Act CXII of 2011
on the right to informational self-determination and on the freedom of information

The National Assembly, in order to ensure the right to informational self-determination and the freedom of information, for the purpose of implementing the Fundamental Law, and on the basis of Article VI of the Fundamental Law, adopts the following Act on the fundamental rules applicable to the protection of personal data and the enforcement of the right to access data of public interest and data accessible on public interest grounds, as well as on the authority empowered to monitor compliance with these rules:

CHAPTER I

GENERAL PROVISIONS

1. Purpose of the Act

Section 1 The purpose of this Act is to lay down, in the areas falling within its scope, the fundamental rules for data processing in order to ensure that natural persons' right to privacy is respected by controllers, and to achieve the transparency of public affairs through the enforcement of the right to access and disseminate data of public interest and data accessible on public interest grounds.

2. Scope of the Act

Section 2 (1) This Act shall apply, with regard to personal data in accordance with the provisions laid down in paragraphs (2) to (6), to all data processing activities that are related to personal data, as well as to data of public interest and data accessible on public interest grounds.

(2) Regulation (EU) 2016/679 of the European Parliament and of the Council (hereinafter "General Data Protection Regulation") shall apply to the processing of personal data falling within the scope of the General Data Protection Regulation, with the additional rules laid down in Chapters III to V and VI/A, as well as in section 3 points 3, 4, 6, 11, 12, 13, 16, 17, 21, 23 to 24, in section 4 (5), section 5 (3) to (5), (7) and (8), section 13 (2), section 23, section 25, section 25/G (3), (4) and (6), section 25/H (2), section 25/M (2), section 25/N, section 51/A (1), sections 52 to 54, section 55 (1) to (2), sections 56 to 60, section 60/A (1) to (3) and (6), section 61 (1) *a)* and *c)*, section 61 (2) and (3), (4) *b)* and (6) to (10), sections 62 to 71, section 72, section 75 (1) to (5), section 75/A and Annex 1.

(3) This Act shall apply to the processing of personal data for law enforcement, national security and national defence purposes.

(4) The following provisions shall apply to the processing of personal data not subject to paragraphs (2) and (3):

a) Article 4, Chapters II to VI and Chapters VIII to IX of the General Data Protection Regulation, as well as

b) Chapters III to V and VI/A, as well as in section 3 points 3, 4, 6, 11, 12, 13, 16, 17, 21, 23 to 24, in section 4 (5), section 5 (3) to (5), (7) and (8), section 13 (2), section 23, section 25, section 25/G (3), (4) and (6), section 25/H (2), section 25/M (2), section 25/N, section 51/A (1), sections 52 to 54, section 55 (1) to (2), sections 56 to 60, section 60/A (1) to (3) and (6), section 61 (1) *a)* and *c)*, section 61 (2) and (3), (4) *b)* and (6) to (10), sections 62 to 71, section 72, section 75 (1) to (5) and Annex 1 of this Act.

(5) Unless otherwise provided by an Act or a binding legal act of the European Union, the provisions of this Act laid down in paragraph (2), as well as other provisions prescribed in an Act on the protection of personal data and on the conditions of processing personal data, shall apply to the processing of personal data under the General Data Protection Regulation if

a) the controller's main establishment specified in Article 4 point 16 of the General Data Protection Regulation or its single establishment within the European Union is in Hungary, or

b) the controller's main establishment specified in Article 4 point 16 of the General Data Protection Regulation or its single establishment within the European Union is not in Hungary, but the processing operation performed by the controller or by the processor acting on behalf of, or instructed by, the controller is related to

ba) offering goods or services to data subjects in Hungary, irrespective of whether it requires payment by the data subject; or

bb) monitoring the data subject's behaviour in the territory of Hungary.

(6) The provisions set out in this Act shall not be applied to natural persons processing data exclusively for their own personal purposes.

(7) With respect to the further use of public sector information, an Act may provide rules derogating from those of this Act in connection with the methods and conditions for the provision of data, the fee payable for it and the legal remedies.

3. Interpretative provisions

Section 3 For the purposes of this Act:

1. *data subject* means a natural person identified or identifiable based on any information;

1a. *identifiable natural person* means a natural person who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, identification number, location data, online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

2. *personal data* means any data relating to the data subject;

3. *sensitive data* means all data falling in the special categories of personal data that are personal data revealing racial or ethnic origin, political opinion, religious belief or worldview, or trade union membership, as well as genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation;

3a. *genetic data* means personal data relating to the inherited or acquired genetic characteristics of a natural person that give unique information about the physiology or health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

3b. *biometric data* means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

3c. *data concerning health* means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his health status;

4. *criminal personal data* means personal data related to the data subject and to a criminal record, generated by organs authorised to conduct criminal proceedings or to detect criminal offences, or by the prison service during or prior to criminal proceedings, in connection with a criminal offence or criminal proceedings;

5. *data of public interest* means information or data other than personal data, registered through any method or in any form, pertaining to the activities of and processed by the organ or person performing state or local government duties and other public duties defined by law, or generated in the course of performing their public duties, irrespective of the method or form in which it is recorded and regardless of its singular or collective nature; in particular, data concerning material competence, territorial competence, organisational structure, professional activities and the evaluation of their performance, the type of data held and the laws governing its operation, as well as data concerning financial management and concluded contracts;

6. *data accessible on public interest grounds* means any data, other than data of public interest, the disclosure, availability or accessibility of which is prescribed by an Act for the benefit of the general public;

7. *consent* means any freely given, specific, informed and unambiguous indication of the data subject's wishes, by which he, by a statement or a clear affirmative action, signifies agreement to the processing of personal data relating to him;

8.

9. *controller* means the natural or legal person, or organisation having no legal personality, which, within the framework laid down in an Act or in a binding legal act of the European Union, alone or jointly with others, determines the purposes of data processing, makes decisions concerning data processing (including the means used) and implements such decisions or has them implemented by a processor;

9a. *joint controller* means the controller which, within the framework laid down in an Act or in a binding legal act of the European Union, jointly with one or more other controllers, determines the purposes and means of data processing, and, jointly with one or more other controllers, makes decisions concerning data processing (including the means used) and implements such decisions or has them implemented by a processor;

10. *processing* means any operation or set of operations that is performed on data, regardless of the procedure applied; in particular collecting, recording, registering, organising, storing, modifying, using, retrieving, transferring, disclosing, synchronising or connecting, blocking, erasing and destroying the data, as well as preventing their further use; taking photos and making audio or visual recordings, as well as registering physical characteristics suitable for personal identification (such as fingerprints or palm prints, DNA samples and iris scans);

10a. *processing for law enforcement purposes* means processing by an organ or person (hereinafter jointly “organ carrying out processing for law enforcement purposes”) which is, within its or his functions and powers laid down by law, engaged in an activity aimed at preventing or eliminating threats to public order or public safety, preventing and detecting criminal offences, carrying out, or contributing to, criminal proceedings and preventing and detecting infractions, as well as carrying out, or contributing to, infraction proceedings, and implementing the legal consequences imposed in criminal proceedings or infraction proceedings, within the limits and for the purpose of this activity, including the processing of personal data connected to this activity for archival, scientific, statistical or historical purposes (hereinafter jointly “law enforcement purpose”);

10b. *processing for national security purposes* means processing by the national security services, within their functions and powers laid down by law, as well as processing under the Act on national security services by the counter-terrorism organ of the police, within its functions and powers laid down by law;

10c. *processing for national defence purposes* means processing under the Act on data processing by the defence forces and the Act on national defence and the Hungarian Defence Forces, as well as the measures that can be introduced during a special legal order, and the Act on the registration of foreign armed forces staying in the territory of the Republic of Hungary for service purposes and of the international headquarters and their staff established in the territory of the Republic of Hungary, as well as on certain provisions concerning their status;

11. *data transfer* means providing access to the data for a designated third party;

11a. *onward data transfer* means the transfer of personal data, by way of transfer to a controller or processor engaged in data processing in any third country or in the framework of an international organisation, to a controller or processor engaged in data processing in any other third country or in the framework of an international organisation;

11b. *international organisation* means an organisation, and its subordinate bodies, governed by public international law, or any other body that is set up by, or on the basis of, an agreement between two or more states;

12. *disclosure* means making the data accessible to anyone;

13. *data erasure* means making the data unrecognisable in such a way that its restoration is no longer possible;

14.

15. *restriction of processing* means the blocking of stored data by marking them with the aim of limiting their processing in the future;

16. *data destruction* means the complete physical destruction of the data medium that contains the data;

17. *technical processing* means the totality of data processing operations performed by the processor acting on behalf of, or instructed by, the controller;

18. *processor* means a natural or legal person, or an organisation not having legal personality which, within the framework and under the conditions laid down in an Act or in a binding legal act of the European Union, acting according to a mandate or instructions given by the controller, processes personal data;

19. *data source* means the organ performing public duties, which generated the data of public interest that is to be published through electronic means, or during the operations of which such data was generated;

20. *data publisher* means the organ performing public duties which, if the data source itself does not publish the data, uploads the data sent to it by the data source to a website;

21. *dataset* means all data processed in a single registry;

22. *third party* means a natural or legal person, or an organisation having no legal personality, other than the data subject, controller, processor and the persons who, under the direct authority of the controller or processor, carry out operations aimed at processing personal data;

23. *EEA State* means any Member State of the European Union and any State 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 State Parties to the Agreement on the European Economic Area on the basis of an international agreement concluded between the European Union and its member states and the state which is not party to the Agreement on the European Economic Area;

24. *third country* means any state that is not an EEA State;

25.

26. *personal data breach* means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised transfer or disclosure of, or unauthorised access to, personal data transferred, stored or otherwise processed;

27. *profiling* means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a data subject, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

28. *recipient* means a natural or legal person, or an organisation having no legal personality, for which the controller or the processor provides access to the personal data;

29. *pseudonymisation* means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

CHAPTER II

RREQUIREMENTS FOR THE PROTECTION OF PERSONAL DATA

4. Principles relating to processing of personal data

Section 4 (1) Personal data shall be processed only for clearly specified and legitimate purposes, in order to exercise certain rights and fulfil obligations. The purpose of processing shall be met in all stages of processing; data shall be collected and processed fairly and lawfully.

(2) Only personal data that is essential and suitable for achieving the purpose of processing may be processed. Personal data may be processed only to the extent and for the period of time necessary to achieve its purpose.

(3) In the course of processing, data shall retain their personal character as long as their connection with the data subject can be restored. The connection with the data subject shall, in particular, be considered restorable if the controller is in possession of the technical means necessary for the restoration.

(4) The accuracy and completeness, and, if deemed necessary with respect to the purpose of the processing, the up-to-date status of the data shall be ensured throughout the processing; the identification of the data subject shall be possible for no longer than necessary for the purpose of the processing.

(4a) During processing, appropriate technical or organisational measures shall be applied to ensure the appropriate security of personal data, including, in particular, protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

(5) The processing of personal data shall be deemed fair and lawful if, for the purpose of ensuring the data subject’s right to the freedom of expression, the person wishing to find out the opinion of the data subject visits him at his domicile or place of residence, provided that the data subject’s personal data are processed in compliance with this Act and contacting him is not intended for business purposes. Personal visits are not permitted on public holidays under the Labour Code.

5. Legal basis and general conditions of processing

Section 5 (1) Personal data may be processed if

a) it is prescribed in an Act or, based on the authorisation of an Act, within the limits set forth therein and for data other than sensitive and criminal personal data, in a local government decree for purposes in the public interest,

b) provided that the conditions under point *a)* are not fulfilled, it is inevitably necessary for the performance of the controller's tasks as provided for by an Act, and the data subject has given explicit consent to the processing of personal data,

c) provided that the conditions under point *a)* are not fulfilled, it is necessary for, and proportionate to, the protection of the vital interests of the data subject or of another person, or the elimination or the prevention of a direct threat to the life, physical integrity or property of persons, or

d) provided that the conditions under point *a)* are not fulfilled, the data subject explicitly disclosed the personal data, and it is necessary for, and proportionate to, the realisation of the purpose of processing.

(2) Sensitive data may be processed under the following circumstances:

a) in accordance with the provisions of paragraph (1) *c)* to *d)*, or

b) if processing is inevitably necessary for, and proportionate to, the implementation of an international agreement promulgated by an Act, or if prescribed by an Act in connection with the enforcement of the fundamental rights ensured by the Fundamental Law or for reasons of national security, the prevention, detection and prosecution of criminal offences or national defence.

(3) For processing according to paragraph (1) *a)*, paragraph (2) *b)* and according to Article 6 (1) (c) and (e) of the General Data Protection Regulation (hereinafter "mandatory processing"), the type of data, the purpose and conditions of processing, the access to such data, the controller and the duration of the processing or the regular examination of its necessity shall be specified by the Act or local government decree ordering mandatory processing.

(4) Only state or local government organs shall be permitted to process criminal personal data for the purposes of performing the duties of the State related to the prevention, detection and prosecution of criminal offences, as well as its administrative and judicial tasks, and to manage registers containing data pertaining to infraction, civil contentious and non-contentious as well as administrative contentious and non-contentious procedures

(5) Unless an Act, a local government decree or a binding legal act of the European Union provides for the period of mandatory processing or the periodic review of its necessity, the controller shall review in every third year from the date of commencing the processing whether the processing of the personal data by the controller or by the processor acting on behalf of, or instructed by, the controller is necessary for the realisation of the purpose of processing. The controller shall document the circumstances and the results of the review, and shall retain this documentation for ten years following the review and it shall make the documentation available to the National Authority for Data Protection and Freedom of Information (hereinafter "Authority") at its request.

(6) For processing sensitive data, the controller, or the processor acting on behalf of or instructed by the controller, shall implement appropriate technical and organisational measures for ensuring that during the processing operations only the persons for whom this is inevitably necessary for the performance of their duties connected to the processing operation shall have access to the sensitive data.

(7) Unless otherwise provided by an Act, an international agreement or a binding legal act of the European Union, the rules of processing sensitive data shall apply to the processing of criminal personal data.

(8) An organ or person engaged in scientific research may disclose personal data provided that it is necessary for the presentation of the results of scientific research on historical events.

Section 6 A decision based solely on automated processing, including profiling, which produces negative effects concerning the person or the legitimate interests of the data subject, or produces legal effects significantly affecting him shall only be made if an explicit authorisation is provided in an Act or in a binding legal act of the European Union and provided that

a) it does not violate the requirement of equal treatment,

b) the controller or the processor acting on behalf of, or instructed by, the controller

ba) informs the data subject, upon his request, of the method and the criteria applied during the decision-making mechanism,

bb) reviews, upon the data subject's request, the result of the decision by applying human intervention, and

c) unless otherwise provided by an Act or a binding legal act of the European Union, no sensitive data are used in the decision making.

Section 7 (1) With regard to processing for law enforcement purposes, the controller or the processor acting on behalf of, or instructed by, the controller shall organise, provided that it does not entail disproportionate difficulties or costs, the personal data it processes by making a distinction between the personal data of data subjects

a) with regard to whom there are serious grounds for believing that they have committed a criminal offence or infraction or are about to commit a criminal offence,

b) whose liability for committing a criminal offence or infraction has been established with final and binding effect,

c) who were the victims of a criminal offence or of an infraction and persons with regard to whom there are serious grounds for believing that they could be victims of a criminal offence or of an infraction, or

d) who, in addition to the persons specified in points *a)* to *c),* may be linked to a criminal offence or infraction or its perpetrators, in particular those who may be heard as witnesses in criminal proceedings, persons who can provide information on the criminal offence or infraction, or persons in contact with or related to one of the persons referred to in points *a)* and *b)*.

(2) With regard to processing for law enforcement purposes, the controller or the processor acting on behalf of, or instructed by, the controller shall make a clear distinction, provided that it does not entail disproportionate difficulties or costs, between the facts and subjective assessments related to the data subject.

6. Conditions of data transfer

Section 8 (1) Prior to the transfer of data, the controller or the processor acting on behalf of, or instructed by, the controller shall assess the degree of accuracy, completeness and up-to-date status of the personal data to be transferred.

(2) If the controller or the processor acting on behalf of, or instructed by, the controller establishes as the result of the assessment specified in paragraph (1) that the data to be transferred are inaccurate, incomplete or no longer up to date, such data shall only be transferred if

a) it is absolutely necessary for the realisation of the purpose of transfer, and

b) notification is provided to the recipient upon the transfer of data of the information available on the degree of accuracy, completeness and up-to-date status of the data.

(3) If, after the transfer, the controller or the processor acting on behalf of, or instructed by, the controller becomes aware that the conditions of data transfer laid down in an Act, an international agreement or in a binding legal act of the European Union have not been fulfilled, it shall notify the recipient without delay.

Section 9 (1) If the controller or processor receives personal data in a way that, on the basis of an Act, an international agreement or a binding legal act of the European Union, the transferring controller or processor indicates to the recipient at the time of the transfer

a) the possible purposes of processing,

b) the possible duration of processing,

c) the possible recipients of the data transfer,

d) the limitation of the data subject's rights ensured by this Act, or

e) other conditions of processing,

(hereinafter the points *a)* to *e)* jointly "processing conditions"), the controller or processor recipient of such personal data (hereinafter "data recipient") shall process the personal data to the extent and using methods in accordance with the processing conditions, and shall ensure the data subject's rights in accordance with the processing conditions.

(2) With the prior consent of the transferring controller, the data recipient shall be allowed to process the personal data and ensure the data subject's rights irrespective of the processing conditions.

(3) If, on the basis of the provisions of an Act, an international agreement or a binding legal act of the European Union, the controller or the processor processes personal data under the obligation to apply processing conditions, it shall indicate the processing conditions and the legal obligation to apply them to the recipient at the time of the transfer.

(4) If the controller falling within the scope of this Act is entitled to give prior consent under paragraph (2) or section 10 (2) *c) ca)*, it shall be allowed to give this prior consent if, considering the circumstances of transfer, including the necessity and purpose of the transfer, it is not contrary to any legal provision applicable to legal entities subject to Hungary's jurisdiction, and especially if for the recipient of the transfer, including onward transfers, the adequate level of the protection of personal data can be presumed under the provisions of section 10 (4) *a)* to *c)*.

(5) The data recipient shall, upon request, inform the transferring controller of the use of the personal data received.

Section 10 (1) The controller or the processor acting on behalf of, or instructed by, the controller falling under the scope of this Act may transfer, including by way of onward data transfer, personal data to a controller or processor engaged in processing in a third country or in the framework of an international organisation (hereinafter jointly "international data transfer") if

a) the data subject has given explicit consent to the international data transfer, or

b) the international data transfer is necessary for the purpose of processing, and

ba) the conditions of processing laid down in section 5 are fulfilled in the course of the international transfer, and

bb) the adequate level of protection of the personal data transferred is provided by the controller or processor engaged in processing in the third country or in the framework of an international organisation, or

c) the international data transfer is necessary in the exceptional cases specified in section 11.

(2) With regard to processing for law enforcement purposes, international data transfer may only take place if, in addition to fulfilling the conditions laid down in paragraph (1),

a) it is necessary for law enforcement purposes,

b) its recipient is

ba) an organ carrying out processing for law enforcement purposes, or

bb) an organ not carrying out processing for law enforcement purposes and the conditions laid down in section 11 (3) are fulfilled, and

c) in the case of receiving personal data involved in international data transfer from the controller of any EEA State,

ca) the controller of the EEA State or another organ or person acting on behalf of that controller has given prior consent to the international data transfer of the personal data concerned, or

cb) with the exception of onward data transfer, international data transfer is necessary for the prevention of a serious and direct threat to the fundamental interests of Hungary or any EEA State, or to the public security of these states or of a third country, and prior consent under subsection *ca)* cannot be obtained before the international data transfer without harming these interests.

(3) The controller shall notify without delay the organ or person entitled to give prior consent according to paragraph (2) *c) ca)* after an international data transfer specified in paragraph (2) *c) cb)* has taken place.

(4) The adequate level of protection of personal data shall be presumed, in the absence of proof to the contrary, if

a) it is established in a binding legal act of the European Union,

b) in the absence of, or in the event of suspending the application of, a legal act under point *a),* the international agreement containing the regulations to guarantee the enforcement of the data subjects' rights laid down in section 14, section 22 and section 23 shall be applied between Hungary and the third country or international organisation the jurisdiction of which is applicable to the recipient of international data transfer, or

c) in the absence of, or in the event of suspending the application of a legal act under points *a)* to *b),* the controller assesses all circumstances of transferring the personal data and establishes that appropriate safeguards exist concerning the adequate level of protection of personal data.

Section 11 (1) If the adequate level of protection of personal data cannot be presumed according to section 10 (4) *a)* to *c),* in the absence of the data subject's explicit consent, the international data transfer may only be carried out if it is necessary

a) for the purpose of protecting the vital interests of the data subject or another person,

b) for the purpose of eliminating a direct and serious threat to the public security of an EEA State or a third country,

c) in the interest of carrying out efficient and effective inquiries or procedures by the controller in specific individual cases and provided that it does not entail the disproportionate restriction of the data subject's fundamental rights, or

d) for the establishment, exercise or defence of legal claims of the data subject or of another person in specific individual cases, and provided that it does not entail the disproportionate restriction of the data subject's fundamental rights.

(2) With regard to processing for law enforcement purposes, if the recipient of the international data transfer is an organ carrying out processing for law enforcement purposes and the adequate level of protection of personal data cannot be presumed according to section 10 (4) *a)* to *c),* in the absence of the data subject's explicit consent, the international data transfer may only be carried out if it is necessary

a) for a purpose specified in paragraph (1) *a)* and *b)*,

b) for the purpose of enforcing the data subject's lawful interests,

c) for a purpose of law enforcement in specific, individual cases and provided that it does not entail the disproportionate restriction of the data subject's fundamental rights, or

d) for the establishment, exercise or defence of legal claims connected to a law enforcement purpose in specific individual cases and provided that it does not entail the disproportionate restriction of the data subject's fundamental rights.

(3) With regard to processing for law enforcement purposes, if the recipient of the international data transfer is not an organ carrying out processing for law enforcement purposes, in the absence of the data subject's explicit consent, the international data transfer may only be carried out in a specific individual case if

a) it is strictly necessary for the purpose of law enforcement within the tasks and powers of the controller carrying out the international data transfer,

b) it does not entail the disproportionate restriction of the data subject's fundamental rights,

c) the purpose of international data transfer cannot be achieved effectively by way of international data transfer to an organ carrying out processing for law enforcement purposes,

d) the controller carrying out the international data transfer shall notify without delay the organ carrying out processing for law enforcement purposes in the third country or in the framework of an international organisation having jurisdiction with regard to the international data transfer of the international data transfer, unless such notification prevents the purpose of the international data transfer from being achieved effectively, and

e) the controller carrying out the international data transfer notifies the recipient of the potential purpose of processing the transferred data.

Section 12 (1) If the controller or the processor carries out the international data transfer

a) on the basis of the presumption under section 10 (4) *c)*, or

b) to a recipient that is not an organ carrying out processing for law enforcement purposes with regard to processing for law enforcement purposes,

the controller shall, following the first occasion of international data transfer for the same purpose to the same recipient, notify the Authority without delay of the purpose of the international data transfer, the recipient and the scope of the transferred data and, in the case laid down in point *a)*, the regularity of the international data transfer.

(2) If the controller or the processor carries out the international data transfer

a) on the basis of the presumption under section 10 (4) *c)*, or

b) with regard to processing for law enforcement purposes

ba) to an organ carrying out processing for law enforcement purposes according to section 11 (2), or

bb) to a recipient which is not an organ carrying out processing for law enforcement purposes,

the controller shall document the circumstances of the international data transfer, in particular the data specified in paragraph (1), as well as the time of the international data transfer, the personal data transferred and, in the case specified in point *a)*, the description of the safeguards assessed and appropriately identified by the controller, maintain this documentation for the period specified in section 25/F (4) and make it available to the Authority on request.

Section 13 (1) Transfer to EEA States, as well as to the agencies, offices and bodies established according to Title V Chapter 4 and 5 of the Treaty on the Functioning of the European Union, shall be regarded as transfer within the territory of Hungary.

(2) For the purposes, under the conditions and in the scope of data laid down in Article 96 of the General Data Protection Regulation and on the basis of the international agreements specified in Article 61 of the Directive (EU) 2016/680, until the amendment, annulment, termination or the suspension of the application of the foregoing, international data transfers may also be carried out in the absence of the conditions laid down in this Act.

CHAPTER II/A

RIGHTS OF THE DATA SUBJECT

7. Entitlements of the data subject

Section 14 With regard to the personal data of the data subject processed by the controller or the processor acting on behalf of, or instructed by, the controller, according to the conditions laid down in this Act, the data subject shall be entitled to

a) receive information, prior to the start of processing, on the facts connected to the processing (hereinafter "right to prior information"),

b) have his personal data and the information related to their processing provided by the controller on his request (hereinafter "right to access"),

c) have his personal data rectified or completed by the controller on his request and in further cases specified in this Chapter (hereinafter "right to rectification"),

d) have the processing of his personal data restricted by the controller on his request and in further cases specified in this Chapter (hereinafter "right to the restriction of processing"),

e) have his personal data erased by the controller on request and in further cases specified in this Chapter (hereinafter "right to erasure").

8. Securing the enforcement of the data subject's rights

Section 15 (1) For the purpose of facilitating the enforcement of the data subject's rights, the controller shall implement appropriate technical and organisational measures, in particular

a) providing, in the cases specified in this Act, the data subject with any notification or information in easily accessible and legible form, with concise, clear and plain content, and

b) assessing, within the shortest possible time from its submission, but not later than within twenty-five days, the request submitted by the data subject for the purpose of the enforcement of his rights, and it shall notify the data subject of the decision in writing or in electronic form if the request has been submitted in electronic form.

(2) With the exception specified in paragraph (3), the controller shall perform its duties laid down in this Act in connection with the enforcement of the rights specified in section 14 free of charge.

(3) If

a) the data subject submits, in the current year, a repeated request to enforce his rights specified in section 14 *b)* to *e)*, and

b) on the basis of this request, the controller lawfully refrains from rectifying, erasing or restricting the processing of the data subject's personal data processed by the controller or the processor acting on behalf of, or instructed by, the controller,

the controller may claim from the data subject the reimbursement of its direct costs incurred in relation to the repeated and unfounded enforcement of the data subject's rights according to the provisions in points *a)* and *b)*.

(4) If there are reasons to assume that the person submitting a request for the enforcement of the rights under section 14 points *b)* to *e)* is not identical to the data subject, the controller shall fulfil the request after verifying the identity of the person submitting the request.

Section 16 (1) For the purpose of enforcing the right to prior information, prior to the start of the processing operations performed by the controller or the processor acting on behalf of, or instructed by, the controller, or at the latest immediately upon the start of the first processing operation, the controller shall provide the data subject with information concerning

a) the name and the contact details of the controller and, if any of the processing operations is performed by a processor, those of the processor,

b) the name and the contact details of the data protection officer,

c) the purpose of the planned processing, and

d) the rights of the data subject under this Act, as well as the method of their enforcement.

(2) Simultaneously with, and the same way as regulated in the provisions under paragraph (1), or addressed to the data subject, the controller shall provide the data subject with information concerning

a) the legal basis of processing,

b) the period of retention of the processed personal data, as well as the criteria for determining this period,

c) in the event of the transfer or planned transfer of the processed personal data, the scope of the recipients of the data transfer, including recipients in third countries and international organisations,

d) the source of collecting the processed personal data and

e) any further material fact related to the circumstances of processing.

(3) Proportionately to the desired objective, the controller may delay the performance of providing the information under paragraph (2), it may restrict the content of the information or it may dispense with providing the information, if this measure is indispensable for ensuring

a) the efficient and effective conduct of the inquiries, in particular criminal proceedings, carried out by or with the participation of the controller,

b) the efficient and effective prevention and detection of criminal offences,

c) the execution of penalties and measures applied against the perpetrators of criminal offences,

d) the efficient and effective protection of public security,

e) the efficient and effective protection of the state's external and internal security, in particular national defence and national security or

f) the protection of the fundamental rights of third parties.

Section 17 (1) For the purpose of the enforcement of the right to access, the controller shall, upon request, inform the data subject whether his data are processed by the controller itself or by the processor acting on behalf of, or instructed by, the controller.

(2) If the data subject's personal data are processed by the controller or by the processor acting on behalf of, or instructed by, the controller, the controller shall, in addition to the provisions laid down in paragraph (1), provide the data subject with his personal data processed by the controller or by the processor acting on behalf of, or instructed by, the controller, as well as with information concerning

a) the source of the personal data processed,

b) the purpose and the legal basis of processing,

c) the scope of the personal data processed,

d) in the event of the transfer of the personal data processed, the scope of the recipients of the data transfer, including recipients in third countries and international organisations,

e) the period of retention of the personal data processed, as well as the criteria for determining this period,

f) the rights to which the data subject is entitled under this Act, as well as the method of enforcing them,

g) the existence of profiling when it is applied and

h) the circumstances of any personal data breaches that occurred in the context of processing the data subject's personal data, as well as their effects and the measures taken to address them.

(3) The controller may restrict or reject, proportionately to the desired objective, the enforcement of the data subject's right to access if this measure is absolutely necessary for securing an interest specified in section 16 (3) *a)* to *f)*.

(4) In the event of the application of a measure under paragraph (3), the controller shall notify the data subject in writing without delay of

a) the existence of restricting or rejecting access, as well as of its legal and factual reasons, if providing the data subject with such information does not impair the enforcement of an interest specified in section 16 (3) *a)* to *f)*,

b) the rights that the data subject is entitled to under this Act, as well as the method of enforcing them, in particular on the data subject's right to exercise the right to access through the Authority.

Section 18 (1) For the purpose of the enforcement of the right to rectification, if the personal data processed by the controller or by the processor acting on behalf of, or instructed by, the controller are inaccurate, incorrect or incomplete, the controller shall, in particular upon the data subject's request, further specify or rectify them without delay, or it shall supplement them with further personal data provided by the data subject or with a declaration attached by the data subject to the personal data processed, provided that it is compatible with the purpose of processing (hereinafter jointly "rectification").

(2) The controller shall be exempted from the obligation specified in paragraph (1) if

a) the accurate, correct or complete personal data are neither available nor provided by the data subject, or

b) the authenticity of the personal data provided by the data subject cannot be verified beyond doubt.

(3) If, according to the provisions of paragraph (1), the controller rectifies the personal data processed by the controller or by the processor acting on behalf of, or instructed by, the controller, it shall notify the controller to whom it has transferred the personal data affected by the rectification on the existence of rectification, as well as on the rectified personal data.

Section 19 (1) For the purpose of enforcing the right to the restriction of processing, the controller shall restrict processing to the processing operations specified in paragraph (2) if

a) the accuracy, the correctness or the completeness of the personal data processed by the controller or by the processor acting on behalf of, or instructed by, the controller is contested by the data subject, and the accuracy, the correctness or the completeness of the personal data processed cannot be verified beyond doubt, for a period enabling the existing doubt to be clarified,

b) the data should be erased according to section 20 point *a),* but there are reasons to assume, on the basis of the data subject's written declaration or the information available to the controller, that the erasure of the data would infringe the lawful interests of the data subject, for the period of the existence of the lawful interests that justify refraining from their erasure,

c) the data should be erased according to section 20 point *a),* but the retention of the data is necessary as evidence in the course of inquiries or proceedings specified by the law, in particular in criminal proceedings, carried out by, or with the participation of, the controller or

another organ performing public duties, for the period of the final and binding conclusion of such inquiries or proceedings,

d) the data should be erased according to section 20 point *a),* but the retention of the data is necessary for the purpose of fulfilling the obligation of documentation under section 12 (2), for the period specified in section 25/F (4).

(2) During the period of the restriction of processing, the controller or the processor acting on behalf of, or instructed by, the controller may only perform processing operations with the personal data affected by the restriction, with the exception of storage, for the enforcement of the data subject's lawful interests or according to the provisions laid down in an Act, an international agreement or a binding legal act of the European Union.

(3) In the course of terminating the restriction of processing specified in paragraph (1) *a),* the controller shall provide the data subject in advance with information on releasing the restriction of processing.

Section 20 For the purpose of the enforcement of the right to erasure, the controller shall erase the data subject's personal data without delay if

a) the processing is unlawful, in particular, if

aa) the processing is contrary to the principles laid down in section 4,

ab) the purpose of processing has terminated, or further processing is not necessary for the realisation of the purpose of processing,

ac) the period laid down in an Act, an international agreement or a binding legal act of the European Union has elapsed, or

ad) the legal basis of processing has terminated and there is no other legal basis of processing,

b) the data subject has withdrawn his consent given to the processing or requests the erasure of his personal data, with the exception of processing based on section 5 (1) *a)* or *c)* or on paragraph (2) *b)*,

c) the erasure of the data is required by the law, a legal act of the European Union, by the Authority or by a court, or

d) the period laid down in section 19 (1) *b)* to *d)* has elapsed.

Section 21 (1) If the controller dismisses the data subject's request for the rectification, erasure or the restriction of processing the personal data processed by the controller or by the processor acting on behalf of, or instructed by, the controller, it shall notify the data subject in writing without delay of

a) the dismissal, as well as of its legal and factual reasons, and

b) the rights to which the data subject is entitled under this Act, as well as the method of enforcing them, in particular of the data subject's right to exercise through the Authority the right to the rectification, erasure or the restriction of processing his personal data by the controller or by the processor acting on behalf of, or instructed by, the controller.

(2) Proportionately to the desired objective, the controller may delay the performance of providing the information under paragraph (1) *a)*, it may restrict the content of the information or it may refrain from providing the information, if this measure is indispensable for securing an interest specified in section 16 (3) *a)* to *f)*.

(3) If the controller rectifies or erases the personal data processed by it or the processor acting on behalf of, or instructed by, the controller, or restricts the processing of such personal data, the controller shall inform the controllers and processors to whom it has transferred the data prior to the measure of the measure and its content for the purpose of making them implement the rectification, erasure or the restriction of processing with regard to their own processing.

Section 22 For the purpose of the enforcement of his rights, according to the provisions laid down in Chapter VI, the data subject

a) may initiate an inquiry with the Authority for the purpose of investigating the lawfulness of the controller's measure if the controller restricts the enforcement of his rights under section 14 or dismisses his request aimed at the enforcement of these rights, and

b) may request the Authority to carry out an authority procedure for data protection if he considers that the controller or the processor acting on behalf of, or instructed by, the controller infringes, in the course of processing his personal data, the provisions laid down in laws or a binding legal act of the European Union on the processing of personal data.

Section 23 (1) In the context of processing operations within the processor's scope of activity, the data subject may seek judicial remedy against the controller or the processor if he considers that the controller or the processor acting on behalf of, or instructed by, the controller infringes, in the course of processing his personal data, the provisions laid down in laws or the binding legal act of the European Union on the processing of personal data.

(2) The controller or the processor shall be obliged to prove that the processing complies with the provisions laid down in laws or the binding legal act of the European Union on the processing of personal data, in particular with the fundamental requirements specified in section 4 (1) to (4a) in the case of processing operations under section 2 (3).

(3) The data subject may bring the action before the regional court having territorial jurisdiction over his domicile or place of residence, according to his choice.

(4) Any person who otherwise does not have the capacity to be a party may be a party to the court action. The Authority may intervene in the action in order to facilitate the success of the data subject.

(5) If the court upholds the claim, it shall establish the existence of the infringement and oblige the controller or the processor to

a) terminate the unlawful processing operation,

b) restore the lawfulness of processing, or

c) undertake the prescribed conduct to ensure the enforcement of the data subject's rights

and it shall also adopt a decision as necessary on the claim for damages or a grievance award.

(6) The court may order the publication of its judgment so as to disclose the identification data of the controller or the processor if the judgment affects a wide scope of persons, the defendant controller or processor is an organ performing public duties or if the gravity of the infringement justifies such publication.

Section 24 (1) The controller or the processor acting on behalf of, or instructed by, the controller shall be liable for compensating any damage which another person may suffer as a result of processing that infringes the provisions laid down in laws or the binding legal act of the European Union on the processing of personal data.

(2) The controller or the processor acting on behalf of, or instructed by, the controller shall be liable for paying a grievance award for the violation of personality rights that another person may suffer as a result of processing that infringes the provisions laid down in law or the binding legal act of the European Union on the processing of personal data, if the person whose personality rights had been violated has made a claim addressed to the controller or the processor acting on behalf of, or instructed by, the controller, for such a grievance award.

(3) The controller shall be exempted from liability for damage and from the obligation to pay the grievance award if he proves that the damage or the violation of the data subject's personality rights occurred as a consequence of an unavertable reason falling outside the scope of processing.

(4) The processor shall be exempted from the liability for the damage caused and for the payment of a grievance award if it proves that, during the processing operations it carried out, it acted in compliance with the obligations explicitly imposed upon processors in laws or the binding legal act of the European Union on the processing of personal data and with the lawful instructions given by the controller.

(5) In the event of the violation of the provisions laid down in laws or the binding legal act of the European Union on the processing of personal data, the controller or the processor acting on behalf of, or instructed by, the controller, as well as joint controllers and the processors acting according to a mandate or instruction given by them, shall bear joint and several liability

a) towards the data subject for the damage resulting from such an infringement, and

b) for paying to the data subject a grievance award in the event of a violation of personality rights resulting from such infringement.

(6) Damages shall not be paid and a grievance award shall not be claimed if the damage was due to the intentional or grossly negligent conduct of the person suffering the damage, or if the infringement of the personality rights arose from the intentional or grossly negligent conduct of the person whose personality rights were infringed.

9. Enforcement of rights related to personal data after the death of the data subject

Section 25 (1) Within five years of the death of the data subject, the rights to which the data subject was entitled in his life, specified in section 14 *b)* to *e)*, or in the case of processing operations under the General Data Protection Regulation, the rights specified in Article 15 to 18 and in Article 21 of the General Data Protection Regulation, may be enforced by a person authorised to do so by the data subject in the form of an administrative disposal or a declaration made at the controller and incorporated in a public deed or a private deed of full probative value, taking into account the declaration of the later date if the data subject has made more than one declaration to the same controller.

(2) If the data subject has not made a juridical act complying with paragraph (1), his close relative according to the Civil Code may enforce, even in the absence of it, within five years of the death of the data subject, the rights to which the data subject was entitled in his life, specified in section 14 *c)*, or in the case of processing operations under the General Data Protection Regulation, the rights specified in Article 16 and Article 21 of the General Data Protection Regulation, as well as in section 14 *d)* and *e)*, or in the case of processing operations under the General Data Protection Regulation, the rights specified in Article 16 and Article 18 of the General Data Protection Regulation, if the processing had already been unlawful in the life of the data subject or if the purpose of processing terminated upon the death of the data subject. The close relative who is the first to exercise his right shall be entitled to enforce the data subject's rights under this paragraph.

(3) In the course of enforcing such rights, in particular during the procedures against the controller and before the Authority or a court, the person enforcing the data subject's rights under paragraph (1) or paragraph (2) shall be entitled to the rights and be bound by the obligations laid down in this Act with regard to the data subject.

(4) The person enforcing the data subject's rights under paragraph (1) or paragraph (2) shall verify the fact and the date of the data subject's death with a death certificate or with a court decision, as well as his own personal identification, together with his status as a close relative in the case under paragraph (2), with a public deed.

(5) Upon request, the controller shall inform the data subject's close relative according to the Civil Code on the measures taken on the basis of paragraph (1) or paragraph (2), unless the data subject had prohibited it in his declaration specified in paragraph (1).

CHAPTER II/B

OBLIGATIONS OF THE CONTROLLER AND THE PROCESSOR

10. General duties of the controller

Section 25/A (1) For the purpose of securing the lawfulness of processing and taking all circumstances of the processing into account, in particular the purpose of processing, as well as the risks for the enforcement of the fundamental rights of the data subjects posed by the processing, the controller shall implement appropriate technical and organisational measures, such as pseudonymisation, where appropriate. Those measures shall be reviewed regularly and updated appropriately where necessary.

(2) The measures specified in paragraph (1) shall be formulated in such a way that they

a) take into account the state of the art and the cost of implementing such measures in order to serve in a reasonably available manner the efficient enforcement of the requirements on processing personal data, in particular the principles of processing and the rights of data subjects, and

b) are suitable and appropriate for ensuring that, by default

ba) only the kind and the quantity of personal data, and only to the extent and in the duration, which are necessary for the purpose of the processing are processed, and

bb) personal data processed by the controller are not made publicly accessible in the absence of the data subject's explicit expression of intent thereto.

(3) If the controller is obliged to designate a data protection officer, it shall adopt and apply an internal data protection and data security policy as a part of the measures specified in paragraph (1).

(4) Unless otherwise provided by an Act, an international agreement or a binding legal act of the European Union, those who have lawful access as processors or in any other way under the controller's instructions to the personal data processed in the controller's scope of activity may only perform the operations specified in the controller's instruction on the personal data accessed.

(5) The controller and the processor shall facilitate the activities of organs and persons authorised to conduct inquiries connected to the lawfulness of the processing operations performed by them, and they shall provide them with the information necessary for carrying out their procedures.

Section 25/B (1) Unless an Act, an international agreement or a binding legal act of the European Union provides a complete or partial determination of the respective responsibilities of the joint controllers for the performance of the obligations related to joint processing, in particular the enforcement of the data subject's rights and omitting to perform these obligations, the joint controllers shall determine it by means of a written and disclosed agreement between them to the extent it is not regulated in the legal obligations to which they are subject.

(2) Unless specified in an Act, an international agreement or a binding legal act of the European Union, a joint controller obliged to act as the contact point for the enforcement of the data subject's rights determined in this Act shall be designated in the agreement under paragraph (1). In the absence of a specified or designated joint controller acting as the contact point, the data subject may exercise his rights under this Act against any of the joint controllers in respect of any processing operation carried out by any one of the joint controllers.

11. The processor

Section 25/C (1) Only persons or organisations that provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirement of lawfulness and ensure the protection of the rights of the data subjects may act as processors. The processor shall verify these guarantees to the controller prior to the start of processing.

(2) The processor may only engage another processor if this is not excluded by the law and the controller has given its prior specific or general authorisation in a public deed or in a private deed of full probative value to the engagement of another processor.

(3) If another processor is engaged on the basis of the controller's general authorisation, the processor shall inform the controller, prior to engaging the other processor, of the person of the other processor and of the planned tasks to be carried out by the other processor. If, on the basis of this information, the controller raises an objection against the engagement of the other processor, the processor may only engage the other processor if the conditions specified in the objection are fulfilled.

Section 25/D (1) The details of the legal relationship between the controller and the processor shall be determined, within the framework specified in this Act and in a binding legal act of the European Union, in the law or in a written contract between the controller and the processor, including a contract concluded by electronic means. The controller shall be responsible for the lawfulness of the instructions it gives to the processor.

(2) The law or the contract referred to in paragraph (1) shall set out the subject matter, the duration, the nature and the purpose of the processing, the type of personal data concerned and the categories of data subjects, as well as the rights and obligations of the processor and the controller not regulated in this Act nor in a binding legal act of the European Union.

(3) The law or the contract referred to in paragraph (1) shall provide in particular that the processor is obliged

a) to act only on the basis of the controller's written instructions in the course of its activity,

b) to ensure in the course of its activity that the persons authorised to access the personal data concerned commit themselves to confidentiality concerning the personal data accessed by them, if they are not otherwise bound by an appropriate obligation of confidentiality under a law,

c) to assist in the course of its activity the controller with all appropriate tools for the purpose of facilitating the enforcement of the data subjects' rights and fulfilling its related obligations ,

d) either to erase without delay the personal data accessed during its activity or to transfer them to the controller and subsequently erase the existing copies following the completion of the processing operations it carried out, according to the choice of the controller and unless otherwise provided by an Act

e) to make available to the controller all information necessary to demonstrate compliance with the legal provisions on engaging the processor, and

f) to engage another processor only upon compliance with the conditions specified in this Act.

(4) If, by way of derogation from the provisions of this Act, a processor itself determines the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.

12. The controller's and the processor's records and the electronic logbook

Section 25/E (1) The controller shall maintain a record of its processing operations related to the personal data that it processes, personal data breaches and the measures taken concerning the data subject's right of access(hereinafter jointly „controller's record"). The controller shall record in the controller's record

a) the name and the contact details of the controller, including each joint controller, as well as of the data protection officer,

b) the purpose or purposes of processing,

c) in the event of the transfer or planned transfer of personal data, the scope of the recipients of the data transfer, including recipients in third countries and international organisations,

d) the scope of data subjects and of the data processed,

e) in the event of profiling, the existence of it,

f) in the event of international data transfer, the scope of the data transferred,

g) the legal bases of the processing operations, including data transfer,

h) where known, the time for the erasure of the personal data processed,

i) the general description of the technical and organisational security measures implemented according to this Act,

j) the circumstances of personal data breaches that occurred in the context of the data that it processes, as well as their effects and the measures taken to address them,

k) the legal and factual reasons for its measures restricting or rejecting, according to this Act, the enforcement of the data subject's right to access.

(2) The processor shall maintain a record of its processing operations carried out under the mandate or according to the instruction given by specific controllers (hereinafter "processor's record"). The processor shall record in the processor's record:

a) the name and the contact details of the controller, the processor and of other processors, as well as of the processor's data protection officer;

b) the types of processing operations carried out on behalf of, or according to the instruction given by, the controller;

c) in the event of international data transfer implemented according to the controller's explicit instruction, the existence of international data transfer, as well as the indication of the recipient third country or international organisation;

d) the general description of the technical and organisational security measures implemented according to this Act.

(3) The controller's record and the processor's record shall be maintained in written or electronic form and they shall be made available to the Authority on request.

(4) The bodies carrying out processing for national security purposes may also perform the obligation of maintaining the controller's record by implementing the recording and documentation obligations specified in the Act on national security services, provided that it is implemented in a manner suitable for fulfilling the requirements under sections 23 (2) and 25/A (5).

Section 25/F (1) For the purpose of ensuring the verifiability of the lawfulness of processing operations carried out with personal data by electronic means, the controller and the processor shall record in an automated processing system (hereinafter "electronic logbook")

a) the scope of the personal data affected by the processing operation,

b) the purpose of and the reason for the processing operation,

c) the exact time of carrying out the processing operation,

d) the person carrying out the processing operation,

e) the recipient of the data transfer if data transfer is implemented.

(2) The data recorded in the electronic logbook may only be accessed and used for the purpose of verifying the lawfulness of processing and enforcing data security requirements, as well as conducting criminal proceedings.

(3) At the request of the Authority or a person or organ engaged in an activity specified by the law for a purpose described in paragraph (2), the controller and the processor shall provide access to the electronic logbook and shall transfer data from the logbook to the requesting party.

(4) The data recorded in the controller's and the processor's record, as well as the electronic logbook, shall be retained for ten years after the erasure of the processed data.

(5) The organs carrying out processing for national security purposes may also perform the obligation of maintaining the electronic logbook by implementing the recording and documentation obligations specified in the Act on national security services in a manner suitable for fulfilling the requirements under sections 23 (2) and 25/A (5).

13. Data protection impact assessment and prior consultation

Section 25/G (1) The controller shall, prior to the start of the planned processing, carry out an assessment of the expected impact of the envisaged processing operations on the enforcement of the data subjects' fundamental rights, taking the circumstances of processing into account, in particular its purpose, the scope of the data subjects and the technology applied during the processing operations.

(2) When, according to the risk assessment implemented according to paragraph (1), the planned processing is likely to have a significant influence on the enforcement of a fundamental right of the data subjects (hereinafter "high-risk processing"), the controller shall prepare, prior to the start of processing, with the exception of the case specified in paragraph (6), a written evaluation of the expected effects of the planned processing on the enforcement of the data subjects' fundamental rights (hereinafter "data protection impact assessment").

(3) If the Authority classifies a specific type of processing as high-risk processing and publishes this finding, the high risk of the planned processing shall be presumed, provided that the planned processing entails the application of the same or similar operation or series of operations as the one applied during the type of processing covered by the finding.

(4) If the Authority classifies a specific type of processing as non-high-risk processing and it publishes this finding, the classification as non-high-risk processing shall be presumed concerning the planned processing, provided that the planned processing exclusively entails the application of the same or similar operation or series of operations as the one applied during the type of processing covered by the finding.

(5) The data protection impact assessment shall contain at least the general description of the envisaged processing operations, the description and the character of the risks to the enforcement of the data subjects' fundamental rights as identified by the controller and the measures planned for addressing these risks, as well as the measures applied by the controller for enforcing the rights related to personal data.

(6) With regard to mandatory processing, including in particular mandatory processing operations carried out for the purposes specified in section 2 (3), the data protection impact assessment under paragraph (5) shall be carried out by the party preparing the legislation that requires processing.

Section 25/H (1) If the planned processing

a) is expected to be of high risk according to the results of the data protection impact assessment carried out concerning the planned processing and in the absence of the controller taking the necessary measures to mitigate the risks implied by the processing, or

b) should be presumed to be of high risk according to section 25/G (3),

the controller, or the processor within its scope, shall initiate, with the exception laid down in paragraph (2), prior to the start of the processing, a consultation with the Authority (hereinafter "prior consultation").

(2) With regard to mandatory processing, including in particular the mandatory processing operations carried out for the purposes specified in section 2 (3), prior consultation shall be initiated and conducted in the framework of the procedure for preparing legislation by the party preparing the legislation.

(3) The controller, or the processor within the limits of its activity, shall, simultaneously with initiating prior consultation, provide the Authority with the results of the data protection impact assessment and it shall inform the Authority of any circumstance that the Authority holds to be in need of clarification in order to carry out the prior consultation successfully.

(4) If the Authority finds in the course of the prior consultation that, with regard to the planned processing, the provisions specified in the relevant legislation are not enforced to the full extent, in particular when it finds that the controller did not identify or mitigate the risks of processing appropriately, it shall, in addition to or instead of taking any other measure in accordance with its tasks and powers, specify those actions suitable for the elimination of the explored deficiencies and it shall recommend to the controller, or to the processor, within the limits of its activities, to implement such actions.

(5) The Authority shall make the recommendations specified in paragraph (4) in writing within six months from the initiation of the prior consultation. The Authority may extend this time limit by no more than one month; in this case it shall provide the controller or the processor with information, within one month from initiating the prior consultation, on the existence of and reasons for that extension.

14. Data security measures

Section 25/I (1) For the purpose of ensuring an appropriate level of security concerning the personal data processed, the controller and the processor shall implement technical and organisational measures to reflect the level of risks, resulting from the processing, to the enforcement of the data subjects' fundamental rights, taking into account, in particular, risks entailed by any processing of the sensitive data of the data subjects.

(2) In the course of developing and implementing the measures specified in paragraph (1), the controller and the processor shall take all circumstances of the processing into account, in particular the state of the art, the cost of implementing the measures and the nature, scope and purposes of processing, as well as the risks of varying likelihood and gravity for the enforcement of the rights of data subjects posed by the processing.

(3) The controller and, within the limits of its activity, the processor shall ensure through the measures specified in paragraph (1)

a) the denial of access by unauthorised persons to the equipment used for the processing (hereinafter "processing system"),

b) the prevention of unauthorised reading, copying, modification or removal of data media,

c) the prevention of unauthorised recording of personal data in the processing system, as well as of unauthorised access to, modification or erasure of the personal data stored therein,

d) the prevention of using the processing system by unauthorised persons by means of data transmission equipment,

e) that the persons authorised to use the processing system shall only have access to the personal data specified in the authorisation of access,

f) the possibility of verifying and determining the identity of the recipients to whom the personal data have been or can be transferred or provided by means of data transmission equipment,

g) the possibility of subsequently verifying and determining the scope of the personal data entered into the processing system, as well as the time of entering such data and the identity of the person who entered them,

h) the prevention of unauthorised access to, copying, modification or erasure of personal data during their transmission or the transportation of the data medium,

i) the recoverability of the processing system in the event of a breakdown, and

j) the operability of the processing system, the reporting of malfunctions that occurred during its operation, and the prevention of the stored personal data being altered through the malfunctioning of the system.

(4) For the purpose of protecting datasets processed electronically in various registers, the controller, or the processor within its scope of activity, shall implement an appropriate technical solution to prevent data stored in the registers from being directly interconnected or assigned to the data subjects, unless an Act allows it.

15. Handling of personal data breaches

Section 25/J (1) The controller or the processor acting on behalf of, or instructed by, the controller shall record the data according to paragraph (5) *a)*, *c)* and *d)* connected to any personal data breach occurring in relation to the data processed by it, and it shall, without undue delay but not later than within seventy-two hours after having become aware of it, notify the personal data breach to the Authority.

(2) The personal data breach should not be notified when it is unlikely to result in a risk to the enforcement of the data subjects' rights.

(3) If the controller is prevented from performing in due time its obligation of notification according to paragraph (1), it shall perform the notification without delay after the obstacle ceases to exist, together with attaching to the notification its statement on the reasons for the delay.

(4) If the personal data breach occurred in the context of the processor's activity, or if the personal data breach is otherwise detected by the processor, it shall notify the controller of the personal data breach without delay upon becoming aware of it.

(5) In the framework of the obligation of notification under paragraph (1), the controller shall

a) describe the nature of the personal data breach, including, where possible, the scope and approximate number of data subjects concerned, as well as the scope and approximate number of personal data records concerned,

b) communicate the name and contact details of the data protection officer or other contact point designated to provide more information,

c) describe the likely consequences of the personal data breach, and

d) describe the measures taken or proposed to be taken by the controller to address the personal data breach for mitigating the possible adverse effects resulting from the personal data breach and for other purposes.

(6) If any of the information specified in paragraph (5) *a)* to *d)* is not at the disposal of the controller at the time of making the notification, the controller shall supplement such data subsequently, without delay, after becoming aware of the availability of the information.

(7) If the personal data breach affects any data transferred to the controller by the controller of another EEA State, or transferred by the controller to the controller of another EEA State, the information specified in paragraph (5) shall be communicated without delay by the controller to the controller of that EEA State.

(8) With the exception of the notifications pertaining to classified data, the obligation of notification specified in paragraph (1) shall be performed by the controller through the electronic platform provided for this purpose by the Authority.

(9) With regard to processing for national security purposes, the provisions of paragraphs (1) to (8) shall be applied, with the derogation that if the performance of the controller's obligation of notification under paragraph (1) and the obligation of communication under paragraph (7) is in conflict with the interests of national security, they shall only be performed after such interests of national security have ceased.

Section 25/K (1) When the personal data breach is likely to result in consequences materially influencing the enforcement of a fundamental right of the data subject (hereinafter "high-risk personal data breach"), the controller shall, with the exception of processing for national security purposes, communicate the personal data breach to the data subject without delay.

(2) The controller shall be exempted from the obligation of informing the data subject according to paragraph (1) if

a) the controller had implemented appropriate technical and organisational protection measures before the personal data breach, and those measures were applied to the personal data affected by the personal data breach, in particular those, such as encryption, that render the personal data unintelligible to any person who is not authorised to access them,

b) after having become aware of the personal data breach, the controller has taken subsequent measures that ensure that the consequences materially influencing the enforcement of a fundamental right of the data subject are not likely to occur,

c) informing the data subject directly according to paragraph (1) requires disproportionate efforts by the controller, and therefore the controller provides the data subjects with adequate information on the personal data breach by way of public communication accessible to anyone, or

d) communication is excluded by an Act according to the provisions of paragraph (6).

(3) In the framework of the obligation of communication under paragraph (1), the controller shall present the nature of the personal data breach and it shall provide the data subject with the information specified in section 25/J (5) *b), c)* and *d)*.

(4) When, on the basis of the notification performed according to section 25/J (1), the Authority establishes that it is necessary to inform the data subject due to the high risk of processing, the controller shall implement any outstanding obligation of communication under paragraph (1) without delay after the establishment of this obligation.

(5) The controller shall not be obliged to perform the obligation of communication according to paragraph (1) if, on the basis of the notification performed under section 25/J (1), the Authority has established the existence of a circumstance specified in paragraph (2) *a)* to *d)*.

(6) By way of derogation from the provisions under paragraphs (1) to (5), an Act may exclude, restrict or require the delayed performance of providing the data subject with information, on the conditions and for the reasons specified in section 16 (3).

16. The data protection officer

Section 25/L (1) The controller and the processor shall designate a data protection officer for the purpose of implementing the legal provisions pertaining to the processing of personal data and to facilitate the enforcement of the rights of the data subjects if

a) the controller or the processor carries out a duty of the State or another public duty specified by the law, except for the courts, or

b) it is prescribed by an Act or legal act of the European Union.

(2) The data protection officer shall be designated on the basis of his adequate level of knowledge concerning the legal rules and the judicial practice on the protection of personal data, as well as his ability to fulfil the duties laid down in section 25/M (1).

(3) The data protection officer may perform the duties under section 25/M (1) for several controllers or processors at the same time, provided that this poses no risk to the professional and efficient performance of his duties. The data protection officer shall provide the controller or the processor with information on the identity of other controllers or processors where he fulfils their data protection officer's duties.

(4) The controller or the processor shall inform the Authority on the name and the postal and electronic mail addresses of the data protection officer, as well as on the change of these data and it shall publicly disclose such data.

(5) The controller and the processor shall engage the data protection officer in due time in the preparation of all decisions that affect the protection of personal data, together with providing him with all the conditions, rights and resources, as well as with access to all the data and information necessary for the performance of his duties and for keeping his professional knowledge up-to-date.

Section 25/M (1) The data protection officer shall facilitate the performance of the duties of the controller and the processor specified in the legal provisions pertaining to the processing of personal data; in particular he shall

a) provide up-to-date information on the legal provisions pertaining to the processing of personal data, and he shall provide the controller, the processor and the persons employed by them and engaged in performing processing operations with advice on the manner of enforcing these provisions;

b) observe and review, on an ongoing basis, the enforcement of the legal provisions, in particular laws and internal data protection and data security policies, pertaining to the processing of personal data, including the clear assignment of responsibilities related to specific processing operations, awareness-raising and data protection training of staff involved in processing operations, and the implementation of regular audits;

c) facilitate the data subjects in exercising their rights, in particular by investigating the data subjects' complaints and by initiating, at the controller or the processor, the implementation of measures necessary for remedying the complaint,

d) facilitate by providing professional advice and by monitoring the performance of the data protection impact assessment,

e) cooperate with the organs and persons entitled to carry out procedures related to the lawfulness of the processing, acting as a contact point in particular with the Authority for the purpose of facilitating prior consultation and the procedures carried out by the Authority,

f) contribute to the drafting of the internal policy on data protection and data security.

(2) During the term of his legal relationship and after the termination of it, the data protection officer shall keep secret the personal data, classified information and data qualified by an Act as protected secret or as a secret linked to exercising a profession that he has become aware of in the context of performing his activity, as well as all data, facts or circumstances that the controller or the processor employing him is not obliged to make publicly accessible according to the provisions of an Act.

25/N. § (1) The conference of data protection officers (hereinafter "conference") is intended to maintain a regular professional relationship between the Authority and the data protection officers; its goal is to develop a consistent legal practice with regard to the application of laws concerning the protection of personal data and access to data of public interest.

(2) The president of the Authority shall convene the conference as necessary, but at least once every year, and shall determine its agenda.

17 to 19

CHAPTER III

ACCESS TO DATA OF PUBLIC INTEREST

20. General rules on access to data of public interest

Section 26 (1) Any person or organ performing state or local government functions, or performing other public duties defined by law (hereinafter jointly "organ performing public duties"), shall allow any person to have free access to data of public interest and data accessible on public interest grounds under its control if so requested, with the exceptions provided by this Act.

(2) The name of the person acting within the functions and powers of the organ performing public duties, as well as his functions and duties, executive mandate, his other personal data relevant to performing public duties, and his personal data to which access is ensured by an Act, shall qualify as data accessible on public interest grounds. Personal data accessible on public interest grounds shall be disseminated in compliance with the principle of data processing limited to the intended purpose. Publishing personal data accessible on public interest grounds on the website shall be regulated by Annex 1 of this Act and a specific Act relating to the legal status of persons performing public duties.

(3) Unless otherwise provided by an Act, any data other than personal data that is in connection with the activities of and processed by organs or persons providing services that are mandatory by virtue of law, or under a contract concluded with any state or local government organ, or services which are impossible to be performed otherwise, shall be deemed data accessible on public interest grounds.

(4) In the course of fulfilling a request for access to data specified in paragraph (3), the organ or person specified in paragraph (3) shall act in accordance with sections 28 to 31.

Section 27 (1) No access to data of public interest or data accessible on public interest grounds shall be provided if it has been classified under the Act on the protection of classified data.

(2) The right to access data of public interest or data accessible on public interest grounds may be restricted by an Act, with the specific type of data indicated, if considered necessary for the purposes of

a) national defence;

b) national security;

c) the prosecution and prevention of criminal offences;

d) environmental protection and nature preservation;

e) central financial or foreign exchange policy;

f) external relations, relations with international organisations;

g) court proceedings or administrative authority procedures;

h) intellectual property rights.

(3) As data accessible on public interest grounds, the following shall not qualify as business secret: the budget of the central government and the local governments; furthermore, data related to the use of European Union funds, to benefits and allowances involving the budget, to the management, possession, use, utilisation and the disposal and encumbering of central and local government assets, and the acquisition of any right in connection with such assets, as well as data, the accessibility or publication of which is prescribed on public interest grounds by a specific Act. Disclosure, however, shall not entail access to data, to know-how in particular, the making available of which would cause disproportionate harm with respect to the performance of business activities, provided that this does not prevent the possibility of access to data accessible on public interest grounds.

(3a) A natural person, legal person or organisation having no legal personality that establishes a financial or business relationship with a person belonging to one of the sub-systems of the public finances shall, upon request, provide information to anyone with respect to data that is public on public interest grounds based on paragraph (3) and that is in connection with such a relationship. The obligation to provide information can be fulfilled by disclosing the data accessible on public interest grounds, or by indicating the public source that contains the data disclosed earlier in an electronic form.

(3b) If the party obliged to provide information on the basis of paragraph (3a) refuses to provide the information, the party requesting information may initiate the procedure of the organ authorised to exercise legal supervision over the party obliged to provide information.

(4) Access to data of public interest may also be limited on the basis of a legal act of the European Union with a view to safeguarding vital economic or financial interests of the European Union, including monetary, fiscal and tax policies.

(5) Any data compiled or recorded by an organ performing public duties as part and in support of its decision-making process within the limits of its powers and duties shall not be disclosed for ten years from the date it was compiled or recorded. After considering the weight of public interest with respect to granting or denying access, the head of the organ that processes the data in question may permit access.

(6) A request to access data underlying a decision may be dismissed after the decision is adopted but within the time limit referred to in paragraph (5), if the data underlies future decisions, or access to it would jeopardise the lawful functioning of the organ performing public duties, or would jeopardise the performance of its duties without any undue external influence, such as, in particular, the free expression of the standpoint of the organ which generated the data during the preliminary stages of its decision-making process.

(7) The time limit for the restriction of access to certain specific data underlying a decision as specified in paragraph (5) may be reduced by law.

(8) The provisions of this Chapter shall not apply to the provision of data from registers of certified authenticity and subject to the provisions of another specific Act.

21. Request for access to data of public interest

Section 28 (1) Data of public interest shall be made available to anyone upon a request presented orally, in writing or by electronic means. Access to data accessible on public interest grounds shall be governed by the provisions of this Act pertaining to data of public interest.

(2) Unless otherwise provided by an Act, processing the personal data of the requesting party is permitted only to the extent necessary for fulfilling the request, or assessing the request on the basis of the conditions referred to in section 29 (1a), or paying the fee determined for the fulfilment of the request. Following the expiry of the interval referred to in section 29 (1a), or following the payment of the fee, the personal data of the requesting party shall be erased without delay.

(3) If the request for data is unclear, the controller shall call on the requesting party to clarify it.

Section 29 (1) The organ performing public duties and processing the data of public interest shall fulfil the request for access to such data as soon as possible, but not later than 15 days from receiving the request.

(1a) The organ performing public duties and processing the data shall not be obliged to fulfil the request for data with respect to the part of the data that had already been requested by the same requesting party and is aimed at an identical set of data, provided that the data belonging to the identical set of data did not change.

(1b) The organ performing public duties and processing the data shall not be obliged to fulfil the request for data if the requesting party fails to indicate his name, its identity, in the case of other than a natural person, or the contact information through which it could be notified and informed in connection with the request for data.

(2) If the request concerns data large in number or in volume, or if fulfilling the request for data requires a disproportionate use of the labour resources needed for the performance of the core duties of an organ performing public duties, the time limit referred to in paragraph (1) may be extended by 15 days on one occasion, of which the requesting party shall be informed within 15 days of the date of receiving the request.

(2a) If the request for data involves data that is generated by an institution of the European Union or its Member States, the controller shall contact the institution of the European Union or the Member State concerned without delay and shall inform the requesting party thereof. The interval between providing this information and the controller's receipt of the response of the European Union institution or the Member State concerned shall not be taken into account when calculating the time limit for fulfilling the request for data.

(3) The requesting party may also be provided with a copy of the document or a part of the document containing the data in question, irrespective of the form of storage. The organ performing public duties and processing the data may charge a fee amounting to the costs incurred by the fulfilment of the request, and shall communicate this amount to the requesting party in advance.

(3a) The requesting party shall make a statement within 30 days from receiving the information as per paragraph (3) as to whether he wishes to maintain his request or not. The interval between providing the information and the receipt of the requesting party's statement shall not be taken into account when calculating the time limit available for the fulfilment of the request. If the requesting party maintains his request, he shall pay the fee to the controller within the time limit determined by the controller, of at least 15 days.

(4) If fulfilling the request for data requires a disproportionate use of the labour resources needed for the performance of the core duties of an organ performing public duties, or the document or a part of the document of which the copy had been requested is large, or if the amount of the fee exceeds the amount determined in a government decree, the request shall be fulfilled within 15 days from the date on which the payment of the fee was made by the requesting party. Within 15 days from the date of receipt of his request, the requesting party shall be notified that the fulfilment of his request for data requires a disproportionate use of the labour resources necessary for the performance of the core duties of an organ performing public duties, or the document or a part of the document of which he requested the copy is

large, also regarding the amount of the fee and the possibility of fulfilling the request without making copies.

(5) When determining the fee, the following items may be taken into account:

a) the cost of the data medium that will contain the requested data;

b) the cost incurred by delivering the data medium containing the requested data to the requesting party; and

c) the cost of labour related to fulfilling the data request if fulfilling the request for data requires a disproportionate use of the labour resources necessary for the performance of the core duties of an organ performing public duties.

(6) The fee items referred to in paragraph (5) that may be charged shall be determined by law.

Section 30 (1) If a document containing data of public interest also contains any other data that the requesting party may not access, the data that must not be accessed shall be made unrecognisable on the copy.

(2) Data shall be supplied in a comprehensible form and in the format and via the means requested by the requesting party, provided that the organ performing public duties and processing the data is capable of fulfilling such a request without disproportionate difficulties. If the data requested had previously been disclosed electronically, the request may also be fulfilled by way of reference to the public source where the data are available. A request for data shall not be dismissed on the grounds that it cannot be complied with in a comprehensible form.

(3) If a request for data is refused, the requesting party shall be notified thereof within 15 days in writing or, if the requesting party has given his electronic mailing address, by electronic means, and he shall be informed of the reasons for refusal, and the legal remedies that are available for him under this Act. The controller shall keep records on the requests dismissed, including the reasons for them, and shall inform the Authority of them each year, by 31 January.

(4) A request for data of public interest made by a person whose native language is not Hungarian shall not be refused because it was written in the requesting party's native language, or in any other language he understands.

(5) If the controller is vested with discretionary authority by an Act with respect to the refusal of requests for access to data of public interest, the grounds serving for refusal shall be interpreted restrictively, and the request for access to data of public interest shall only be refused if the underlying public interest outweighs the public interest of allowing access to the data of public interest.

(6) Organs performing public duties shall adopt regulations governing the procedures for fulfilling requests for access to data of public interest.

(7) Access to data aiming to provide a comprehensive examination of the financial management of organs performing public duties, including accounting and itemised audits, shall be regulated in specific Acts. By referring to this, the controller may, instead of providing a copy of the document containing the requested data, also fulfil the request by indicating the persons involved in the legal relationship, the type of the legal relationship, the subject of the legal relationship and the volume of the service and the amount of consideration paid, as well as the date of performance.

Section 31 (1) In the event that the request for access to data of public interest of a requesting party is dismissed, or the time limit or, if the controller extended it pursuant to section 29 (2), the extended time limit expires with no result, as well as for the judicial review of the fee determined for the fulfilment of the request, the requesting party may turn to court.

(2) The burden of proof for the lawfulness and the reasons for refusal, as well as the reasons based on which the amount of the fee is payable for fulfilling the request, shall lie with the controller.

(3) The action shall be brought against the organ performing public duties that dismissed the request within thirty days from communicating the dismissal, the expiry of the time limit with no result, or the time limit for the payment of the fee. If the requesting party makes a notification to the Authority aimed at initiating the Authority's inquiry regarding the dismissal or the non-fulfilment of the request, or with respect to the amount of the fee charged for fulfilling the request, the action may be brought within thirty days following the receipt of the notification of the refusal to examine the request on its merits, of the termination of the inquiries, of its conclusion under section 55 (1) *b)*, or of the notification under section 58 (3). An application for excuse may be submitted in the event of failure to meet the time limit for bringing the action.

(4) Any person who does not otherwise have the capacity to be a party may be a party to the court action. The Authority may intervene in the action in order to facilitate the success of the requesting party.

(5) With the exception of actions brought against organs performing public duties having national territorial competence, the action shall be brought before a district court having territorial jurisdiction and located where the regional court has its seat or before the Pest Central District Court in Budapest. The territorial jurisdiction of the court shall be established by the location of the seat of the organ performing public duties acting as defendant.

(6) The court shall hear such cases as a matter of priority.

(6a) If the request for access to data of public interest is refused by the controller on the basis of section 27 (1), and the requesting party turns to court on the basis of paragraph (1) for the judicial review of the dismissal of his request, the court shall initiate an administrative authority procedure for the review of the data classification with the Authority and shall simultaneously suspend the court proceedings. No separate appeal shall be available against the order initiating the administrative authority procedure for the review of the data classification or suspending the court proceedings.

(7) If the decision of the court is in favour of the request for access to data of public interest, the court shall, also determining the applicable time limit for fulfilling the request, order the controller to disclose the data of public interest. The court may modify the amount charged for fulfilling the request for access to the data of public interest, or may order the organ performing public duties to commence a new procedure to determine the amount of the fee payable.

CHAPTER IV

PUBLICATION OF DATA OF PUBLIC INTEREST

22. Obligation to provide information on data of public interest

Section 32 With respect to matters falling under their scope of duties, organs performing public duties shall promote and ensure that the general public is promptly provided with accurate information, such as regarding the budgets of the state and local governments, as well as their implementation, the management of assets controlled by the state and local governments, the appropriate use of public funds and contracts concluded in connection with public funds, and special and exclusive rights conferred upon market actors, private organisations or individuals.

23. Obligation of electronic publication

Section 33 (1) Access to data of public interest, the publication of which is rendered mandatory under this Act, shall be made available to the general public, without personal identification, on the internet website without any restriction, in digital format, capable of being printed or copied without any partial loss or distortion of data, free of charge, including accessing, downloading, printing, copying and transmitting through a network (hereinafter "electronic publication"). Access to published data shall not be made subject to the provision of personal data.

(2) Unless otherwise provided by an Act, the following organs shall publish data specified in the publication schemes referred to in section 37 on their websites:

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

b)

c) the central state administration organs, with the exception of governmental committees, as well as the national chambers of professions; and

d) capital and county government offices.

(3) Apart from those listed in paragraph (2), organs performing public duties shall have the option to fulfil their obligation of electronic publication, as defined in section 37, on their own website, another website maintained jointly with their associations, or by other organs fulfilling their supervision, professional control or operational coordination, or a central website set up for this purpose.

(4) Any public education institution without national or regional responsibilities shall fulfil its obligation of electronic publication under this Act by providing data to the information systems specified by sectoral laws.

Section 34 (1) The data source, if publishing data on a website other than its own, shall transfer the data, in accordance with section 35, to the data publisher, which shall ensure that the data is published on its website, and that the name of the organ from which the data of public interest originates, or to which it pertains, is clearly indicated.

(2) The data publisher shall design the website used for publication in such a way that it enables the publication of data and shall ensure the continuous operation of the website and recovery from breakdowns and that data are updated on a regular basis.

(3) The website used for publication shall offer comprehensible information concerning the rules on individual requests for access to data of public interest. The information provided shall also include the description of available legal remedies.

(4) In addition to the data of public interest specified in the publication scheme, other data of public interest and data accessible on public interest grounds may also be published electronically on the website designated thereto.

Section 35 (1) The head of the data source organ under the obligation of electronic publication shall ensure that the data included in the publication scheme specified in section 37 are published accurately and are updated on an ongoing basis, and shall ensure that such data are sent to the data publisher.

(2) Liability for the electronic publication of the data sent, ensuring continuous access to them and keeping the data authentic and continuously updated shall lie with the data publisher.

(3) The data source and the data publisher shall adopt internal regulations laying down the detailed rules for fulfilling their obligations as referred to in paragraphs (1) and (2), respectively.

(4) Unless otherwise provided by this Act or another law, data published electronically shall not be removed from the website. In the event of the termination of the organ, the obligation of publication shall lie with the legal successor of that organ.

Section 36 The publication of data specified in the publications schemes referred to in section 37 shall be without prejudice to the obligation of the given organ concerning the publication of data of public interest or data accessible on public interest grounds as prescribed in other laws.

24. Publication schemes

Section 37 (1) The organs referred to in section 33 (2) to (4) (hereinafter jointly "organs subject to the obligation of publication") shall, with the exception set out in paragraph (4), publish the data pertaining to their activities that are specified in the general publication scheme referred to in Annex 1 in the way defined in Annex 1.

(2) With respect to certain specific sectors, additional data may be prescribed by law to be published by certain types of organs performing public duties (hereinafter "sector-specific publication schemes").

(3) The publication of other specific data may be rendered mandatory by the head of the organ subject to the obligation of publication, upon consulting with the Authority, as well as by laws with respect to organs performing public duties and to other agencies controlled or supervised by such organs, or to the sections of such agencies (hereinafter "organ-specific publication schemes").

(4) Upon consulting with the Authority, the Government shall determine in a decree the set of data that shall be published by the national security services.

(5) With regard to collegiate organs subject to the obligation of publication, the competence to determine or amend the sector-specific publication schemes, upon consulting with the Authority, shall lie with these organs.

(6) The head of the organ subject to the obligation of publication shall review, at least annually, the publication scheme he published under paragraph (3), with a view to requests for access to data of public interest not included in the publication scheme, and shall supplement it on the basis of such requests received in a substantial rate or number.

(7) The publication schemes shall also determine the frequency of publication, depending on the type of data to be published.

(8) The Authority may make recommendations for drawing up or amending the sector-specific and organ-specific publication schemes.

24/A Central electronic register of data of public interest and the integrated retrieval system for public data

Section 37/A (1) For the purpose of providing fast and easy access to data of public interest that shall be published electronically under this Act, the central electronic register published on the designated website, specifically created and operated by the minister responsible for the implementation of infrastructure requirements for administrative information technology systems, shall contain all the relevant descriptive data related to the websites, databases and records operated by organs that, under this Act, are subject to the obligation of electronic publication of data of public interest.

(2) Electronic access to data of public interest of organs referred to in paragraph (1) via uniform criteria, as well as facilities for searching data of public interest, shall be ensured by the integrated search system for public data operated by the minister responsible for the implementation of infrastructure requirements for administrative information technology systems.

Section 37/B (1) The data source shall ensure that the descriptive data of the websites, databases and records that it operates and that contain data of public interest are forwarded to the minister responsible for the implementation of infrastructure requirements for administrative information technology systems, and shall ensure that the forwarded data of public interest are updated on a regular basis; moreover, the data source shall also be responsible for the content of the data of public interest transferred to the integrated retrieval system for public data, as well as for having such data updated on a regular basis.

(2) Maintaining the registers of databases and records that contain data of public interest or linking up with the integrated retrieval system for public data shall not exempt the data source from the obligation of electronic publication.

CHAPTER V

NATIONAL AUTHORITY FOR DATA PROTECTION AND FREEDOM OF INFORMATION

25. Legal status of the Authority

Section 38 (1) The Authority shall be an autonomous state administration organ.

(2) The Authority shall be responsible for monitoring and promoting the enforcement of rights to the protection of personal data and access to data of public interest and data accessible on public interest grounds, as well as promoting the free movement of personal data within the European Union.

(2a) For natural persons and legal entities under the jurisdiction of Hungary, the tasks and powers specified in the General Data Protection Regulation for the supervisory authority shall be exercised by the Authority according to the provisions of the General Data Protection Regulation and of this Act.

(2b) In contentious and non-contentious proceedings aimed at adopting a judicial decision, the functions of the Authority specified in paragraph (2) concerning personal data shall not extend to exercising the powers specified in paragraph (3) with regard to the data processing operations carried out by the court on the basis of the provisions pertaining to such proceedings.

(3) Acting within its functions referred to in paragraphs (2) and (2a), and under the provisions of this Act, the Authority:

a) shall conduct inquiries upon notification and *ex officio*;

b) shall conduct at the application of the data subject or *ex officio* authority procedures for data protection;

c) shall conduct *ex officio* authority procedures for the supervision of data classification;

d) may turn to court in connection with any infringement of rights concerning data of public interest and data accessible on public interest grounds;

e) may intervene in actions brought by others;

f)

g) shall conduct, upon application, procedures for the authorisation of data processing;

h) shall perform the tasks specified for the supervisory authority of a Member State in a binding legal act of the European Union and in particular in the General Data Protection Regulation and in Directive (EU) 2016/680, and other tasks specified in an Act.

(4) Acting within its functions referred to in paragraphs (2) and (2a), the Authority:

a) may make recommendations with respect to new laws and to the amendment of laws pertaining to the processing of personal data, the access to data of public interest and to data accessible on public interest grounds, and shall give its opinion with respect to draft laws affecting its functions;

b) shall publish a report on its activities each year, by 31 March, and shall submit this report to the National Assembly;

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

d) shall give its opinion on sector-specific and organ-specific publication schemes under this Act and relating to the activities of the given organ performing public duties;

e) shall cooperate with the organs and persons specified in Acts to represent Hungary in the common data protection supervisory bodies of the European Union;

f) shall organise the conference of data protection officers;

g) to *h)*.

(5) The Authority shall be an independent organ subject to Acts only; it may not be instructed in its functions and shall operate independently of other organs and of undue influence. The tasks of the Authority may only be determined by an Act.

26. Budget and financial management of the Authority

Section 39 (1) The Authority shall be a central budgetary organ with the powers of a budgetary chapter, and its budget shall constitute an independent heading within the budgetary chapter of the National Assembly.

(2) The main totals of expenditures and incomes of the Authority for the given budgetary year may only be reduced by the National Assembly, 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 material competence or in its material competence as a governing organ.

(3) The fines imposed by the Authority shall constitute part of the central budget's revenue.

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

27. President of the Authority

Section 40 (1) The head of the Authority shall be its president. The president of the Authority shall be appointed by the President of the Republic, on the proposal of the Prime Minister. The president of the Authority shall be selected from those Hungarian citizens who have a law degree and the right to stand as candidates in parliamentary elections, have at least ten years of experience in auditing procedures related to data protection or freedom of information, or who hold an academic degree in either of those fields.

(2) A person who served as a member of the National Assembly or the European Parliament, a national minority advocate, the President of the Republic, a member of the Government, a state secretary, a representative of a local government, a mayor or deputy mayor, a lord mayor or deputy lord mayor, chair or deputy chair of a county assembly, a member of a national minority self-government or an officer or employee of a political party in the four-year period before the proposal for appointment shall not be appointed as president of the Authority.

(3) The President of the Republic shall appoint the president of the Authority for a term of nine years. After the termination of his mandate, the president of the Authority may be reappointed as the president of the Authority on one occasion.

(4) Upon being appointed, the president of the Authority shall take an oath before the President of the Republic in accordance with the Act on the oath and vow taken by certain public officials.

Section 41 (1) The president of the Authority shall not be a member of any political party, shall not engage in political activities, and his mandate shall be considered irreconcilable with other state or local government offices or mandates.

(2) The president of the Authority may not pursue any other gainful occupation and may not receive remuneration for any other activity, except for scientific, educational and artistic activities or activities falling under copyright protection, revising and editorial activities, and the activities of a foster parent conducted in the framework of an employment relationship.

(3) The president of the Authority shall not hold any executive office in a company and shall not be a member of the supervisory board of a company, nor shall he be a member of a company undertaking personal assistance.

Section 42 (1) The president of the Authority shall submit a declaration of personal assets in accordance with the provisions on the declarations of personal assets of members of the National Assembly within thirty days from his appointment, and subsequently by 31 January of each year, and also within thirty days after the date of termination of his mandate.

(2) In the event of non-compliance with the requirement of submitting the declaration of personal assets, the president of the Authority shall not be entitled to exercise his office and shall not receive any remuneration until his declaration of personal assets is submitted.

(3) The declaration of personal assets shall be public; its page-for-page-identical copy shall be posted on the Authority's website without delay. The declaration of personal assets shall not be removed from the website for a period of one year following the termination of the mandate of the president of the Authority.

(4) Anyone may request the Prime Minister to conduct a procedure regarding the declaration of personal assets of the president of the Authority by making a claim on the specific sections of the declaration and the disputed contents of those sections. If the request is not in conformity with the requirements set out in this paragraph, if it is manifestly unfounded, or if the request is re-submitted offering no new claim or data, the Prime Minister shall dismiss the request without commencing an inquiry on its merits. The Prime Minister shall assess the veracity of the data supplied in the declaration of personal assets.

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

(6) The verifying data submitted by the president of the Authority in connection with his declaration of personal assets shall be erased on the thirtieth day following the date of the conclusion of the procedure.

Section 43 (1) The president of the Authority shall be entitled to the same remuneration and benefits as the salary and benefits of ministers, including an executive bonus amounting to one and a half times the executive bonus of ministers.

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

Section 44 (1) In terms of eligibility for social security benefits, the president of the Authority shall be regarded as a person employed in a public service relationship.

(2) The period of the president's mandate shall be recognised as spent in public service at an administrative organ.

Section 45 (1) The mandate of the president of the Authority shall terminate

a) upon the expiry of his term of office;

b) upon his resignation;

c) upon his death;

d) if the conditions required for the appointment are no longer met or upon the violation of the rules regarding the declaration of his assets;

e) upon a conflict of interest being established with regard to him;

f)

g)

(2) The president of the Authority shall be entitled to resign from office at any time by tendering his resignation in writing to the President of the Republic via the Prime Minister. The mandate of the president of the Authority shall terminate on the day after the date of resignation, as indicated in the resignation, or, failing this, on the day his resignation is submitted. A declaration of acceptance is not required for the resignation to take effect.

(3) If the president of the Authority fails to resolve the conflict of interest under section 41 within thirty days from the date of his appointment, or if any cause of conflict of interest arises while he is in office, the President of the Republic, upon the motion of the Prime Minister, shall decide on the issue of establishing a conflict of interest.

(4)

(5)

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

(6a) The Prime Minister shall send a copy of his motion under paragraphs (3) and (6) to the President of the Republic and to the president of the Authority simultaneously.

(6b) The president of the Authority may bring an administrative court action for declaring the motion unfounded. No application for excuse may be filed upon failure to meet the time limit for bringing the action. The court shall proceed according to the rules on court actions relating to public service relationship, with the proviso that the action shall be brought against the Prime Minister, and the court of the place of employment shall have exclusive territorial jurisdiction. The court shall communicate the statement of claim and the final and binding decision adopted on the merits of the case to the President of the Republic as well.

(6c) If, on the basis of the action brought by the president of the Authority in accordance with paragraph (6b), the court finds in its final and binding decision that the motion of the Prime Minister made under paragraphs (3) and (6) is unfounded, the President of the Republic shall not declare the mandate of the president of the Authority to be terminated.

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

a) within fifteen days after the time limit for bringing an action expires if the president of the Authority does not bring an administrative court action,

b) within fifteen days from the receipt of the final and binding decision on the merits of the case if the president of the Authority brings an administrative court action.

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

(8) No counter-signature shall be required for the decisions of the President of the Republic conferred upon him by paragraphs (3) and (6) and by section 40.

Section 45/A The president of the Authority shall have the right to participate in, and voice his opinion at, the committee meetings of the National Assembly.

28. Vice-president of the Authority

Section 46 (1) The president of the Authority shall appoint a vice-president for an indefinite period to assist his work. The president of the Authority shall exercise the employer's rights in respect of the vice-president.

(2) The vice-president shall meet the requirements set out in paragraphs (1) and (2) of section 40 for the appointment of the president of the Authority, with the proviso of having at least five years' experience in auditing procedures related to data protection or freedom of information.

(3) The provisions of section 41 on conflict of interest shall apply to the vice-president as well.

(4) In the event that the president is temporarily prevented from performing his duties, or if the office of the president is vacant, the powers and duties of the president shall be exercised by the vice-president.

Section 47 The provisions of section 42 shall also apply to the obligation of the vice-president to submit the declaration of personal assets, as well as to the related procedure, with the proviso that the president of the Authority shall adjudicate cases related to his declaration of personal assets instead of the Prime Minister, and that the President of the Republic shall not need to be informed of the findings of the procedure.

Section 48 (1) The vice-president shall be entitled to the same remuneration and benefits as those of state secretaries.

(2) The vice-president shall be entitled to forty working days of paid annual leave per calendar year.

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

(4) The term of the mandate of the vice-president shall be recognised as spent in public service at an administrative organ.

Section 49 (1) The mandate of the vice-president of the Authority shall terminate

a) upon his resignation;

b) upon his death;

c) if the conditions required for his appointment are no longer met;

d) upon a conflict of interest being established with regard to him;

e) upon being discharged;

f) upon his removal from office.

(2) The vice-president of the Authority shall be entitled to resign from office at any time by submitting his resignation in writing to the president of the Authority. The mandate of the vice-president of the Authority shall terminate on the day after the date of resignation, as indicated in the resignation or, failing this, on the day when the resignation is submitted. A declaration of acceptance shall not be required for the resignation to take effect.

(3) If the vice-president of the Authority fails to resolve a conflict of interest under section 41 within thirty days from the date of his appointment, or if any cause of conflict of interest arises while he is in office, the president of the Authority shall decide on the issue of establishing a conflict of interests.

(4) The president of the Authority shall discharge the vice-president of the Authority if the vice-president of the Authority is unable to perform his vested duties for a period of over ninety days for reasons beyond his control.

(5) The president of the Authority shall be entitled to discharge the vice-president of the Authority and shall, at the same time, offer a public official employment relationship to the vice-president at the Authority and an investigator's position, even in the absence of the requirements set out in section 51 (1).

(6) The president of the Authority shall remove the vice-president of the Authority from office if the vice-president fails to perform his vested duties for a period of over ninety days for reasons within his control, or if the vice-president has knowingly included false data or facts in his declaration of personal assets.

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

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

29. Staff of the Authority

Section 50 The president of the Authority shall exercise the employer's rights over the public officials and employees of the Authority.

Section 51 (1) The president of the Authority shall be entitled to appoint as investigators up to twenty per cent of all public officials of the Authority, from among those public officials employed by the Authority that have a degree of higher education in information technology or law and at least three years of experience as data protection experts or data protection officers, and who passed the professional examination in public administration or law, or have a specialised qualification in public administration or governmental studies.

(2) Investigators are appointed for an indefinite period of time, and may be discharged by the president of the Authority at any time, without giving the reasons thereof. If the president of the Authority withdraws the appointment of an investigator, the public official shall be reinstated in his last position before his appointment as investigator.

(3) Investigators shall be entitled to the remuneration of a head of unit, reduced by the executive officers' bonus.

CHAPTER VI

PROCEDURES OF THE AUTHORITY

30. Authority inquiries

Section 51/A (1) If commencing an authority procedure is not mandatory according to this Act, the Authority may commence an inquiry *ex officio*.

(2) In the case specified in section 22 *a)*, the data subject may initiate an inquiry with the Authority by submitting a notification thereto. In the notification, the data subject shall indicate the data supporting that he has attempted to enforce his rights under section 14 with the controller.

Section 52 (1) Any person shall have the right to initiate an inquiry with the Authority by submitting a notification of an alleged infringement relating the processing of personal data or concerning the exercise of the right to access data of public interest or data accessible on public interest grounds, or of an imminent threat of such an infringement.

(1a) If the notification is based on a reason specified in section 31 (1), the inquiry of the Authority may be initiated within one year from communicating the dismissal of the request, or from the expiry of the time limit with no result, or from the expiry of the time limit for the payment of the fee.

(2) The inquiry of the Authority shall not qualify as an administrative authority procedure.

(3) Submitting a notification to the Authority shall not give rise to any disadvantages to the notifier. The Authority may only reveal the person of the notifier if the inquiry cannot be carried out otherwise. If so requested by the notifier, the Authority shall not reveal his identity, even if the inquiry cannot be carried out otherwise. The Authority shall inform the notifier of this circumstance.

(4) The inquiry of the Authority shall be free of charge; the costs of the inquiry shall be advanced and borne by the Authority.

Section 53 (1) Subject to the exceptions set out in paragraphs (2) and (3), the Authority shall be obliged to examine the notifications received on their merits.

(2) The Authority may dismiss a notification without examining it on its merits if

a) the infringement alleged in the notification is of minor importance; or

b) the notification is anonymous.

(3) The Authority shall dismiss the notification without examining it on its merits if

a) court proceedings are in progress or a final and binding court decision has previously been rendered in the given case;

b) the notifier maintains his request for his identity not to be revealed, despite the information provided under section 52 (3);

c) the notification is clearly unfounded;

d) the notification has been re-submitted and it contains no new facts or data on its merits;

e) the notification was submitted following the expiry of the time limit referred to in section 52 (1a)

f) the notification does not meet the requirements of section 51/A (2),

g) it carries out an administrative audit or an administrative authority procedure concerning the subject matter of the notification, or

h) the subject matter of the notification does not fall within its material competence, and there is no sufficient information available to determine the competent authority with regard to the subject matter of the notification.

(4) The Authority shall only be allowed to dismiss a notification submitted by the Commissioner for Fundamental Rights without an examination on its merits if court proceedings are in progress or a final and binding court decision has previously been rendered in the given case.

(5) The Authority shall terminate the inquiry if

a) the request should have been dismissed without examination on its merits pursuant to paragraphs (3) to (4), but the Authority obtained information concerning the grounds for dismissal after the inquiry was commenced;

b) the circumstances giving rise to the inquiry no longer exist.

(6) The Authority shall inform the notifier of the dismissal of the notification without an examination on its merits and of the termination of the inquiry, also giving the reasons for dismissal or termination.

(7) The Authority shall transfer a case for which it has no material competence to the competent authority, provided that there is sufficient information available to determine the competent authority; at the same time, the Authority shall inform the notifier of the transfer. If, based on a notification received in a case for which it has no material competence, the Authority comes to the conclusion that the case needs to be brought before a court, it shall inform the notifier of this.

(8) The Authority shall also inform the controller or processor under inquiry of the transfer if it took part in the inquiry.

Section 54 (1) In the course of its inquiry, the Authority

a) shall be given access to, and may make copies of, all data processed by the controller under inquiry that are presumed to relate to the case at hand, and shall have the right of access to, and may request copies of, such documents, including documents stored in an electronic data medium;

b) shall be given access to any data processing operation presumed to relate to the case at hand, shall be authorised to enter any premises where data processing is carried out, and shall have access to any equipment used for the data processing operations;

c) shall have the right to request written or oral information from the controller under inquiry, and from any employee of the controller;

d) shall have the right to request written information from any organisation or person presumed to have any connection with the case at hand and copies of any data and documents, including documents stored in an electronic data medium, presumed to relate to the case at hand; and

e) may request the head of the organ supervising the controller authority to conduct an inquiry.

(2) The controller under inquiry and the organisation or person concerned with regard to the procedural act shall fulfil the request of the Authority made under paragraph (1) within the time limit prescribed by the Authority. The time limit prescribed by the Authority shall not be less than fifteen days in the cases referred to in paragraph (1) *d)* and *e)*.

(3) The person requested to provide information in accordance with paragraph (1) *c)* and *d)* may refuse to fulfil the request if

a) the person affected by the notification providing the basis for the inquiry of the Authority is his relative or former spouse, as defined in the Civil Code;

b) by providing the information he would incriminate himself, or his relative as defined in the Civil Code, or his former spouse of committing a criminal offence with respect to the question related to this.

Section 55 (1) Within two months from commencing *ex officio* the inquiry or the day following receipt of the notification, the Authority

a) shall establish that an infringement relating to the exercise of rights specified in the General Data Protection Regulation or in this Act occurred, or there is an imminent threat of such an infringement, and

aa) shall take the measures specified in sections 56 and 57,

ab) shall conclude the inquiry, and institute an authority procedure for data protection in accordance with section 60, or

ac) shall conclude the inquiry, and institute an authority procedure for the supervision of data classification in accordance with section 62;

b) shall establish that there has been neither an infringement nor the imminent threat of it, and shall conclude the inquiry.

(1a) The following shall not be included in the time limit specified in paragraph (1):

a) the period between the notification requesting the communication of the data necessary for the clarification of the facts and the fulfilment of the request;

b) the time required for having the document related to the inquiry translated; and

c) the duration over which circumstances, other malfunctions or unavoidable events obstruct the operation of the Authority for at least a day.

(2) The Authority shall inform the notifier and, if it took part in the inquiry, the controller or processor under inquiry, of the findings of its inquiry, the reasons for concluding the inquiry, the measures taken, if any, or the commencing of authority procedures.

(3) If the Authority concludes, according to paragraph (1) *b),* its inquiry carried out on the basis of a notification under section 51/A (2), it shall inform the notifier, at the same time as providing the information specified in paragraph (2), of the possibility to exercise the right to legal remedies to which he is entitled.

Section 56 (1) If the Authority finds that there is an infringement relating to the processing of personal data or concerning the exercise of the right to access data of public interest or data accessible on public interest grounds, or that there is an imminent threat of such an infringement, it shall require the controller to remedy the infringement and eliminate the imminent threat of such an infringement.

(2) The controller, if in agreement, shall take the necessary measures indicated in the notice referred to in paragraph (1) without delay, and shall inform the Authority concerning the measures taken, or, if in disagreement, shall inform the Authority of its position in writing within thirty days from receiving the notice.

(3) In the case of a controller authority having a supervisory organ, the Authority, if the notice referred to in paragraph (1) does not produce results, may present a recommendation to the controller's supervisory organ, of which the controller shall be notified simultaneously. The Authority may also present a recommendation directly to the supervisory organ of the controller, without sending a notice to the controller under paragraph (1), if it is of the opinion that this is a more effective way to remedy the infringement and to eliminate the imminent threat of such an infringement.

(4) Within thirty days from receiving the recommendation, the supervisory organ shall inform the Authority in writing with respect to its standpoint on the merits of the recommendation, or the measures it has taken.

Section 57 If, based on the findings of the inquiry, the Authority considers that the infringement or its imminent threat is attributable to an unnecessary, unclear or inadequate provision of law or a public law regulatory instrument, or it can be traced back to the lack or deficiency of legal regulations concerning the issues of data processing, then, in order to prevent future infringements and their imminent threat, the Authority may present recommendations to the organ authorised to adopt such laws or issue such public law regulatory instruments, or to the organ drafting the law. In the recommendation, the Authority may propose to amend, repeal or adopt a law or public law regulatory instrument. The requested organ shall inform the Authority within sixty days of its position, or of the measures taken in conformity with the recommendation.

Section 58 (1) If, after the notice issued or the recommendation presented in accordance with section 56, the infringement has not been remedied or its imminent threat has not been eliminated, the Authority shall decide regarding further necessary measures to be taken within a period of thirty days following the expiry of the time limit for providing information as specified in section 56 (2) or, if a recommendation was presented, in section 56 (4).

(2) If paragraph (1) applies, as further necessary measures, the Authority:

a) shall or may commence an authority procedure for data protection under section 60;

b) shall or may commence an authority procedure for the supervision of data classification under section 62;

c) may institute court proceedings according to section 64; or

d) may draw up a report according to section 59.

(3) The Authority shall inform the notifier of the results of the measures taken under sections 56 and 57, and of further measures taken in accordance with paragraph (2).

31. The report of the Authority

Section 59 (1) If the Authority did not commence an authority procedure or court proceedings, it may draw up a report on the inquiry conducted on the basis of the notification.

(2) The report shall contain the facts revealed during the inquiry, as well as the resulting findings and conclusions.

(3) The report of the Authority shall be public. The president of the Authority shall classify the report if it contains any classified data, or shall confirm its classification status. If the report contains any classified data or any secrets protected by an Act, it shall be published in such a way that the classified data or secrets protected by an Act cannot be accessed.

(4) The report made by the Authority regarding the inquiry of the activities of organs authorised to secret information gathering or to use covert devices shall not contain any data that may suggest that secret gathering of information was conducted or covert devices were used in the given case.

(5) The report of the Authority may not be challenged in court or before any other authority.

32. Authority procedure for data protection

Section 60 (1) To ensure that the right to the protection of personal data is enforced, the Authority shall commence an authority procedure for data protection at the application of the data subject, and may commence an authority procedure for data protection *ex officio*.

(2) An application for commencing an authority procedure for data protection may be submitted in the cases under Article 77 (1) of the General Data Protection Regulation and 22 *b)* of this Act.

(3) The Authority shall commence an authority procedure for data protection *ex officio* if

a) it finds on the basis of its inquiry that an infringement related to the processing of personal data has occurred or there is an imminent threat of such an infringement, and, after the notification issued or the recommendation presented in accordance with section 56, the infringement has not been remedied or its imminent threat has not been eliminated within the time limit specified by the Authority,

b) it finds on the basis of its inquiry that an infringement related to the processing of personal data has occurred or there is an imminent threat of such an infringement, and a fine may be imposed according to the provisions of the General Data Protection Regulation.

(4) If the authority procedure for data protection was preceded by an inquiry of the Authority initiated upon notification, the Authority shall inform the notifier of commencing and concluding the authority procedure for data protection.

(5) In the case specified in paragraph (2), the application shall contain, in addition to the elements specified in the Act on the Code of General Administrative Procedure, the following:

a) the identification of the alleged infringement,

b) the description of the concrete conduct or state resulting in the alleged infringement,

c) the data available to the applicant and necessary for the identification of the controller or processor committing the alleged infringement,

d) the facts that support the statements related to the alleged infringement, as well as the evidences of such facts, and

e) an explicit request to adopt a decision on remedying the indicated infringement.

(6) In the authority procedure for data protection, the applicant shall be entitled to cost exemption, and the Authority shall advance those procedural costs, the advancing of which would be borne by the applicant.

Section 60/A (1) The administrative time limit in authority procedures for data protection shall be one hundred and fifty days.

(2) The Authority shall suspend the authority procedure for data protection for the period of the application of

a) the cooperation procedure referred to in Article 60 (3) to (5) and

b) the consistency mechanism referred to in Articles 63 to 66

of the General Data Protection Regulation, with the proviso that the Authority shall implement the procedural acts necessary in the cooperation procedure and in the consistency mechanism during the period of suspension as well.

(3) If the Authority establishes, in any phase of the procedure launched on application, that it has no jurisdiction, it shall reject the application or terminate the procedure.

(4) If the jurisdiction of the supervisory authority of another EEA State can be established beyond doubt, the Authority shall forward the application to the supervisory authority with jurisdiction. In this case, the decision rejecting the application or terminating the procedure shall also contain the name of this supervisory authority.

(5) After forwarding the application to the supervisory authority with jurisdiction in accordance with the provisions of paragraph (4), at the request of the data subject, the Authority shall provide the data subject with information on how to enforce his rights before the supervisory authority with jurisdiction.

(6) If the Authority does not terminate the authority procedure for data protection or make a decision on the merits of the case within ninety days of the submission of the application, it shall inform the applicant of the procedural acts implemented up to the date of the information.

Section 61 (1) In its decision adopted in authority procedures for data protection, the Authority

a) may apply the legal consequences specified in the General Data Protection Regulation concerning the data processing operations specified in section 2 (2) and (4) of this Act;

b) concerning the data processing operations specified in section 2 (3)

ba) may establish that the processing of personal data was unlawful;

bb) may order the rectification of any personal data that are inaccurate;

bc) may order the blocking, deletion or destruction of personal data subject to unlawful processing;

bd) may prohibit the unlawful processing of personal data;

be) may prohibit the transfer or disclosure of personal data to foreign countries;

bf) may order the provision of information to the data subject if the controller has refused to do so unlawfully; and

bg) may impose a fine,

c) may apply the legal consequences specified in Article 41 (5) of the General Data Protection Regulation against bodies carrying out the monitoring under Article 41 (1) of the General Data Protection Regulation.

(2) The Authority may order the publication of its decision so as to include the identification data of the controller or processor as well if

a) the decision concerns a wide range of persons,

b) the decision was adopted in connection with the activities of an organ performing public duties, or

c) the gravity of the infringement justifies publication.

(3) No warnings shall be issued and no security shall be required in procedures of the Authority where it establishes, applying the provisions relating to its discretionary power, that a fine needs to be imposed.

(4) The amount of the fine shall be between one hundred thousand and twenty million forints if the fine is imposed

a) pursuant to paragraph (1) *b) bg)*, or

b) pursuant to Article 83 of the General Data Protection Regulation and the party required to pay the fine imposed in a decision adopted in accordance with an authority procedure for data protection is a budgetary organ.

(5) In deciding whether it is justified to impose a fine pursuant to paragraph (1) *b) bg)*, and in determining the amount of the fine, the Authority shall take all circumstances of the case into account, in particular the number of data subjects affected by the infringement, the gravity of the infringement, the fault, and whether the infringing party was previously found to have committed an infringement concerning the processing of personal data.

(6) Prior to the expiry of the time limit for bringing an action to challenge the decision, or, in the event of bringing an administrative court action, until the final and binding decision of the court is adopted, the data affected by the processing operation in dispute shall not be erased or destroyed.

(7) The execution of the Authority's decision shall be carried out by the Authority with regard to the obligation of performing a specific act, specific conduct, tolerating or ceasing.

(8) The payment obligation set forth in the Authority's decision may not be mitigated at the request of the obligor (hereinafter "mitigation"). The obligor may request a deferral or performance in instalments of the payment obligation or the obligation specified in paragraph (7) (hereinafter "performance concession"). The obligor shall verify in his request that a cause beyond his control makes it impossible for him to perform in due time, or that it would be disproportionately burdensome for him.

(9) If the request under paragraph (8) is submitted by the obligor after ordering the execution of the Authority's decision, the Authority shall only allow a performance concession when a cause beyond the obligor's control has prevented the performance of the obligation in due time.

(10) In the course of assessing requests regarding the mitigation of the payment obligation established in the Authority's decision or a performance concession, the state tax and customs authority shall proceed with the application of section 110 of Act CLIII of 2017 on the enforcement measures executable by the tax authority.

33. Authority procedure for the supervision of data classification

Section 62 (1) If the findings of an inquiry or other evidence substantiate that the classification of certain national classified data is unlawful, the Authority may commence an authority procedure for the supervision of data classification.

(1a) If the court initiates an authority procedure for the supervision of data classification on the basis of section 31 (6a) to be launched by the Authority, the Authority shall commence an authority procedure for the supervision of data classification.

(1b) The authority procedure for the supervision of data classification by the Authority shall not affect the duties of the National Security Authority as specified in the Act on the protection of classified data.

(2)

(2a) In authority procedures for the supervision of data classification and in court actions initiated for contesting the decision adopted in such procedures, classified data shall be treated in accordance with the security requirements set forth in the Act on the protection of classified data and this Act.

(3) Authority procedures for the supervision of data classification shall only be commenced *ex officio*, and shall not be deemed to have been commenced upon application, even if the authority procedures for the supervision of data classification were preceded by the inquiry of the Authority initiated upon notification, or if such procedures were initiated by the court on the basis of section 31 (6a). If, however, the Authority has conducted an inquiry initiated upon notification prior to the authority procedure for the supervision of data classification, the notifier shall be informed of the commencement and conclusion of the procedure.

(4) In authority procedures for the supervision of data classification, the classifier shall be a party.

(5) During the clarification of the facts in authority procedures for the supervision of data classification, the witness, the expert and the holder of the object of the on-site inspection may be heard, even if these persons have not been exempted from the secrecy obligation with respect to the national classified data under examination.

(6) The administrative time limit in authority procedures for the supervision of data classification shall be ninety days.

Section 63 (1) In its decision adopted in authority procedures for the supervision of data classification, the Authority shall

a) in the event of any infringement of the laws pertaining to the classification of certain national classified data, require the classifier to modify, in accordance with the law, the level or term of the national classified data, or to have it declassified, or

b) establish that the classifier proceeded in accordance with the laws on the classification of national classified data.

(2) If the classifier finds the decision of the Authority under paragraph (1) *a)* unsubstantiated, it may contest it within sixty days following the date of communicating the decision. The submission of the statement of claim contesting the decision shall have suspensive effect on the entry into force of the decision. If the classifier does not turn to the court within sixty days of the communication of the decision, the classification of the national classified data shall cease on the sixty-first day following the communication of the decision, or the level or term of classification shall be modified in accordance with the decision.

(2a)

(3) The court shall hold a closed hearing in an action specified in paragraph (2).

(4)

(5) The decision of the court or Authority shall not affect the obligation of the classifier with respect to the review of classified national data under the Act on the protection of classified data.

(6) The judge proceeding in such action shall hold a security clearance in accordance with the Act on national security agencies.

(7) In the course of court actions specified in paragraph (2), persons other than the judge, the plaintiff and the defendant shall be allowed access to the classified data only if they hold a personal security clearance certificate of the same level as the classification of the classified data.

34. Court action brought by the Authority

Section 64 (1) If the controller fails to comply with the notice issued under section 56 (1), the Authority may bring an action before the court, due to the infringement in connection with data of public interest and data accessible on public interest grounds, within thirty days following the date of expiry of the time limit for providing the information under section 56 (2), and seek the decision of the court to order the controller to act in accordance with the notice issued by the Authority.

(2) The material and territorial jurisdiction of the court shall be established according to section 31 (5).

(3) The burden of proof evidencing that data processing is in compliance with the law shall lie with the controller.

(4) Any person who does not otherwise have the capacity to be a party may also be a party to such a court action.

(5) The court, upon request, may order the publication of its judgment, including the identification data of the controller, if it is necessary in the interests of data protection and the freedom of information, or in connection with the rights of a larger number of data subjects under protection according to this Act.

34/A. Procedure for the authorisation of data processing

Section 64/A (1) The Authority shall conduct a procedure for the authorisation of data processing if an application

a) for the approval of the draft, extension or amendment of the codes of conduct referred to in Article 40;

b) for the authorisation of the monitoring activity referred to in Article 41;

c) for the approval of the certification criteria referred to in Article 42 (5);

d) for the authorisation of the contractual clauses referred to in Article 46 (3) (a);

e) for the authorisation of the provisions referred to in Article 46 (3) (b);

f) for the approval of the binding corporate rules referred to in Article 47

of the General Data Protection Regulation is submitted.

(2) In addition to the provisions laid down in the Code of General Administrative Procedure, the application referred to in

a) paragraph (1) *a)* shall contain the draft code of conduct, the extension or the amendment;

b) paragraph (1) *b)* shall contain the data demonstrating that the conditions specified in Article 41 (2) of the General Data Protection Regulation and in the authorisation requirements issued by the Authority are complied with;

c) paragraph (1) *c)* shall contain a general description of the certification mechanism and the draft certification criteria;

d) paragraph (1) *d)* shall contain the draft contractual clauses;

e) paragraph (1) *e)* shall contain the draft provisions;

f) paragraph (1) *f)* shall contain the data demonstrating the binding nature of the binding corporate rules and the draft binding corporate rules.

Section 64/B An administrative service fee, as determined in a ministerial decree, shall be paid for a procedure for the authorisation of data processing.

Section 64/C (1) The administrative time limit in authority procedures for the authorisation of data processing shall be

a) one hundred and eighty days for applications referred to in section 64/A (1) *a)* to *c)* and *f)*;

b) ninety days for applications referred to in section 64/A (1) *d)* and *e)*.

(2) The Authority shall suspend the authority procedures for the authorisation of data processing for the period of the application of

a) the cooperation procedure referred to in Article 60 (3) to (5) and

b) the consistency mechanism referred to in Articles 63 to 66

of the General Data Protection Regulation, with the proviso that the Authority shall implement the procedural acts necessary in the cooperation procedure and in the consistency mechanism also during the period of suspension

(3) Where an application referred to in section 64/A (1) *a)* to *c)* and *f)* is submitted, the Authority, in the authority procedure for the authorisation of data processing, may invite the applicant, on as many occasions as necessary, to make a statement with respect to amending or supplementing the application or the drafts included in it so that approval or authorisation can be granted.

(4) No summary procedure shall be allowed in procedures for the authorisation of data processing.

Section 64/D In its decision adopted in a procedure for the authorisation of data processing, the Authority

a) shall

aa) approve the draft code of conduct, the extension or the amendment referred to in Article 40;

ab) authorise the monitoring activity referred to in Article 41;

ac) approve the certification criteria referred to in Article 42 (5);

ad) authorise the application of the contractual clauses referred to in Article 46 (3) (a);

ae) authorise the application of the provisions referred to in Article 46 (3) (b);

af) approve the binding corporate rules referred to in Article 47

of the General Data Protection Regulation, or

b) shall dismiss the application.

35. International cooperation

Section 65 (1) The Authority shall cooperate with the authorities of third countries and with international organisations, in particular as laid down and in the manner prescribed in Article 50 of the General Data Protection Regulation and in Article 40 of Directive (EU) 2016/680.

(2) In the framework of the cooperation set forth in paragraph (1), the Authority may approach the authority of a third country or an international organisation with a request for legal assistance, and, with the exception laid down in section 67, it shall perform the requests for legal assistance received from the authority of a third country or an international organisation, if that it is allowed under an administrative legal assistance treaty between the third country or the international organisation and Hungary, another international treaty, laws or a legal act of the European Union.

Section 66 The Authority shall refuse to perform a request for legal assistance received from the authority of a third country or an international organisation and it shall provide the authority of the third country or the international organisation with information on the reasons of the refusal if performing the request for legal assistance

a) is beyond its tasks and powers,

b) would impair the national security interests or the public safety of Hungary,

c) would impair the fundamental right of the person affected in the case, or

d) would be against the law.

Section 67 (1) The Authority shall cooperate with the supervisory authorities of EEA States in the manners prescribed in a binding legal act of the European Union, in particular in the

framework of mutual assistance as laid down, and in the manner prescribed, in Article 61 of the General Data Protection Regulation and in Article 50 of Directive (EU) 2016/680.

(2) In the manner prescribed in Article 62 of the General Data Protection Regulation, in the course of joint operations with the supervisory authority of an EEA State,

a) the public servant staff member of the Authority designated by the president of the Authority for contributing to a joint operation shall contribute to exercising, in the territory of another EEA State, the tasks and powers transferred by the supervisory authority of the other EEA State, and

b) the person acting within the tasks and powers of the supervisory authority of another EEA State and designated by that supervisory authority shall contribute to exercising, in the territory of Hungary, the tasks and powers of the Authority to the extent specified in writing by the president of the Authority.

(3) The person specified in paragraph (2) *b)* shall act according to the law of Hungary.

Section 68 If data or documents need to be acquired or other procedural acts need to be carried out for performing a request, not directly linked to a procedure pending at the Authority, received from the authority of a third country or of an EEA State or from an international organisation, the Authority shall conduct an administrative audit for this purpose. In this event, the audit shall be concluded by the Authority's ruling on transferring the pieces of evidence acquired.

36. Certification

Section 69 (1) The Authority shall conduct the certification specified in Article 42 of the General Data Protection Regulation at the initiative of the controller or the processor, on the basis of an agreement concluded with the controller or the processor.

(2) The Authority shall publish the conditions of concluding the agreement on the certification and the consideration to be provided for the certification, as well as the process of carrying out the certification and the criteria for certification.

(3) The Authority shall determine, proportionately to the activity to be performed, the conditions of concluding the agreement on the certification and the consideration to be provided. The consideration to be provided for carrying out the certification shall be the revenue of the Authority.

(4) If the Authority issues a certification or a European Data Protection Seal on the certification, it shall publish

a) the name of the controller and/or processor entitled to use it, and

b) the processing operations covered by the certification or the European Data Protection Seal.

37. Initiating criminal, infraction and disciplinary proceedings

Section 70 (1) In the event that, in the course of its procedures, the Authority has a well-founded suspicion of a criminal offence, it shall initiate criminal proceedings before the organ entitled to commence criminal proceedings. If, in the course of its procedures, the Authority has a well-founded suspicion of an infraction or a disciplinary offence, it shall initiate infraction or disciplinary proceedings before the organ entitled to conduct infraction or disciplinary proceedings.

(2) The organ referred to in paragraph (1) shall inform the Authority of its opinion with respect to commencing the proceedings within thirty days, unless otherwise provided by an Act and, with respect to the outcome of the proceedings, within thirty days from the time of concluding the proceedings.

38. Other regulations applicable to the procedures of the Authority, data processing and confidentiality

Section 70/A (1) No administrative audit shall be carried out at the request of the controller or the processor.

(2) The controller or the processor shall prove that the processing complies with the provisions pertaining to the processing of personal data as laid down by law or a binding legal act of the European Union, in particular with the fundamental requirements specified in section 4 (1) to (4a) with regard to processing operations under section 2 (3).

Section 70/B (1) For the purpose of keeping data subjects and controllers informed, the Authority shall publish

a) according to the decisions published under section 61 (2),

aa) the identification data of the controller or the processor,

ab) the designation of the infringement,

ac) the designation of the legal consequence applied,

b) according to the decisions specified in section 64/D *a)*,

ba) the identification data of the applicant,

bb) the designation of the subject of the Authority's decision,

bc) if the Authority's decision is in force for a definite period of time, the designation of the temporal effect of the decision,

c) concerning the data protection officer notified to the Authority,

ca) his name,

cb) his postal and electronic mailing address,

cc) the name of the controller or the processor he represents.

(2) The data under paragraph (1) are data accessible on public interest grounds.

(3) The Authority shall publish

a) the data specified in paragraph (1) *a) aa)* until the date of the decision losing force, or

ab) upon the expiry of ten years after issuing the decision,

b) the data specified in paragraph (1) *b),* until the date of the decision losing force,

c) the data specified in paragraph (1) *c),* until the change of the data is notified.

Section 70/C Access to data, to be disclosed or published by the Authority according to a binding legal act of the European Union or this Act, shall be made available to the general public on the Authority's own website without any restriction, in digital format, without personal identification, and in a format capable of being printed or copied without any partial loss or distortion of data, free of charge, including accessing, downloading, printing, copying and transmitting through a network.

Section 71 (1) In the course of its procedure, the Authority shall be entitled to process, to the extent and for the duration necessary for the procedure, personal data, as well as data that qualify as secrets protected by an Act and secrets obtained in the course of professional activities, which are related to the given procedure or which have to be processed for the purpose of concluding the procedure effectively.

(1a) If the controller lawfully restricts or it is entitled to restrict, on the basis of an Act or a binding legal act of the European Union, the rights to which the data subject is entitled according to the provisions under Articles 13 to 18 and 21 of the General Data Protection Regulation and under section 14 of this Act, the Authority shall, in the context of its procedures,

a) ensure the data subject's rights in a manner and at a time, and

b) perform the mandatory notifications of the data subject specified in this Act as the obligation of the Authority in a manner and at a time,

guaranteeing that the interest that may serve as a basis of lawfully restricting the data subject's rights shall not be impaired.

(1b) At the request of the Authority, the local government clerk shall review the actual circumstances of data processing carried out in the area of its territorial competence as indicated by the Authority in its request, in particular the scope of the processed personal data, the operations carried out with personal data and the means used for these operations, as well as the technical and organisational measures applied by the processor.

(2) The Authority may use the documents, data or other tools of evidence acquired lawfully during its procedures in other procedures it conducts.

(2a) For documents drawn up for defence purposes, the provisions of paragraphs (1) and (2) shall apply with the derogations set out in the Act on the professional activities of attorneys-at-law.

(2b) The personal data and the protected data processed by the Authority during an inquiry or procedure shall be blocked after closing the inquiry or after the decision closing the authority procedure has reached administrative finality. Blocked data may be retained until the disposal of the documents of the case subject to the procedure or until handing them over to the archives for preservation; such documents, with the exception of the use according to paragraph (2), may only be processed for the purpose of executing the decision with administrative finality, monitoring the implementation of the decision, providing legal remedy or decision review related to the decision with administrative finality, and they shall only be made accessible to the court, other organ or person entitled to process or have access to such data, in the manner and in the scope specified in an Act.

(3) In its procedures, the Authority shall have access to the data specified in section 23 (1) *a)* to *f)* and *i),* (2), (3) *c)* to *f),* (4) *c)* to *g)* and (5) *d)* of Act CXI of 2011 on the Commissioner for Fundamental Rights (hereinafter the "Ajbtv.") in accordance with section 23 (7) of the Ajbtv.

(3a) Irrespective of paragraph (3), the Authority shall have access to the data specified in section 23 (3) *e),* (4) *f)*, and (5) *d)* of the Ajbtv. if it is necessary in the following procedures commenced in connection with the protection of the participating person's personal rights:

a) in inquiries,

b) in authority procedures for data protection, or

c) in authority procedures for the supervision of data classification.

(3b) Irrespective of paragraph (3), the Authority shall have access to the data specified in section 23 (3) *f)* and (4) *g)* of the Ajbtv. which allow the identification of persons using devices and methods for secret information gathering or covert devices if it is necessary in the following procedures initiated for the protection of the personal data of these persons:

a) in inquiries,

b) in authority procedures for data protection, or

c) in authority procedures for the supervision of data classification.

(3c) If the document to be examined by the Authority contains data which may be accessed by the Authority only in accordance with paragraph (3), access to the document shall be granted to the Authority by making the non-accessible data unrecognisable.

(4) In procedures related to the processing of classified data, the vice-president of the Authority and the public officials acting as executive officers, as well as the investigators, shall, if they possess a personal security certificate with the appropriate level of clearance, be entitled to access classified data, even without the authorisation for use set forth in the Act on the protection of classified data.

(5) During the term of their legal relationship and also following its termination, the president and the vice-president of the Authority, as well as persons currently or formerly employed in a public service relationship or other employment relationship by the Authority, shall keep any personal data, classified data, secrets protected by an Act, and secrets obtained in the course of professional activities they may have learnt in connection with the operation and activities of the Authority, as well as any other data, fact or circumstance that the Authority is not obliged by virtue of an Act to publish, except for any publication or provision of data to other organisations prescribed by an Act, as confidential.

(6) In accordance with the confidentiality obligation, the persons mentioned in paragraph (5) shall not disclose unlawfully any data, fact or circumstance of which they obtained knowledge during the performance of their duties, and they shall not be allowed to use such information or reveal it to third parties.

CHAPTER VI/A

SUPERVISION OF DATA PROCESSING OPERATIONS BY COURTS

Section 71/A (1) In contentious and non-contentious proceedings aimed at adopting a judicial decision (hereinafter "basic case"), the supervision of the enforcement of the right to the protection of personal data in the context of data processing operations carried out by the courts in accordance with the relevant provisions shall take place through data protection complaints (hereinafter "complaint").

(2) The complaint shall be judged upon, in accordance with the procedural rules applicable to the basic case, according to

a) section 143 (3) and section 144 (3) and (8) *a)* of Act XC of 2017 on the Code of Criminal Procedure if the rules of criminal or infraction proceedings are applicable to the basic case,

b) section 36 (2) of Act I of 2017 on the Code of Administrative Court Procedure with regard to section 157 (3) and section 158 (3) and (6) of Act CXXX of 2016 on the Code of Civil Procedure if the rules of the administrative court procedure are applicable to the basic case,

c) section 157 (3) and section 158 (3) and (6) of Act CXXX of 2016 on the Code of Civil Procedure or, if Act III of 1952 on the Code of Civil Procedure (hereinafter "Pp. of 1952") is applicable in the basic case, sections 114/A (4) and 114/B (3) and (6) of the Pp. of 1952, in the cases not falling under points *a)* and *b),*

with the derogations laid down in this Chapter.

(3) The complaint may be filed with the court proceeding in the basic case in writing, addressed to the court with material jurisdiction to decide on the complaint.

(4) The complaint may be filed by the party, the accused party and by other participants of the proceedings, in particular by the aggrieved party, the private party, the witness and the expert, as well as by the person who substantiates his legal interest upon filing the complaint.

Section 71/B (1) The court shall examine, on the basis of the complaint, whether the judge, the lay judge or the judicial employee complied, in the course of his processing activity, with the provisions of the laws and of Union law on the protection of personal data.

(2) The data subject may file a complaint by referring to

a) an infringement, or the imminent threat of it, related to the processing of his personal data, or

b) the unlawful conduct of the controller performed in the course of the enforcement of the data subject's rights specified in the General Data Protection Regulation and in section 14 of this Act.

(3) In the complaint under paragraph (2) *b),* the data subject shall indicate the data supporting that he has made an attempt to enforce the data subject's rights with the controller.

(4) On the basis of the complaint, the court proceeding in the basic case, if it finds the complaint justified, shall take, within eight days, the necessary measures to mitigate the consequences of the infringement or to eliminate the threat of the infringement, and at the same time it shall notify the complaining party thereof and of the measures taken, also providing him with information on the possibility of submitting in writing his statement thereon within eight days from the receipt of the notification if he maintains the complaint despite the measures taken.

(5) If the court proceeding in the basic case has not taken any measure referred to in paragraph (4), or if the data subject submitted a statement specified in paragraph (4), the court proceeding in the basic case shall, for the purpose of deciding on the complaint, submit the necessary documents, including its statement on the complaint, to the court with material jurisdiction to decide on the complaint within eight days.

(6) A complaint submitted in the course of the proceedings shall be decided on its merits, even if the contentious or non-contentious proceedings are concluded in the meantime.

Section 71/C (1) The court deciding on the complaint shall, with a reasoned decision,

a) reject the complaint in the cases under section 53 (2) and section 53 (3) *a)* to *d)*, and (4),

b) dismiss the complaint if the complaint should have been rejected on the basis of point *a)*, but the court only acquired knowledge of the cause of rejection after starting to examine the merits of the case.

(2) The court deciding on the complaint shall, unless rejecting or dismissing the complaint according to paragraph (1), with a reasoned decision delivered within two months from the date of submitting the complaint and the necessary documents of the case to the court,

a) establish that the processing of personal data was unlawful or an infringement relating to the exercise of the data subjects' rights specified in the General Data Protection Regulation or in this Act occurred,

b) establish the circumstances under point *a),* or their imminent threat, and

ba) shall order the termination of the unlawful processing operation or the elimination of the imminent threat of unlawful processing, or the restitution of the lawfulness of processing,

bb) shall order the implementation of measures by the controller that serve the purpose of enforcing the data subjects' rights granted in the General Data Protection Regulation or in this Act, or

c) shall establish that there has been neither an infringement nor the imminent threat of it, and dismiss the complaint.

(3) The court proceeding in the basic case and the court deciding on the complaint may, in its procedure related to the complaint, request the opinion of the Authority in the interest of the consistent application of the provisions on the protection of personal data.

(4) The following shall not be included in the time limit open for the court to proceed with the complaint:

a) the period between the notifications requesting the communication of the data necessary for the clarification of the factual situation and the opinion of the Authority according to paragraph (3) and its fulfilment;

b) the time required for having the document related to the proceedings translated; and

c) the day when circumstances, another malfunction or an unavertable event obstruct the operation of the court for at least four hours.

(5) The provisions of section 52 (3) and (4), section 53 (1) and (7), as well as of section 54 (1) *a)* to *d)*, and (2) and (3), shall apply with regard to the questions not regulated in this Chapter to the procedure of the court deciding on the complaint.

CHAPTER VII

FINAL PROVISIONS

Section 72 (1) The Government shall be authorised to determine in a decree

a) the detailed rules for the electronic publication of data of public interest;

b) the amount of the fee payable in connection with requests for data of public interest, and the highest amount that can be determined pursuant to section 29 (4);

c) the compilation of sector-specific publication schemes;

d) the contents of the integrated retrieval system for public data and the central register, and the rules for data integration;

e) the scope of data to be published by the national security services, after seeking the opinion of the Authority.

(2) The minister

a) vested with the relevant functions shall be authorised to determine in a decree special sector-specific publication schemes with respect to organs he controls or supervises,

b) responsible for e-administration shall be authorised to determine in a decree the templates for the standard forms to be used for the publication of data contained in the publication schemes,

c)

(3) The minister responsible for justice shall be authorised to determine in a decree, after seeking the opinion of the Authority and in agreement with the minister responsible for taxation, the amount of the administrative service fee payable for procedures for the authorisation of data processing, as well as the detailed rules concerning collecting, managing, registering and refunding such fees.

Section 73 (1) With the exceptions specified in paragraphs (2) and (3), this Act shall enter into force on the day following its promulgation.

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

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

Section 73/A (1) Section 26 (2) and section 30 (7) of this Act as established by Act XCI of 2013 amending Act CXII of 2011 on the right to informational self-determination and on the freedom of information shall apply to procedures pending at the time of the entry into force of Act XCI of 2013 amending Act CXII of 2011 on the right to informational self-determination and on the freedom of information.

Section 74 The Prime Minister shall present a recommendation to the President of the Republic with regard to the first president of the Authority by 15 November 2011. The President of the Republic shall appoint the first president of the Authority effective as of 1 January 2012.

Section 75 (1) The Authority shall proceed in accordance with the provisions of this Act in pending cases based on a submission filed to the Commissioner for Data Protection before 1 January 2012.

(2) As of 1 January 2012, data that were processed within the functions of the Commissioner for Data Protection before 1 January 2012 shall be processed by the Authority.

(3) Concerning processing operations started prior to 25 May 2018, the periodic review specified in section 5 (5) shall be implemented until 25 May 2021.

(4) Inquiries and authority procedures for data protection launched by the Authority before the entry into force of Act XXXVIII of 2018 on amending in the context of the data protection

reform of the European Union Act CXII of 2011 on the right to informational self-determination and on freedom of information and on amending other connected Acts (hereinafter the " Amending Act") shall be carried out by the Authority with the application of the provisions of Chapter VI in force on the day preceding the day of entry into force of the Amending Act.

(5) The data processed in the data protection register prior to the entry into force of the Amending Act shall be blocked by the Authority and it may only use them in a procedure launched in relation to processing operations carried out prior to the entry into force of the Amending Act.

(6) The controller shall be exempted until 31 December 2022 from the application of the provisions laid down in section 25/F (1) if it substantiates that the application of the provisions specified in section 25/F (1) with regard to the automated processing system complying with the requirements specified in Article 63 (2) of the Directive (EU) 2016/680 and used for the processing operations carried out by the controller or by the processor acting on behalf of, or instructed by, the controller would entail disproportionate difficulties or costs.

Section 75/A The Authority shall exercise its powers specified in Article 83 (2) to (6) of the General Data Protection Regulation according to the principle of proportionality, in particular by primarily issuing, in compliance with Article 58 of the General Data Protection Regulation, a warning to the controller or processor for the purpose of remedying the infringement when the provisions, laid down by law or a binding legal act of the European Union, on the processing of personal data are first infringed.

Section 76 Chapter V of this Act qualifies as cardinal on the basis of Article VI (3) of the Fundamental Law.

Section 77 This Act serves the purpose of compliance with the following legal acts of the European Union:

a)

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;

e) Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013 amending Directive 2003/98/EC on the re-use of public sector information.

Section 77/A Chapters III to V and VI/A, section 3 points 3., 4., 6., 11., 12., 13., 16., 17., 21., 23. to 24., section 4 (5), section 5 (3) to (5), (7) and (8), section 13 (2), section 23, section 25, section 25/G (3), (4) and (6), section 25/H (2), section 25/M (2), section 25/N, section 51/A (1), sections 52 to 54, section 55 (1) and (2), sections 56 to 60, section 60/A (1) to (3) and (6), section 61 (1) *a)* and *c)*, section 61 (2) and (3), (4) *b)* and (6) to (10), sections 62 to 71, section 72, section 75 (1) to (5) and Annex 1 contain provisions for the implementation of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Section 78 (1) to (2)

(3) to (9)

Sections 79 to **89**

Annex 1 to Act CXII of 2011

GENERAL PUBLICATION SCHEMES

I. Organisational and staff information

	Data	Updating	Storing
1	Official name, seat, postal address, telephone and fax number, electronic mail address, website and customer service contact information of the organ performing public duties	Immediately upon the change taking effect	Previous data to be erased
2	Organisational structure of the organ performing public duties, showing the departments, and the tasks and duties of each department	Immediately upon the change taking effect	Previous data to be erased
3	Name and title of the executive officers of the organ performing public duties, as well as the executive officers for each of its departments, including contact information (telephone and fax number, electronic mail address)	Immediately upon the change taking effect	Previous data to be erased
4	Name of the head of customer relations within the organisation, including contact information (telephone and fax number, electronic mail address) and customer service hours	Immediately upon the change taking effect	Previous data to be erased
5	With respect to collegiate organs, the number of members and the composition, name, title and contact information of the members	Immediately upon the change taking effect	Previous data to be erased
6	Name of any other organ performing public duties under the control, supervision or oversight of, or subordinated to the organ performing public duties, including the data specified in Point 1	Immediately upon the change taking effect	Previous data to be archived for a period of 1 year
7	Name, seat and contact information (postal address, telephone and fax number, electronic mail address) of any economic operator in which the organ performing public duties has a majority ownership share, or participates in its operations, including scope of activities, name of its representative and the percentage of shares owned by the organ performing public duties	Immediately upon the change taking effect	Previous data to be archived for a period of 1 year
8	Name, seat and contact information (postal address, telephone and fax number, electronic mail address) of any public foundation established by the organ performing public duties, including the instrument of incorporation and the members of the managing organ	Immediately upon the change taking effect	Previous data to be archived for a period of 1 year
9	Name and seat of any budgetary organ founded by the organ performing public duties, reference to the law or resolution based on which the budgetary organ is founded, instrument of incorporation, head of the budgetary organ, website address, operating permit	Immediately upon the change taking effect	Previous data to be archived for a period of 1 year

10	Name of any newspaper founded by the organ performing public duties, editor's and publisher's name and address, name of the editor-in-chief	Immediately upon the change taking effect	Previous data to be archived for a period of 1 year
11	Data specified in Point 1 related to the superior or supervisory organ of the organ performing public duties, or the organ authorised to hear appeals relating to its authority decisions, or failing this, of the organ exercising legal supervision over the organ performing public duties	Immediately upon the change taking effect	Previous data to be archived for a period of 1 year

II. Data related to activities and operations

	Data	Updating	Storing
1	Unabridged and effective text of the laws governing the responsibilities, material competence and main activity of the organ performing public duties, public law regulatory instruments, organisational and operational rules or operating procedures, data protection and data security rules	Immediately upon the change taking effect	Previous data to be archived for a period of 1 year
2	In connection with organs of national territorial competence and capital and county government offices, a prospectus in Hungarian and English on the duties and activities of the organ performing public duties	Immediately on the change taking effect	Previous data to be deleted
3	Tasks voluntarily undertaken by local governments	Quarterly	Previous data to be archived for a period of 1 year
4	With regard to public administration, local government and other authority cases, name of the organ having material competence separately for each type of case and procedure, or the name and area of territorial competence of the organ actually proceeding, if powers have been transferred, description of documents and other deeds required, procedural fees (administrative service fees), basic procedural rules, means (place and time) for the submission of documents for the commencing of procedures, customer service hours, administrative time limits (time limits for processing and for appeals), guidelines, general information on handling cases and standard forms for downloading, access to electronic programmes available for use, appointments, list of legislation for different types of cases, information on clients' rights and obligations	Immediately upon the change taking effect	Previous data to be erased
5	Description and contents of public services rendered by the organ performing public duties or financed from	Immediately upon the change	Previous data to be

	budget, rules of access to public services, amount of fees payable for public services, any allowances from such fees	taking effect	archived for a period of 1 year
6	Descriptive information on databases and registers maintained by the organ performing public duties (name, format, purpose and legal basis of processing, duration of processing, data subjects involved, sources of data, questionnaire, if applicable), data for the identification of records to be registered in the data protection register; type of data collected and technically processed by the organ performing public duties within the framework of its main activity, means of access, costs of making copies	Immediately upon the change taking effect	Previous data to be archived for a period of 1 year
7	Title and subject of publications of the organ performing public duties, means of access, free availability or price of the publication	Quarterly	Previous data to be archived for a period of 1 year
8	With respect to collegiate organs, the decision-making process, means of participation by the general public (providing opinion), procedural rules, place and time of meetings of the collegiate organ, publicity, decisions, minutes or summaries of meetings; information on voting in the collegiate organ, if this is not restricted by an Act	Immediately upon the change taking effect	Previous data to be archived for a period of 1 year
9	Draft laws and related documents to be published by virtue of an Act; proposals submitted to local government representative bodies from the time of submission	Unless otherwise provided by an Act, immediately from the time of submission	Previous data to be archived for a period of 1 year
10	Public announcements and statements made by the organ performing public duties	Continuously	Archived for a period of at least 1 year
11	Technical description of tenders published by the organ performing public duties, the outcome of such procedure and the reasoning	Continuously	Previous data to be archived for a period of 1 year
12	Public findings of examinations and inspections carried out in connection with the main activity of the organ performing public duties	Immediately upon receiving the report on the examination	Previous data to be archived for a period of 1 year
13	Procedure for handling requests for access to data of	Quarterly	Previous

	public interest, name and contact information of the competent department, the person responsible for information rights		data to be erased
14	Results of collecting statistical information relating to the activity of the organ performing public duties, showing changes over time thereof	Quarterly	To be archived for a period of at least 1 year
15	Data on the organ concerned resulting from the mandatory provision of statistical information in connection with data of public interest	Quarterly	To be archived for a period of at least 1 year
16	List of contracts for the use of data of public interest to which the organ performing public duties is a party	Quarterly	To be archived for a period of at least 1 year
17	Standard contract terms related to the use of data of public interest processed by the organ performing public duties	Immediately upon the change taking effect	To be archived for a period of at least 1 year
18	Sector-specific and organ-specific publication schemes related to the organ performing public duties	Immediately upon the change taking effect	Previous data to be erased
19	The list of public cultural data intended for re-use in accordance with the Act on the re-use of public sector information and processed by the organ performing public duties, with indication to their available format, furthermore, the provision of information on the type of public sector information allowed to be re-used in accordance with the Act on the re-use of public sector information and processed by the organ performing public duties, with indication to their available format.	Within 15 days from the changes taking effect	To be archived for a period of at least 1 year
20	Standard contract terms related to the re-use of public data and public cultural data defined in Point 19 in an electronically editable form	Within 15 days from the changes taking effect	Previous data to be erased
21	Schedule of fees to be paid for making available public data and public cultural data defined in Point 19 for the purpose of re-use, with the individual items of the fees	Within 15 days from the changes taking effect	Previous data to be erased
22	Information on the available legal remedies in accordance with the Act on the re-use of public sector information	Within 15 days from the changes taking effect	Previous data to be erased
23	Indication of the parties to the exclusive arrangements	Within 15 days	Previous

	concluded by the organ performing public duties in accordance with the Act on the re-use of public sector information, the duration and subject of the exclusive rights, and other important elements of the arrangements	from the changes taking effect	data to be erased
24	Text of exclusive arrangements on the digitalisation of cultural public data concluded by the organ performing public duties in accordance with the Act on the re-use of public sector information data	Within 15 days from the changes taking effect	Previous data to be erased
25	As defined in the Act on the re-use of public data, the law,, the public law regulatory instrument, the contract for public service, or other binding document (or reference whereby it can be accessed), that require the organ performing public duties to generate sufficient revenue to cover a substantial part of the costs relating to the collection, production, technical processing and dissemination of public data that can be made available for the purposes of re-use	Within 15 days from the changes taking effect	Previous data to be erased

III. Financial management data

	Description of data	Updating	Storing
1	Annual (fiscal) budget of the organ performing public duties, annual accounts under the Act on accounting or the annual budget report	Immediately upon the change taking effect	For 10 years following the time of publication
2	Consolidated data on the staff of the organ performing public duties, including personal benefits provided, and the remuneration, salary and regular benefits of executive officers and other executives, in total, including their expense accounts, description and amounts of benefits provided to other employees	Quarterly	For the time period defined by a specific law, but archived for at least 1 year
3	Data related to the names of beneficiaries to whom the organ performing public duties provided any central subsidies, the purpose and the amount of the support, showing also the place of implementation of the support program, except if the central subsidies are withdrawn before the time of publication, or if the beneficiary declined to accept	By the sixtieth day following the date of the decision	For 5 years following the time of publication
4	Description of contracts relating to the allocation of public funds, management of public assets concerning the purchases of supplies and services, and work contracts worth 5 million forints or more, or to the sale or utilisation of assets, for the transfer of assets or rights, as well as concession contracts, including the type and	By the sixtieth day following the date of the decision	For 5 years following the time of publication

	subject matter of such contracts, names of the parties to the contract, the contract amounts, and the duration of fixed term contracts, including changes in the data mentioned above, with the exception of data on procurements directly related to and deemed necessary for reasons of national security or national defence, and with the exception of classified data. Contract value shall mean the price agreed upon for the subject of the contract, exclusive of value added tax, or in the case of gratuitous transactions, the market value or book value of the asset in question, whichever is higher. As regards periodically recurring contracts concluded for more than 1 year the contract value shall indicate the price calculated for 1 year. The value of contracts concluded within the same financial year with the same party shall be applied cumulatively.		
5	Data made public according to the Act on concessions (tender notices, particulars of tenderers, memos on evaluation procedures, outcomes of such tender procedures)	Quarterly	For the time period defined by a specific law, but archived for at least 1 year
6	Payments of more than 5 million forints made by the organ performing public duties outside the scope its main activities (such as payments made to support associations, to trade organisations representing the interests of its workers, to organisations active in educational, cultural, social and sports activities and services provided to its employees, and to foundations to support their activities)	Quarterly	For the time period defined by a specific law, but archived for at least 1 year
7	Description of developments implemented from European Union funding, including the related contracts	Quarterly	Archived for a period of at least 1 year
8	Public procurement information (annual plan, summary of the evaluation of tenders, contracts awarded)	Quarterly	Archived for a period of at least 1 year