agreement – shall immediately take the necessary measures in the notification specified in paragraph (1) and shall notify the Authority of the measures taken, or – in case of disagreement – shall inform the Authority of their position in writing within thirty days of the receipt of the 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 body, notifying the data control body at the same time, should the notification issued in accordance with paragraph (1) have proved ineffective. Should the supervisory body of the data control body have not been notified in accordance with paragraph (1), the Authority may also directly make recommendations, if, in their view, these recommendations would effectively remedy the violation of rights or eliminate the immediate threat of it.

(4) The supervisory body shall notify the Authority in writing of their position in respect of the recommendation, as well as of the measures taken, within a period of thirty days following the receipt of the recommendation.

Article 57

Should, pursuant to the investigation, the Authority establish that the violation of rights or its immediate threat ensues from an unnecessary, ambiguous or inappropriate provision of legislation or regulatory instrument of public law, or the lack or deficient nature of the legal regulation of data control issues, the Authority may make recommendations to the body authorised to legislate or issue regulatory instruments of public law, as well as to the drafter of legislation to prevent the future occurrence of the violation of rights or its immediate threat. The Authority may recommend the amendment, repeal or drafting of legislation or the regulatory instrument of public law. The body contacted shall notify the Authority of their position, as well as of measures taken in accordance with the recommendation within a period of sixty days.

Article 58

(1) Should, pursuant to the notification or the recommendation issued in accordance with Article 56, the violation of rights not have been remedied or its immediate threat not have been eliminated, the Authority shall make a decision on further measures to be taken within a period of thirty days following the expiry of the deadline for notification specified in Article 56 (2), or Article 56 (4) if a recommendation was issued.

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

a) may launch a data protection procedure in accordance with Article 60;

b) may launch a procedure for the supervision of classified data in accordance with Article 62;

c) may launch legal proceedings in accordance with Article 64, or

d) may compile a report in accordance with Article 59.

(3) The Authority shall notify the reporting person of the outcome of measures taken in accordance with Article 56 and Article 57, as well as further measures taken in accordance with paragraph (2).

31. Report of the Authority

Article 59

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

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

(3) The report of the Authority is public. The president of the Authority is entitled to classify reports containing classified information, or repeatedly classify the report. 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) The report of the Authority on investigations regarding activities of bodies authorised to use intelligence instruments and methods shall not contain data from which it would be possible to deduce information regarding the confidential information collection activity of the body.

(5) The report of the Authority cannot be contested in court or before other authorities.

32. Data Protection Procedure of the Authority

Article 60

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

(2) Unless otherwise provided by this Act, the act on the general rules of administrative proceedings shall apply to the data protection procedure.

(3) The data protection procedure can only be launched ex officio, and shall not qualify as a procedure launched on request even if it was preceded by an investigation of the Authority based on a report. Should, however, an investigation of the Authority based on a report have preceded the data protection procedure, the reporting person 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 can be presumed and the unlawful control

a) concerns a wide range of persons;

b) concerns special data, or

c) can significantly harm interests or engenders the risk of damage.

(5) The deadline for administration in the data protection procedure is two months.

Article 61

(1) In the decision made in 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 or delivery of the personal data to other countries;

e) order the notification of the data subject, should the data controller have unlawfully refused it, and

f) impose a fine.

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

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

(4) To decide whether a fine should be imposed and to determine its amount, the Authority shall consider all circumstances of the case, in particular, the number of individuals affected by the violation of rights, its weight and repetition.

(5) The disputed data cannot be deleted or destroyed until the deadline for initiating judicial review had expired, or, in the case of initiating a review, until the final decision of the court.

33. Procedure for the Supervision of Classified Data

Article 62

(1) The Authority is authorised to launch a procedure for the supervision of classified data, if, pursuant to the investigation conducted based on the report made or otherwise, it can be presumed that national classified data 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 in the act on the protection of classified information.

(2) Unless otherwise provided by this act, the act on the general rules for administrative proceedings shall apply to the procedure for the supervision of classified data.

(3) The procedure for the supervision of classified data can only be launched ex officio, and shall not qualify as a procedure launched on request even if it was preceded by an investigation of the Authority based on a report. Should, however, an investigation of the Authority based on a report have preceded the procedure for the supervision of classified data, the reporting person must be notified of the launch and the closing of the procedure for the supervision of classified data.

Article 63

(1) Should the Authority establish in its decision that legislation applicable in connection with the classification of national classified information has been infringed, the Authority shall call on 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 of the Authority pursuant to paragraph (1) is unfounded, the classifier may request that it be reviewed by a court within a period of sixty days of the announcement of the decision. The execution of the decision shall be suspended by submitting the statement of claim. Should the classifier not turn to the court within a period of sixty days of the announcement of the decision, the classification of the national classified information becomes null and void in accordance with the decision on the sixty-first day following the announcement of the decision and its classification level or period of validity changes in accordance with the decision.

(3) Provisions of the code of civil procedure governing administrative litigation shall apply to the proceedings of the court, with the specification that the court shall immediately proceed with the case, in a closed session.

(4) The court shall confirm, amend or reverse the Authority’s decision, or instruct the Authority to launch a new procedure, if 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 undergone the highest level of national security screening specified in the act on national security services shall proceed in the case.

(7) Besides the judge, the plaintiff and the defendant, only persons undergone the highest level of national security screening specified in the act on national security services shall gain access to the classified information.

34. Litigation initiated by the Authority

Article 64

(1) Should the data controller fail to comply with the notification issued pursuant to Article 56 (1), the Authority may, due to the violation of rights related to 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 notification within a period of thirty days following the expiry of the deadline for providing information specified in paragraph of Article 56 (2).

(2) The litigation falls under the jurisdiction of the court specified in Article 31 (5).

(3) The data controller is obliged to prove that the data control complies with the provisions of relevant legislation.

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

(5) If requested, the court can disclose its judgment – by disclosing the ID data of the data controller – if it deems 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 by this Act.

35. Data Protection File

Article 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 subjects, which – with exceptions set out in paragraph (2) - contains:

a) the objective of the data control;

b) the legal grounds of the data control;

c) the scope of data subjects;

d) the description of the data concerning the data subjects;

e) the source of the data;

f) the duration of the control of the data;

g) the type of data transferred, its recipients and the legal grounds of transfer, including data transfers to third countries;

h) the name and address of the data controller and the data processor, place of the actual data control and data processing and the activity undertaken by the data processor in connection with the data control;

i) the type of the data processing technology applied;

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

(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 clients of financial organisations, public utility services, electronic telecommunications service providers - or who are clients of the data controller;

b) are carried out in accordance with the internal regulations of a church, 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 providing medical therapy, health preservation or enforcing 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, 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 provided 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 in 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 shall be public and available for consultation and taking notes to anyone.

Article 66

(1) The data controller shall request the Authority to register the control of the personal data in a file, with the exception of mandatory data control, prior to starting the data control. The data control cannot be started prior to registration in the file, with the exception of mandatory data control and the case specified in Article 68 (2).

(2) The data controller shall request the registration of mandatory data control in the file from the Authority within a period of twenty days following the entering into force of the legislation regulating mandatory 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 Article 65 (1) and (2).

Article 67

An administration service fee defined in the ministerial decree shall be paid for the registration of the data control in the data protection file, with the exception of mandatory data control.

Article 68

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

(2) With the exception of the case defined in paragraph (3), should the Authority fail to assess the request for registration within the deadline set, the data controller can start the data control in accordance with the content of the request submitted.

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

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

(5) The precondition for registration defined in paragraph (4) relates to

a) the control of national official, occupational and criminal data files;

b) data control concerning clients by 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 data 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 points b)-j) of Article 65 (1), the data controller shall submit a request for registration of change to the Authority within a period of eight days of the occurrence of changes. The rules defined in paragraphs (1), (3) and (5) shall apply in the case of the registration procedure of change with the exception that the request should only contain the data changed.

36. Data Protection Audit

Article 69

37. Initiating Criminal, Offence and Disciplinary Proceedings

Article 70

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

(2) The body defined in paragraph (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 thirty days and shall notify the Authority of its outcomes within a period of thirty days following its completion.

38. Data Control and Confidentiality

Article 71

(1) The Authority is authorised to control – to the extent and duration required for conducting the procedure – personal data during the procedure, as well as data classified by law as confidential information and confidential information related to the exercise of a 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 in its administrative proceedings.

(3) The Authority shall 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) In the procedure conducted in connection with the control of classified information, the vice president, civil servant holding a managerial position 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 formerly 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 became aware of in connection with the activities of the Authority during the course of their employment, as well as after it, in addition to all data, facts and circumstances the Authority is not obliged to disclose pursuant to the provisions of the relevant legislation.

(6) The obligation of individuals listed in paragraph (5) to safeguard information means that they shall not unlawfully disclose any data, fact or circumstance they became aware of during the course of performing their responsibilities; shall not use it or disclose it to third parties.

CHAPTER VII

FINAL PROVISIONS

Article 72

(1) The Government shall be authorised to establish in a decree

a) the detailed rules of the electronic disclosure of data of public interest;

b) the cost items and their highest level to be taken into account when determining the fee to be paid for making copies to satisfy requests for data of public interest, as well as the criteria of determining the large size of the document of which a copy is requested;

c) the special disclosure list,

d) the data content of the uniform public data search system and the central register, as well as the rules on data integration.

(2) Authorisation shall be provided to

a) the minister competent to determine in a decree a special disclosure list for bodies under their direction or supervision ;

b) the minister responsible for e-administration to define in a decree disclosure templates required for publishing data listed in special disclosure lists;

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 in a decree – by requesting the position of the Authority – the scope of data to be disclosed by national security agencies under their supervision.

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

Article 73

(1) This Act - with the exceptions defined in paragraphs (2) and (3) - shall enter into force following the day of its proclamation.

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

(3) Points g) and h) of Article 38 (4) and Article 69 shall enter into force on 1 January 2013.

Article 74

The Prime Minster shall propose a candidate for President of the Authority to the President of the Republic by 15 November 2011. The President of the Republic shall appoint the first President of the Authority with effect of 1 January 2012.

Article 75

(1) The Authority shall proceed in accordance with the provisions of this Act in pending cases based on submissions received by the data protection commissioner prior to 1 January 2012.

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

(3) The registration of data control under the scope of data protection registration pursuant to this Act for data controls started prior to 1 January 2012 but not registered in the data protection file until 1 January 2012 must be requested from the Authority until 30 June 2012 in accordance with the provisions of this Act, otherwise the data control cannot be continued after 30 June 2012. Data control activities defined under this article cannot be continued if, on the grounds of the request for registration submitted after 31 December 2011, the Authority have rejected registration.

Article 76

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

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

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

Article 78

Article 79

Article 80

Article 81

Article 82

Article 83

Article 84

Article 85

Article 86

Article 87

Article 88

Article 89

Annex 1 to Act CXII of 2011

GENERAL LIST OF DATA PUBLISHED

I. Organisational and Staff 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 performing public tasks	Immediately following modification	Previous state to be deleted
2.	Organisational structure of the body performing public tasks by indicating organisational units and the responsibilities of specific organisational units	Immediately following modification	Previous state to be deleted
3.	Name of the heads of the body performing public tasks; name of the heads of specific organisational units, their positions and contact details (telephone and fax number, email address)	Immediately following modification	Previous state to be deleted
4.	Name and contact details of the competent client service manager within the organisation (postal address, telephone and fax number, email address) and client service business hours	Immediately following modification	Previous state to be deleted
5.	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
6.	Name of other bodies under the	Immediately	By preserving the

	direction, supervision or control of the body performing public tasks, or subordinate to the latter, as well as their data as defined under Point 1	following modification	previous state in the archives for one year
7.	Name, seat and contact details (postal address, telephone and fax number, email address) of the business organisation under the partial or majority ownership of the body performing public tasks,; their scope of activities, name of the representative, ratio of shares held by the body performing public tasks	Immediately following modification	By preserving the previous state in the archives for one year
8.	Name, seat and contact details (postal address, telephone and fax number, email address) of the public foundation founded by the body performing public tasks; its statutes and members of its executive body.	Immediately following modification	By preserving the previous state in the archives for one year
9.	Name, seat and indication of the act establishing the budgetary organisation founded by the body performing public tasks, as well as the decision on the foundation, the statutes of the budgetary organisation, its head, website and operating license	Immediately following modification	By preserving the previous state in the archives for one year
10.	Name of newspapers founded by the body performing public tasks; name and address of its seat and publisher, the name of the editor-in-chief	Immediately following modification	By preserving the previous state in the archives for one year
11.	Date defined under point 1 of the supervisory body of the body performing public tasks, of the body authorised to consider	Immediately following modification	By preserving the previous state in the archives for one

	appeals against its administrative decisions, or the body supervising the lawful operation of the body performing public tasks		year

II. Data concerning activities, operations

	Data	Updated	Safeguarding
1.	Key legislation, instruments of public law, as well as the organisational and operational regulations or rules of procedure relevant to defining the responsibilities, scope of authority and basic activities of the body performing public tasks 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
2.	English and Hungarian versions of the document on the responsibilities and activities of the body performing public tasks in the case of bodies with a country-wide competence, as well as the regional state administration body of the Government with general competence.	Immediately following modification	Previous state to be deleted
3.	Responsibilities assumed by the local government on a voluntary basis	Quarterly	By preserving the previous state in the archives for one year
4.	Name of the body, by type of case and procedure, competent in state or local administration and other official matters; name of the body competent to act in the case of delegating the competence, its	Immediately following modification	Previous state to be deleted

	scope of regional competence; the documents, papers required and the procedural duties (administration service fees); to be paid for the administration, the fundamental rules of procedure, mode of submission of the application initiating the procedure (time and place); client service business hours, deadline for administration (deadline for processing and lodging appeals); information regarding procedures and downloadable forms used for processing cases; access to available electronic programmes; making appointments, list of legislation related to the type of procedures, information on rights of the client and the obligations of the client		
5.	Name and content of public services provided by the body performing public tasks 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
6.	Databases maintained by the body performing public tasks, as well as the descriptive data of files (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 of files to be registered in the data protection file as specified in this Act; type of data collected and processed by the body performing public tasks within its scope of basic activities, their mode of access and fee charged for	Immediately following modification	By preserving the previous state in the archives for one year

	making copies		
7.	Title, theme, mode of access, free availability of the publications of the body performing public tasks, or the fee charged to access these.	Quarterly	By preserving the previous state in the archives for one year
8.	Rules of procedure for preparing the decisions of corporate bodies; mode of participation (commenting) by nationals; rules of procedure; the place and time of the sessions, whether they are open to the public, the decisions made, the minutes and summaries; data concerning the votes if this is not restricted by relevant legislation.	Immediately following modification	By preserving the previous state in the archives for one year
9.	Draft legislation and related documents to be published by law; submissions to the open session of local government representative bodies from the 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
10.	Notices and announcements published by the body performing public tasks	Continuously	By preserving them in the archives for at least one year
11.	Technical description of tenders by the body performing public tasks, their results and their justification.	Continuously	By preserving the previous state in the archives for one year
12.	The public findings of investigations, reviews carried out at the body performing public tasks in connection with its basic activities	Immediately after obtaining the findings of the investigation report	By preserving the previous state in the archives for one year

13.	Rules of procedure of requests 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 rights in units if applicable.	Quarterly	Previous state to be deleted
14.	Results and changes to statistical data collected in relation to the activities of the body performing public tasks	Quarterly	By preserving the previous state in the archives for one year
15.	Data on the mandatory data provision for statistical purposes in relation to data of public interest concerning the given body	Quarterly	By preserving the previous state in the archives for one year
16.	List of contracts aimed at using data of public interest of where the body performing public tasks is a contracting party.	Quarterly	By preserving the previous state in the archives for one year
17.	General terms of contract concerning the use of data of public interest controlled by the body performing public tasks	Immediately following modification	By preserving the previous state in the archives for one year
18.	Special disclosure list concerning the body performing public tasks	Immediately following modification	Previous state to be deleted

III. Financial Data

	Data	Updating	Safeguarding
1.	Annual budget of the body	Immediately	For a period of ten

	performing public tasks, its report or its report on the annual budget pursuant to the Accountancy Act.	following modification	years following the publication
2.	Aggregated data regarding the staff size and remuneration of employees at the body performing public tasks; total amount of remuneration paid to executive staff members and executive officers, their salaries, regular benefits and reimbursements; total type and rate of benefits offered to other employees.	Quarterly	For a period specified under separate legislation; however, by keeping it in the archives for at least one year
3.	Data concerning the name of the beneficiary of the budgetary subventions granted by the body performing public tasks under the Act on Public Finances, the objective of the subvention, its amount and the place of implementation of the aid scheme, except if the budgetary aid is withdrawn before the publication or the beneficiary renounce it.	Until the 60th day following the decision	For a period of five years following the publication
4.	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 of which amounts to at least HUF five million; 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, as well as the changes of these data, with the	Until the 60th day following the decision	For a period of five years following the publication

	exception of data relating to procurements directly linked to national defence interest and classified data. The value of the contract shall mean the consideration determined for the object of the contract less VAT; in the case of free transactions, it is the market value or – if higher – the book value that has to be taken into account. Concerning periodic contracts with duration of more than one year, the value shall be calculated on the basis of the amount of the consideration calculated for one year. The values of various contracts with the same object, concluded with the same party within the same budgetary year shall be calculated aggregately.		
5.	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
6.	Payments made by the body performing public tasks exceeding HUF five million in connection with the provision of non-statutory responsibilities (in particular, payments made for funding associations, professional and interest representation bodies of their employees, organisations of their employees and clients engaging in educational, cultural, social and sports activities, payments in connection with responsibilities undertaken by foundations)	Quarterly	For the period specified under separate legislation; however, by keeping it in the archives for at least one year

7.	Description of projects implemented with the support of the European Union and the related contracts	Quarterly	By keeping it in the archives for at least one year
8.	Public procurement information (annual plan, summary of the assessment of offers submitted and the contracts concluded)	Quarterly	By keeping it in the archives for at least one year