Act CXII of 2011

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

The National Assembly, to ensure the right to informational self-determination, the freedom of information, and the free movement of data, to lay down fundamental rules promoting the protection of personal data, the right of access to data of public interest and data accessible on public interest grounds and the right to disseminate such data, as well as to set up an authority to monitor compliance with these rules, for the purpose of implementing the Fundamental Law and on the basis of Article VI of the Fundamental Law, adopts the following Act:

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 processing data in order to ensure that the privacy of natural persons is respected by controllers, and to achieve the free movement of data and transparency in public affairs through the effective implementation of the right of access to data of public interest and data accessible on public interest grounds and the right to disseminate such data.

2. Scope of the Act

Section 2 (1) All processing activities related to personal data as well as to data of public interest and data accessible on public interest grounds shall fall within the scope of this Act, with the proviso that in respect of personal data, the provisions laid down in paragraphs (2) to (6) shall apply.

(2) To the processing of personal data falling within the scope of Regulation (EU) 2016/679 of the European Parliament and of the Council (hereinafter the "General Data Protection Regulation"), the General Data Protection Regulation shall apply supplemented by the provisions of Chapters III to V and VI/A, points 3, 4, 6, 11, 12, 13, 16, 17, 21, 23 to 24 of section 3, 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 61/A to 61/D, sections 62 to 71, section 72, section 75 (1) to (5), section 75/A and Annex 1.

(2a) The provisions of Regulation (EU) 2022/868 of the European Parliament and of the Council (hereinafter the "Data Governance Act") shall apply with the additions provided for in subtitles 34/B to 34/E, Chapter V, and section 72.

(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 falling within the scope of paragraphs (2) and (3):

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

b) Chapters III to V and VI/A, as well as points 3, 4, 6, 11, 12, 13, 16, 17, 21, 23 to 24 of section 3, 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 61/A to 61/D, sections 62 to 71, section 72, section 75 (1) to (5), section 75/A and Annex 1 to 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, laid down in an Act, relating to personal data protection and the conditions for personal data processing shall apply to personal data processing under the General Data Protection Regulation if

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

b) the controller's main establishment specified in point 16 of Article 4 of the General Data Protection Regulation or the controller's 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 residing 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.

(5a) Unless otherwise provided by an Act or a binding legal act of the European Union, in applying the Data Governance Act, the provisions of paragraph (2a) shall apply if a data intermediation services provider or data altruism organisation under the Data Governance Act has its main establishment defined in point 15 of Article 2 of the Data Governance Act in Hungary, or if it performs an activity covered by the Data Governance Act in Hungary without having its main establishment in the European Union.

(6) The provisions laid down in this Act shall not apply to the processing activities of natural persons exclusively serving their own personal purposes.

(7) With respect to the further use of public sector information, an Act may provide for rules other than 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 information relating to the data subject;

3. *sensitive data* means all data falling within the special categories of personal data, that is, 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, health data 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 which 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. *health data* 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 which can be connected to the data subject and are related to criminal records, 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, recorded through any method or in any form, processed by, and pertaining to the activities of, or generated in the context of the performance of public duties by, an organ or person performing state or local government duties as well as other public duties defined by law, irrespective of the method in which it is processed and regardless of its singular or collective nature; in particular, data concerning subject-matter competence, territorial competence, organisational structure, professional activities and the evaluation of such activities, including their effectiveness, the type of data held and the laws governing its operation, as well as financial management and concluded contracts;

6. *data accessible on public interest grounds* means any data other than data of public interest the disclosure, accessibility or availability of which is required 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 without 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 the processing of data, makes decisions concerning 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 processing, and, jointly with one or more other controllers, makes decisions concerning 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 which is performed on data, regardless of the procedure applied; in particular collection, entering, recording, organisation, storage, alteration, use, retrieval, data transfer, disclosure, alignment or combination, blocking, erasure and destruction, as well as the prevention of the further use of data; taking photos and making audio or visual recordings, as well as the recording of physical characteristics suitable for 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 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 enforcing the legal consequences imposed in criminal proceedings or infraction proceedings (hereinafter jointly “organ carrying out processing for law enforcement purposes”), within the limits and for the purposes 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 police organ within its functions and powers laid down by law;

10c. *processing for national defence purposes* means processing under the Act on national defence processing activities 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, including their personnel, established in the territory of the Republic of Hungary, as well as on certain provisions concerning their status;

11. *data transfer* means making the data available to a specific third party;

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

11b. *international organisation* means an organisation and its subordinate bodies governed by public international law, or any other body which 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 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-storage medium that contains the data;

17. *technical processing* means the totality of 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 without 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 on behalf, or according to the instructions, of the controller, processes personal data;

19. *data source* means the organ performing public duties which generated the data of public interest that are to be published by electronic means or during the operations of which such data were generated;

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

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

22. *third party* means a natural or legal person, or an organisation without legal personality other than the data subject, controller, processor and persons who, under the direct direction 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 other State Party to the Agreement on the European Economic Area, as well as any other state not party to the Agreement on the European Economic Area whose nationals enjoy the same legal status as the nationals of State Parties to the Agreement on the European Economic Area on the basis of an international treaty between the European Union and its Member States and the state concerned;

24. *third country* means any state other than 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 which is aimed at evaluating, analysing or predicting certain personal aspects relating to a data subject, in particular 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 without legal personality, to which the controller or the processor makes personal data available;

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, for exercising a right and fulfilling an obligation. Processing shall comply with the purpose of processing in all stages; data shall be collected and processed fairly and lawfully.

(2) Personal data shall be essential and adequate in relation to the purposes for which they are processed. The processing of personal data shall be limited to the extent and period of time necessary in relation to the purposes for which they are processed.

(3) In the course of processing, personal data shall be considered personal data as long as the relation to the data subject can be restored. The relation to the data subject shall be considered restorable if the controller has the technical means necessary for restoration.

(4) Throughout processing, the data shall be accurate and complete, and, where necessary for the purposes of processing, kept up to date, and it shall be ensured that identification of the data subject is permitted for no longer than is necessary for the purposes of processing.

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

(5) The processing of personal data shall be deemed to be fair and lawful if, for the purpose of ensuring the data subject's right to freedom of expression, the person wishing to obtain 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 the personal visit is made for non-business purposes. A personal visit shall not be made on public holidays under the Labour Code.

5. Legal basis and general conditions for processing

Section 5 (1) Personal data may be processed only if

a) an Act or, on the basis of authorisation by an Act, within the limits set forth therein and for data other than sensitive and criminal personal data, a local government decree so requires for purposes in the public interest,

b) it is strictly necessary for the performance of the controller's tasks provided for by an Act and the data subject has given explicit consent to the processing of personal data, where point a) does not apply,

c) this is necessary in order to protect the vital interests of the data subject or of another person and to avert or prevent imminent threats to the lives, physical integrity or property of persons, and is proportionate thereto, where point a) does not apply, or

d) the data subject manifestly disclosed the personal data, and this is necessary and proportionate to achieve the purpose of processing, where point a) does not apply.

(2) Sensitive data may be processed only

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

b) if it is strictly necessary for the implementation of an international treaty promulgated by an Act and is proportionate thereto, or an Act so requires for the promotion of a fundamental right guaranteed by the Fundamental Law or for reasons of national security, the prevention, detection and prosecution of criminal offences or national defence.

(3) Where processing is based on paragraph (1) a) or paragraph (2) b), or on Article 6 (1) (c) or (e) of the General Data Protection Regulation (hereinafter "mandatory processing"), the Act or local government decree that orders such processing shall determine the types of data to be processed, the purpose of, and conditions for, processing, the accessibility of such data, the controller and the duration of processing or the periodic review of its necessity.

(4) Only state or local government organs may keep registers containing criminal personal data that are processed for the purpose of performing the duties of the State related to the prevention, detection and prosecution of criminal offences as well as to public administration and the administration of justice, and data pertaining to infraction, civil contentious and non-contentious, and administrative contentious and non-contentious proceedings.

(5) Unless an Act, a local government decree or a binding legal act of the European Union provides for the duration of mandatory processing or the periodic review of its necessity, the controller shall review at least once every three years after the start of processing whether the processing of the personal data processed by the controller or by the processor acting on behalf of, or instructed by, the controller is necessary to achieve the purpose of processing. The controller shall record the circumstances and the outcome of the review, retain this documentation for ten years following the review, and make it available to the National Authority for Data Protection and Freedom of Information (hereinafter the "Authority") at the request of the Authority.

(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 strictly necessary for the performance of their duties connected to the processing operation have access to the sensitive data.

(7) Unless otherwise provided by an Act, international treaty, or a binding legal act of the European Union, the rules relating to the conditions for 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 research on historical events.

Section 6 A decision based solely on automated processing, including profiling, which produces adverse effects to the data subject or the legitimate interests of the data subject, or produces legal effects significantly affecting the data subject 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, applying human intervention, the result of the decision at the request of the data subject, 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) In the case of processing for law enforcement purposes, the controller or the processor acting on behalf of, or instructed by, the controller shall, unless this involves disproportionate difficulties or costs, organise the personal data it processes according to whether they are the personal data of data subjects

a) as to whom it is reasonable to assume that they have committed a criminal offence or infraction or are about to commit a criminal offence,

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

c) who were the aggrieved parties of a criminal offence or infraction or as to whom it is reasonable to assume that they can be the aggrieved parties of any criminal offence or infraction, or

d) who can be linked, in any other way than is specified in points a) to c), to a criminal offence or infraction or a perpetrator thereof, in particular those who can be interviewed as witnesses in criminal proceedings, can provide information about the criminal offence or infraction, or are in contact with, or related to, a data subject referred to in points a) and b).

(2) In the case of processing for law enforcement purposes, the controller or the processor acting on behalf of, or instructed by, the controller shall, unless this involves disproportionate difficulties or costs, clearly distinguish between facts that can be linked to the data subject and personal assessments that can be linked to the data subject.

6. Conditions for data transfer

Section 8 (1) Prior to data transfer, the controller or the processor acting on behalf of, or instructed by, the controller shall verify the accuracy and completeness of the personal data to be transferred and whether they are up to date.

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

a) it is strictly necessary for the achievement of the purpose of data transfer; and

b) upon data transfer, it provides the recipient with information available to it regarding the accuracy and completeness of the data and whether they are up to date.

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

Section 9 (1) Where the controller or the processor receives personal data on the basis of a provision of an Act, international treaty or a binding legal act of the European Union in a way that upon data transfer the transferring controller or processor indicates

a) the possible purposes of processing,

b) the possible duration of processing,

c) the possible recipients of data transfer,

d) the limitation of the data subject’s rights guaranteed by this Act, or

e) other conditions for processing,

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

(2) The data recipient shall be allowed to process the personal data and ensure the data subject's rights without regard to the processing conditions if the transferring controller has given its prior authorisation to it.

(3) Where a provision of an Act, international treaty or a binding legal act of the European Union requires the controller or the processor to apply processing conditions to the processing of personal data, upon transferring such data, the controller or the processor shall inform the recipient of such processing conditions and the legal obligation to comply with them.

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

(5) If the transferring controller so requests, the data recipient shall inform it about the use of the personal data received.

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

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

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

ba) the conditions for processing referred to in section 5 are met in the course of the international data transfer, and

bb) an adequate level of protection of the personal data transferred is ensured with respect to the controller or processor engaged in processing activities in the third country or international organisation, or

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

(2) In the case of processing for law enforcement purposes, international data transfer may take place only if, in addition to meeting 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) not an organ carrying out processing for law enforcement purposes and the conditions laid down in section 11 (3) are met, 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 gave prior authorisation 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 immediate threat to the essential interests of Hungary or any EEA State, or to the public security of these states or a third country, and the prior authorisation under subpoint ca) cannot be obtained before the international data transfer without harming these interests.

(3) The controller shall inform the organ or person entitled to give prior authorisation according to paragraph (2) c) ca) of any international data transfer specified in paragraph (2) c) cb) without delay after it.

(4) An adequate level of protection of the personal data shall be presumed to be ensured, unless proven to the contrary, if

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

b) in the absence, or in the event of suspending the application, of a legal act under point a), an international treaty containing safeguards regarding the data subjects' rights laid down in section 14, section 22 and section 23 is applicable between Hungary and the third country or international organisation whose jurisdiction applies to the recipient of the international data transfer, or

c) in the absence, or in the event of suspending the application, of a legal act under points a) to b), the controller assessed all circumstances of the transfer of personal data before the international data transfer and established that appropriate safeguards exist concerning the adequate level of protection of the personal data.

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

a) in order to protect the vital interests of the data subject or another person,

b) for the elimination of an imminent and serious threat to the public security of an EEA State or a third country,

c) in the interest of the efficient and effective conduct of inquiries or proceedings by the controller in specific individual cases, provided that it does not entail a 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 another person in specific individual cases, provided that it does not entail a disproportionate restriction of the data subject's fundamental rights.

(2) In the case of 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 the personal data according to section 10 (4) a) to c) cannot be presumed, in the absence of the data subject's explicit consent, an international data transfer may take place only if it is necessary

a) for any of the purposes specified in paragraph (1) a) and b),

b) for the purposes of the legitimate interests pursued by the data subject,

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

(3) In the case of 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, an international data transfer may take place only in specific individual cases if

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

b) it does not entail a 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 informs the organ carrying out processing for law enforcement purposes in the third country or international organisation having jurisdiction with regard to the international data transfer without delay of the international data transfer, unless such information prevents the purpose of the international data transfer from being achieved effectively, and

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

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

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

b) in the case of processing for law enforcement purposes to a recipient other than an organ carrying out processing for law enforcement purposes,

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

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

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

b) in the case of processing for law enforcement purposes

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

bb) to a recipient other than an organ carrying out processing for law enforcement purposes,

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

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

(2) Where international data transfer is based on an international treaty referred to in Article 96 of the General Data Protection Regulation and in Article 61 of Directive (EU) 2016/680, it may be carried out for the purposes, under the conditions and regarding the set of data specified therein until the treaty is amended or terminated, until it terminates or until its application is suspended, regardless of whether or not the conditions laid down in this Act are met.

Chapter II/A

RIGHTS OF THE DATA SUBJECT

7. Data subject rights

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

a) to obtain information as to the facts connected to the processing prior to the start of processing (hereinafter “right to prior information”),

b) to receive, at his request, from the controller his personal data and information related to their processing (hereinafter “right of access”),

c) to obtain, at his request and in further cases as set out in this chapter, from the controller the rectification or completion of his personal data (hereinafter "right to rectification"),

d) to obtain, at his request and in further cases as set out in this chapter, from the controller the restriction of processing of his personal data (hereinafter "right to restriction of processing"),

e) to obtain, at his request and in further cases as set out in this chapter, from the controller the erasure of his personal data (hereinafter "right to erasure").

8. Securing data subject rights

Section 15 (1) To facilitate securing data subject rights, the controller shall take appropriate technical and organisational measures and in particular it

a) shall ensure that any notification and information to be provided to the data subject in the cases set out in this Act be provided in an easily accessible and legible form using concise, clear and plain language, and

b) shall assess any request submitted by the data subject for the exercise of his rights within the shortest possible time, but within not more than twenty-five days from its submission, and shall notify the data subject of the decision in writing or, where the request was submitted in electronic form, by electronic means.

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

(3) If

a) with respect to the same set of data, the data subject submits in the same year a repeated request for the exercise of 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 costs incurred directly in relation to the repeated and unfounded exercise of the data subject rights under the provisions of points a) and b).

(4) If it is reasonable to assume that the person submitting a request for the exercise of the rights specified in section 14 b) to e) is not the data subject, the controller shall comply with the request after the identity of the person submitting it is credibly verified.

Section 16 (1) To give effect to the right to prior information, before 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 after the start of the first processing operation, the controller shall provide the data subject with the following information:

a) the name and the contact details of the controller and, where a processing operation is performed by a processor, of the processor,

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

c) the purpose of the intended processing, and

d) description of the rights of the data subject under this Act and the method to exercise them.

(2) Simultaneously with the information referred to in paragraph (1), the controller shall, in the same way or addressed specifically to the data subject, provide the data subject with the following information:

a) the legal basis of processing,

b) the period for which the processed personal data will be retained and the criteria used to determine that period,

c) when the processed personal data are transferred or planned to be transferred, the scope of the recipients of data transfer, including recipients in third countries and international organisations,

d) the source from which the processed personal data originate, and

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

(3) The controller may delay the information referred to in paragraph (2) proportionately to the objective pursued, it may restrict the content of information or may refrain from providing information, on condition that this measure is strictly necessary for ensuring

a) the efficient and effective conduct of inquiries or proceedings, 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 enforcement 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, and in particular national defence and national security, or

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

Section 17 (1) To give effect to the right of access, the controller shall, at the request of the data subject, inform the data subject whether his personal data are processed by the controller itself or by a 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 a processor acting on behalf of, or instructed by, the controller, the controller shall, in addition to the information referred to 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, and shall communicate to the data subject the following information:

a) the source of the processed personal data,

b) the purpose and legal basis of the processing,

c) the scope of the processed personal data,

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

e) the period for which the processed personal data will be retained and the criteria used to determine that period,

f) a description of the rights of the data subject under this Act and the method to exercise them,

g) the use of profiling where applicable 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 refuse the data subject's right of access proportionately to the objective pursued on condition that this measure is strictly necessary for ensuring an interest specified in section 16 (3) a) to f).

(4) When a measure referred to in paragraph (3) is applied, the controller shall inform the data subject in writing without delay

a) of the restriction or refusal of access, and shall provide also the legal and factual reasons for it, unless providing the data subject with such information would impair the safeguarding of an interest specified in section 16 (3) a) to f), and

b) of the rights of the data subject under this Act and the method to exercise them, and in particular of the possibility of exercising his right of access through the Authority.

Section 18 (1) To give effect to 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 at the request of the data subject, clarify or rectify them without delay, or it shall supplement them with further personal data provided by the data subject or with a statement attached by the data subject to

the processed personal data, provided that it is compatible with the purpose of processing (hereinafter jointly "rectification").

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

a) the accurate, correct or complete personal data are not available to it and the data subject does not make them available to it either, or

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

(3) If the controller rectifies the personal data processed by the controller or by the processor acting on behalf of, or instructed by, the controller in accordance with to the provisions of paragraph (1), it shall inform the controller to whom it had transferred the personal data affected by the rectification thereof and of the rectified personal data.

Section 19 (1) To give effect to the right to restriction of processing, the controller shall restrict processing to the processing operations specified in paragraph (2) if

a) the accuracy, correctness or 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, correctness or completeness of the processed personal data cannot be verified beyond doubt, for a period until the doubts are cleared,

b) the data should be erased pursuant to section 20 a), but it is reasonable to assume from the data subject's written declaration or the information available to the controller that the erasure of the data would infringe the legitimate interests of the data subject, for a period until the legitimate interest that justifies refraining from the erasure exists,

c) the data should be erased pursuant to section 20 a), but they must be retained as evidence in 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 a period until the conclusion with administrative finality or final and binding effect of those inquiries or proceedings,

d) the data should be erased pursuant to section 20 a), but they must be retained for the purpose of fulfilling the documentation obligation under section 12 (2), for the period set 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 perform processing operations other than storage with the personal data affected by the restriction only for the purposes of the legitimate interests pursued by the data subject or in accordance with the provisions laid down in an Act, international treaty or a binding legal act of the European Union.

(3) In the case of lifting the restriction of processing specified in paragraph (1) a), the controller shall inform the data subject of the lifting of the restriction of processing in advance.

Section 20 To give effect to 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 no longer applies, or further processing is not necessary to achieve the purpose of processing,

ac) the period of processing set in an Act, international treaty or a binding legal act of the European Union has elapsed, or

ad) the legal basis of processing no longer applies, and there is no other legal basis of processing,

b) the data subject withdraws consent to processing or requests the erasure of personal data, except where processing is based on section 5 (1) a) or c) or paragraph (2) b),

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

d) the period set in section 19 (1) b) to d) has elapsed.

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

a) of the refusal and shall provide also the legal and factual reasons for it, and

b) of the rights of the data subject under this Act and the method to exercise them, and in particular of the possibility of exercising through the Authority the right to the rectification, erasure, or the restriction of processing, of personal data processed by the controller or by the processor acting on behalf of, or instructed by, the controller.

(2) The controller may delay the information referred to in paragraph (1) a) proportionately to the objective pursued, it may restrict the content of information or may refrain from providing information, on condition that this measure is strictly necessary for ensuring an interest specified in section 16 (3) a) to f).

(3) If the controller rectifies or erases the personal data processed by it or a processor acting on behalf of, or instructed by, the controller, or restricts the processing of such data, the controller shall inform the controllers and processors to whom it has transferred the data prior to this 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 To give effect to his rights, in accordance with the provisions laid down in Chapter VI, the data subject

a) may apply to the Authority for the initiation of inquiry to investigate the lawfulness of the controller's measure if the controller restricts his rights under section 14 or refuses his request for the exercise of these rights, and

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

Section 23 (1) The data subject may bring proceedings before the court against the controller or, in the context of processing operations within the processor's scope of activity, the processor if he considers that in processing his personal data, the controller or the processor acting on behalf of, or instructed by, the controller infringes the personal data processing provisions laid down in the national law or a binding legal act of the European Union.

(2) It shall be for the controller or the processor to prove that the processing complies with the personal data processing provisions laid down in the national law or a binding legal act of the European Union, 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 to a court action may be a party to the action. The Authority may intervene in the action in order to facilitate the success of the data subject.

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

a) terminate the unlawful processing operation,

b) restore the lawfulness of processing, or

c) engage in a conduct specifically prescribed to give effect to the data subject rights,

and, where necessary, it shall also decide on claims for damages or grievance award.

(6) The court may order its judgment to be published together with the identification data of the controller or processor if the judgment concerns a wide range of persons, the defendant controller or processor is an organ performing public duties, or the gravity of the injury justifies publication.

Section 24 (1) If a controller or a processor acting on behalf of, or instructed by, the controller infringes the personal data processing provisions laid down in the national law or a binding legal act of the European Union and thereby causes damage to someone else, it shall be liable for compensation for the damage caused.

(2) If a controller or a processor acting on behalf of, or instructed by, the controller infringes the personal data processing provisions laid down in the national law or a binding legal act of the European Union and thereby violates the personality rights of another person, the person whose personality rights are violated may claim grievance award from the controller or the processor acting on behalf of, or instructed by, the controller.

(3) A controller shall be exempt from liability for the damage caused and from the obligation to pay grievance award if it proves that the damage or the injury caused by the violation of personality rights is the result of an irresistible reason external to processing.

(4) A processor shall be exempt from liability for the damage caused and from the obligation to pay grievance award if it proves that in performing processing operations, it acted in compliance with the personal data processing obligations laid down in the national law or a binding legal act of the European Union explicitly imposed upon processors and with the lawful instructions given by the controller.

(5) The controller and the processor acting on behalf of, or instructed by, the controller, and the joint controllers and the processors acting on behalf of, or instructed by, the joint controllers shall be jointly and severally liable

a) towards the data subject for any damage caused by their violation of the personal data processing provisions laid down in the national law or a binding legal act of the European Union, and

b) for paying to the data subject grievance award for the violation of personality rights caused by their violation of the personal data processing provisions laid down in the national law or a binding legal act of the European Union.

(6) No compensation need be paid and grievance award shall not be claimed if and to the extent that the damage or the injury caused by the violation of personality rights resulted from the intentional or grossly negligent conduct of the injured party or of the person whose personality rights are infringed, respectively.

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

Section 25 (1) For a period of five years after the death of the data subject, the rights specified in section 14 b) to e) and, as regards processing operations under the General Data Protection Regulation, in Articles 15 to 18 and Article 21 of the General Data Protection Regulation to which the deceased had been entitled while alive may be exercised by a person who has been authorised to do so by the data subject by way of an administrative setting or a declaration made at the controller and incorporated in a public deed or a private deed of full probative value; where the data subject has made more than one declaration at the same controller, the later-dated declaration shall prevail.

(2) If the data subject has not made a juridical act pursuant to paragraph (1), his close relative within the meaning of the Civil Code may, despite the lack of such juridical act, for a period of five years after the death of the data subject, exercise the rights specified in section 14 c) and, as regards processing operations under the General Data Protection Regulation, in Article 16 and Article 21 of the General Data Protection Regulation, and, where processing was unlawful already while the data subject was still alive or where the purpose of processing

ceased to exist upon the death of the data subject, in section 14 d) and e) and, as regards processing operations under the General Data Protection Regulation, in Article 17 and Article 18 of the General Data Protection Regulation to which the deceased had been entitled while alive. The close relative who was the first to use this entitlement shall be entitled to exercise the data subject rights under this paragraph.

(3) In exercising the data subject rights under paragraph (1) or (2), in particular in proceedings against the controller and before the Authority or the court, the person exercising those rights shall have the same rights and obligations as the data subject under this Act.

(4) The person exercising the data subject rights under paragraph (1) or (2) shall produce an Extract from the Register of Deaths or a court decision to prove the death, and the date of death, of the data subject and, where paragraph (2) applies, a public deed to prove his identity and his being a close relative.

(5) Upon request, the controller shall inform the data subject's close relative within the meaning of the Civil Code about the measures taken under paragraph (1) or (2), unless the data subject prohibited it in his declaration referred to in paragraph (1).

Chapter II/B

OBLIGATIONS OF THE CONTROLLER AND THE PROCESSOR

10. General responsibilities of the controller

Section 25/A (1) In order to ensure the lawfulness of processing, the controller shall implement technical and organisational measures adapted to the particularities of processing, in particular its purpose as well as the risks posed by the processing for the fundamental rights of the data subjects, including, where appropriate, pseudonymisation. The controller shall regularly review and, where necessary, appropriately modify those measures.

(2) The measures referred to in paragraph (1) shall be designed so as to

a) serve the effectiveness of the personal data processing requirements, in particular the principles of processing and the rights of data subjects, in a manner reasonably available taking account of the state of the art and the cost of implementation of those measures, and

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

ba) where personal data are processed, the kind and the quantity of the personal data concerned and the extent and duration of processing is in line with the purposes of the processing, and

bb) personal data processed by the controller are not made publicly available in the absence of express intent to that effect on the part of the data subject.

(3) Where the controller is obliged to designate a data protection officer, the measures referred to in paragraph (1) shall include the adoption and implementation of data protection and data security policies by the controller.

(4) The processor and any person acting under the authority of the controller who has lawful access to the personal data processed within the scope of the activities of the controller shall not perform operations on the data accessed this way except on instructions from the controller, unless otherwise provided by an Act, international treaty or a binding legal act of the European Union.

(5) The controller and the processor shall facilitate the activities of the organs and persons authorised to conduct proceedings concerning the lawfulness of their processing operations and provide them with the information necessary for conducting such proceedings.

Section 25/B (1) Where, and in so far as, the respective responsibilities of the joint controllers for compliance with the obligations related to the processing activities performed by them, in particular as regards the exercising of the rights of the data subject and non-compliance with these obligations are not determined by an Act, international treaty or a binding legal act of the European Union, the joint controllers shall, to the extent they are not determined by the legal obligations to which the joint controllers are subject, determine the respective responsibilities by means of a written agreement between them which shall be published.

(2) Unless it is specified in an Act, international treaty or a binding legal act of the European Union, the agreement under paragraph (1) shall designate a joint controller to act as a contact point that may be approached by the data subject seeking to exercise his rights under this Act. Where no joint controller is specified or designated to act as a contact point, the data subject may exercise his rights under this Act in respect of each of the processing operations and against each of the joint controllers.

11. The processor

Section 25/C (1) A person or organisation may act as processor only if that person or organisation provides 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. The processor shall demonstrate these guarantees to the controller prior to the start of processing.

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

(3) If the engagement of the other processor is based on the controller's general authorisation, the processor shall inform the controller of the identity of the other processor and of the planned tasks to be carried out by the other processor prior to engaging the other processor. If, on the basis of this information, the controller objects to the engagement of the other processor, the processor shall not engage the other processor unless it fulfils the conditions specified in the objection.

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

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

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

b) to ensure in the course of its activity that persons authorised to access the personal data concerned commit themselves to confidentiality concerning the personal data accessed by them, unless they are otherwise bound by an appropriate obligation of confidentiality established by law,

c) to assist, using all appropriate tools, in the course of its activity the controller in promoting the data subjects' rights and fulfilling the related obligations,

d) at the choice of the controller, either to delete without delay the personal data accessed during its activity or to transfer them to the controller and subsequently delete the existing copies following the completion of the processing operations it carried out, 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 if the conditions specified in this Act are complied with.

(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 activities related to the personal data that it processes, personal data breaches and the measures concerning the data subject's right of access (hereinafter jointly "controller's record"). The controller shall record the following information in the controller's record:

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

b) the purpose or purposes of the processing,

c) when the personal data are transferred or planned to be transferred, the scope of the recipients of data transfer, including recipients in third countries and international organisations,

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

e) the use of profiling where applicable,

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

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

h) the time of erasure of the processed personal data if known,

i) a general description of the technical and organisational security measures taken in accordance with 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 refusing, according to this Act, the data subject's right of access.

(2) The processor shall maintain a record of its processing activities carried out on behalf, or according to the instructions, of specific controllers (hereinafter "processor's record"). The processor shall record the following information in the processor's record:

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

b) the types of processing activities carried out on behalf, or according to the instructions, of the controller;

c) reference to the international data transfer and the indication of the recipient third country or international organisation where international data transfer is made on the controller's explicit instruction;

d) a general description of the technical and organisational security measures taken in accordance with this Act.

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

(4) The organs carrying out processing for national security purposes may fulfil the obligation to maintain the controller's record also 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 that the lawfulness of processing operations performed on personal data by electronic means can be verified, the controller and the processor shall record in an automated processing system (hereinafter the "electronic logbook")

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

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

c) the exact time of performance of the processing operation,

d) the person carrying out the processing operation,

e) the recipient of the data transfer, where personal data are transferred.

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

(3) If the Authority or a person or organ engaged in an activity specified by the law for a purpose described in paragraph (2) so requests, the controller and the processor shall provide access to the electronic logbook for, and transfer data from the logbook to, the Authority or that person or organ.

(4) The data recorded in the controller's and the processor's record as well as in 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 fulfil the obligation to maintain the electronic logbook also 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 intended processing, carry out an assessment of the expected impact of the envisaged processing operations on the data subjects' fundamental rights, taking into account the circumstances of processing, in particular its purpose, the scope of data subjects and the technology used during the processing operations.

(2) Where the risk estimation carried out under paragraph (1) indicates that the intended processing is likely to result in a significant influence on a fundamental right of the data subjects (hereinafter "high-risk processing"), the controller shall, except where paragraph (6) applies, prepare a written assessment of the expected impact of the intended processing on the data subjects' fundamental rights prior to the start of processing (hereinafter "data protection impact assessment").

(3) If the Authority qualifies a specific type of processing as high-risk processing and publishes this finding, and the intended processing involves the application of an operation or set of operations of the same or similar type as the one applied during the type of processing referred to in the finding, it shall be presumed that the intended processing is of high risk.

(4) If the Authority finds that a specific type of processing does not qualify as high-risk processing and publishes this finding, and the intended processing exclusively involves the application of an operation or set of operations of the same or similar type as the one applied during the type of processing referred to in the finding, the intended processing shall be presumed not to qualify as high-risk processing.

(5) The data protection impact assessment shall contain at least a general description of the envisaged processing operations, a description and the character of the risks to the data subjects' fundamental rights identified by the controller, and the measures envisaged to address these risks as well as those applied by the controller to ensure the exercise of the right related to personal data.

(6) Where processing is mandatory, including in particular mandatory processing for the purposes specified in section 2 (3), the data protection impact assessment under paragraph (5) shall be carried out by the entity in charge of the preparation of the law requiring such processing.

Section 25/H (1) The controller or, in the context of its activities, the processor shall, except where paragraph (2) applies, initiate consultation with the Authority prior to the start of processing (hereinafter "prior consultation") where

a) a data protection impact assessment carried out concerning the intended processing indicates that the intended processing would be of high risk in the absence of measures taken by the controller to mitigate the risks involved by the processing, or

b) the intended processing is to be presumed to be of high risk in accordance with section 25/G (3).

(2) Where processing is mandatory, including in particular mandatory processing for the purposes specified in section 2 (3), prior consultation shall be initiated and conducted by the entity responsible for the preparation of the law requiring such processing in the context of the preparation of law.

(3) Simultaneously with initiating prior consultation, the controller or, in the context of its activities, the processor shall provide the Authority with the outcome of the data protection impact assessment and inform the Authority of any circumstance that the Authority considers necessary for successfully carrying out the prior consultation.

(4) If the Authority finds in the course of the prior consultation that, with regard to the intended processing, the provisions specified in the relevant law are not fully complied with, in particular if it finds that the controller has insufficiently identified or mitigated the risks involved by the processing, it shall, in addition to or instead of taking any other measure within its functions and powers, determine suitable actions for the elimination of the explored deficiencies and shall provide advice to the controller or, in the context of its activities, the processor as to their implementation.

(5) The Authority shall provide the advice referred to in paragraph (4) in writing within six weeks from the initiation of prior consultation. The Authority may extend this time limit by no more than one month; if this is the case, it shall inform the controller or the processor of the extension and the reasons for it within one month from initiating prior consultation.

14. Data security measures

Section 25/I (1) To ensure an appropriate level of security for the processed personal data, the controller and the processor shall implement technical and organisational measures appropriate to the degree of risks for the fundamental rights of data subjects posed by processing, in particular from the processing of the sensitive data of data subjects.

(2) In designing and implementing the measures referred to in paragraph (1), the controller and the processor shall take into account all circumstances of the processing, in particular the state of the art, the costs of implementation and the nature, scope and purposes of processing as well as the risks of varying likelihood and severity for the rights of data subjects posed by processing.

(3) The controller and, within the scope of its activities, the processor shall through the measures referred to in paragraph (1) ensure that

a) unauthorised persons are denied access to the equipment used for processing (hereinafter the "processing system"),

b) the unauthorised reading, copying, modification and removal of data-storage media are prevented,

c) the unauthorised entering of personal data in the processing system as well as the unauthorised access to, alteration and erasure of, personal data stored therein are prevented,

d) unauthorised persons are prevented from using the processing systems by means of data transmission equipment,

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

f) it can be verified and ascertained to which recipients the personal data have been or can be transferred or provided by means of data transmission equipment,

g) it can be subsequently verified and ascertained which personal data have been entered into the processing system, and when and by whom,

h) the unauthorised access to, copying, alteration and erasure of personal data during transfer or the transportation of the data-storage medium are prevented,

i) in the case of breakdown, the processing system can be restored, and

j) the processing system is operational, any malfunction occurring during its operation is reported, and the stored personal data cannot be altered even through making the system malfunction.

(4) To protect datasets processed electronically in various registers, the controller or, within the scope of its activities, the processor 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) In the case of a personal data breach occurring in relation to data processed by the controller or the processor acting on behalf of, or instructed by, the controller, the controller shall record the data referred to in paragraph (5) a), c) and d), and shall without undue delay but within not more than seventy-two hours after having become aware of it notify the personal data breach to the Authority.

(2) The personal data breach need not be notified when it is unlikely to result in a risk to data subject rights.

(3) If the controller is prevented from fulfilling its notification obligation under paragraph (1) within the time limit, it shall perform notification without delay after the obstacle ceases to exist and shall attach to the notification a 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 communicate the personal data breach to the controller without undue delay after becoming aware of it.

(5) In fulfilling the notification obligation 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, and 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, including, where appropriate, measures to mitigate the possible adverse effects resulting from the personal data breach.

(6) If any of the information referred to in paragraph (5) a) to d) is not available to the controller at the time of notification, the controller shall supplement the notification with such information subsequently, without undue delay after becoming aware of the availability of the information.

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

(8) With the exception of notifications including classified data, the controller shall fulfil the notification obligation under paragraph (1) through the electronic platform provided for this purpose by the Authority.

(9) In the case of processing for national security purposes, the provisions of paragraphs (1) to (8) shall apply with the derogation that if fulfilling the notification obligation under paragraph (1) or the communication obligation under paragraph (7) would be against national security interests, the obligation in question shall be fulfilled after the national security interests concerned no longer apply.

Section 25/K (1) When the personal data breach is likely to result in consequences that have significant influence on 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 undue delay.

(2) The controller shall be exempt from the obligation to communicate to the data subject under paragraph (1) if

a) the controller has 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 that render the personal data unintelligible to any person who is not authorised to access it, such as encryption,

b) after having become aware of the personal data breach, the controller has taken subsequent measures which ensure that the consequences that have significant influence on a fundamental right of the data subject are not likely to occur,

c) direct communication to the data subject in accordance with paragraph (1) would involve disproportionate effort by the controller, and therefore the controller informs the data subjects about the personal data breach by way of public communication accessible to anyone, or

d) such communication is excluded by an Act in accordance with the provisions of paragraph (6).

(3) In fulfilling the communication obligation under paragraph (1), the controller shall describe in clear and plain language the nature of the personal data breach and provide the data subject with the information referred to in section 25/J (5) b), c) and d).

(4) If, on the basis of notification under section 25/J (1), the Authority finds that it is necessary to inform the data subject due to the personal data breach involving high risk, the controller shall fulfil its communication obligation under paragraph (1) not yet fulfilled without undue delay after the finding is made.

(5) The controller shall not be obliged to fulfil the communication obligation under paragraph (1) if, on the basis of notification under section 25/J (1), the Authority finds that a circumstance specified in paragraph (2) a) to d) exists.

(6) By way of derogation from the provisions under paragraphs (1) to (5), an Act may exclude or restrict communication to the data subject or require delayed communication, subject to the conditions and on the grounds referred to in section 16 (3).

16. Data protection officer

Section 25/L (1) The controller and the processor shall employ a data protection officer to promote the implementation of personal data processing provisions and the data subject rights if

a) the controller or the processor performs state duties or other public duties specified by the law, except for courts, or

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

(2) A person may be designated as a data protection officer if that person has an appropriate level of knowledge of the legal rules and legal practice relating to personal data protection and is able to fulfil the tasks referred to in section 25/M (1).

(3) The data protection officer may fulfil the tasks referred to in section 25/M (1) for more than one controller or processor at the same time, provided that this poses no risk to the professional and efficient fulfilment of his tasks. The data protection officer shall inform the controller or the processor of any other controllers or processors for whom he fulfils data protection officer's tasks.

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

(5) The controller and the processor shall involve the data protection officer in a timely manner in the preparation of all decisions which relate to personal data protection, together with providing him with all the conditions, rights and resources, as well as with access to all the data and information, necessary to carry out the data protection officer's tasks and to maintain his expert knowledge up-to-date.

Section 25/M (1) The data protection officer shall facilitate compliance with the obligations of the controller and processor set out in personal data processing provisions, and in particular the data protection officer shall

a) provide the controller, the processor and the persons employed by them who carry out processing operations with up-to-date information on personal data processing provisions and advise them on how to implement these provisions;

b) on an ongoing basis, monitor and check compliance with personal data processing provisions, in particular laws and internal data protection and data security policies, including the clear assignment of responsibilities related to specific processing operations, enhancement of knowledge and awareness raising in data protection of staff involved in processing operations, and the regular audits;

c) assist in exercising data subjects' rights, in particular by investigating the data subjects' complaints and by proposing to the controller or processor to take the measures necessary for remedying the complaint;

d) provide advice to promote and shall monitor the performance of the data protection impact assessment;

e) cooperate with the organs and persons entitled to bring proceedings relating to the lawfulness of processing, acting in particular as a contact point for the Authority for the purpose of facilitating prior consultation and proceedings by the Authority;

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

(2) During and after his term of office as data protection officer, the data protection officer shall keep confidential the personal data, classified data and data classified as secret protected by law and secret related to the exercise of a profession which have come to his knowledge in connection with his activity and its performance, as well as all data, facts or circumstances that the controller or processor employing him is not obliged, by virtue of an Act, to make publicly available.

Section 25/N (1) The conference of data protection officers (hereinafter "conference"), aimed at maintaining regular professional contact between the Authority and data protection officers, shall have the objective of developing consistent legal practice relating to the application of laws governing personal data protection 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 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 organ or person performing state or local government functions or other public duties defined by law (hereinafter jointly "organ performing public duties") shall allow everyone access, if requested, to data of public interest and data accessible on public interest grounds processed by it, except where this Act provides otherwise.

(2) Data accessible on public interest grounds shall include the name, responsibilities, job and managerial position of a person acting within the functions and powers of the organ performing public duties as well as that person's other personal data relevant to performing the public duties and personal data whose accessibility is required by an Act. Personal data accessible on public interest grounds shall be disseminated observing the purpose limitation principle of data processing. Publishing the personal data accessible on public interest grounds on a website shall be governed by the provisions of Annex 1 and the separate Act regulating the legal status of the person performing public duties.

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

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

Section 27 (1) No access shall be provided to data of public interest and data accessible on public interest grounds that are classified data within the meaning of the Act on the protection of classified data.

(2) The right of access to data of public interest and 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 or prevention of criminal offences;

d) environmental protection or nature preservation;

e) central financial or foreign exchange policy;

f) external relations, relations with international organisations;

g) court proceedings or administrative authority proceedings;

h) intellectual property rights.

(3) Since data related to the use of the central budget, local government budget and European Union funds, to benefits and allowances involving the budget, to the management, possession, use, utilisation and the disposal and encumbering of state and local government assets, and to the acquisition of any right connected to such assets, as well as data whose accessibility or disclosure is required on public interest grounds by a separate Act are data accessible on public interest grounds, they shall not qualify as trade secrets. 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) Where a request to this effect is made, a natural person, legal person or an organisation without legal personality that establishes a financial or business relationship with a person belonging to a subsector of the general government sector shall provide information to anyone with respect to data linked to that relationship if accessible on public interest grounds under on paragraph (3). The information obligation may be fulfilled by disclosing the data accessible on public interest grounds or by way of reference to the public source that contains the data disclosed earlier in electronic form.

(3b) If a party refuses to provide information despite being obliged to do so under paragraph (3a), the party requesting information may apply to the organ authorised to exercise legality supervision over the party obliged to provide information for the initiation of proceeding.

(4) Access to data of public interest may be restricted on the basis of a legal act of the European Union with a view to safeguarding an important economic or financial interest of the European Union, including monetary, budgetary and taxation interests.

(5) Any data produced or recorded in the course of a decision-making process to support decision making within the functions and powers of an organ performing public duties shall not be disclosed for ten years from it being generated. Considering the weight of the public interest in granting access and in denying access, the head of the organ that processes the data in question may permit access.

(6) Within the time limit referred to in paragraph (5), a request for access to data used for supporting decision making may be refused after the decision is adopted if the data supports also future decision making, or if access to it would jeopardise the lawful functioning of the organ performing public duties or the performance of its functions and powers without undue external influence, such as, in particular, the free expression of its views generating the data during the preparatory stage of decision making.

(7) For the restriction of the accessibility of certain data used for supporting decision making, a law may set a period shorter than the time limit referred to in paragraph (5).

(8) The provisions of this chapter shall not apply to the provision of data from publicly certified registers which is regulated by a separate Act.

21. Request for access to data of public interest

Section 28 (1) Anyone may request access to data of public interest orally, in writing or by electronic means. The provisions pertaining to access to data of public interest shall apply to access to data accessible on public interest grounds.

(2) Unless otherwise provided by an Act, personal data of the requesting party may be processed only to the extent necessary for compliance with the request, the assessment of the request under the criteria referred to in section 29 (1a), or the payment of a fee charged for compliance with the request. After the expiry of the period referred to in section 29 (1a) or the payment of the fee, the personal data of the requesting party shall be erased without delay.

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

Section 29 (1) The organ performing public duties that processes the data in question shall comply with the request for access to data of public interest as soon as possible, but at the latest within 15 days from receiving the request.

(1a) Where any part of a data request is identical to another data request of the same requesting party submitted regarding the same set of data in the preceding year, the organ performing public duties that processes the data in question shall not be obliged to comply with that part of the request, provided that the data belonging to the same set of data did not change.

(1b) The organ performing public duties that processes the data in question shall not be obliged to comply with the data request if the requesting party does not indicate his name or, for a requesting party other than a natural person, its designation, or the contact information

through which the requesting party can be provided with any information and notification in connection with the data request.

(2) If the data request concerns a significant volume or large number of data, or if compliance with the data request involves a disproportionate use of the labour resources needed for the performance of the core activities of an organ performing public duties, the time limit referred to in paragraph (1) may be extended by 15 days on one occasion. The requesting party shall be informed accordingly within 15 days of the receipt of the request.

(2a) If the data request concerns data generated by an institution or Member State of the European Union, the controller shall contact the institution or Member State of the European Union concerned without delay and shall inform the requesting party thereof. The period between the provision of information and the receipt by the controller of the response of the institution or Member State of the European Union concerned shall not be counted into the time limit available for compliance with the data request.

(3) The requesting party may be provided with a copy of the document or the part of the document that contains the data in question, irrespective of the form of storage. The organ performing public duties that processes the data in question may charge, up to the amount of the costs incurred in relation to compliance with the data request, a fee for compliance, provided that the amount of the incurred costs exceeds the minimum chargeable amount specified in a government decree, with the proviso that the amount of the fee thus determined may not exceed the maximum amount specified in a government decree. The requesting party shall be informed of the amount of the fee and the possibilities of compliance with the data request that do not require making copies within 15 days of the receipt of the request.

(3a) The requesting party shall make a statement within 30 days from receiving the information under paragraph (3) as to whether he maintains the request. The period between the provision of information and the receipt by the controller of the statement of the requesting party shall not be counted into the time limit available for compliance with the data request. If the requesting party maintains the request, he shall pay the fee to the controller within a time limit of not less than 15 days determined by the controller.

(4) If the organ performing public duties that processes the data in question charges a fee in accordance with paragraph (3), the data request shall be complied with within 15 days from the date of payment of the fee by the requesting party.

(5) In determining the amount of the fee, the following cost elements may be taken into account:

a) the cost of the data-storage medium that contains the requested data; and

b) the cost incurred by delivering the data-storage medium that contains the requested data to the requesting party

c)

(6) The level of cost elements 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 contains also data to which access by the requesting party is not permitted, the data that must not be accessed shall be made unrecognisable on the copy.

(2) Data requests shall be complied with in a comprehensible manner and, if the organ performing public duties that processes the data in question is able to bring it about without disproportionate difficulties, in the form and manner requested by the requesting party. If the data requested has previously been disclosed in an electronic form, the request may be complied with also by way of reference to the public source that contains the data. A data request shall not be refused on the grounds that it cannot be complied with in a comprehensible form.

(2a) The organ performing public duties shall not be obliged to comply with the data request if complying with the request would necessitate

a) procuring or collecting data other than those the organ performing public duties effectively processes, including in particular data that are processed by an organ performing public duties under the direction or supervision of the former; or

b) producing, by consulting the data of public interest or data accessible on public interest grounds effectively processed by the organ performing public duties, new data as compared to those it processes.

(3) A refusal to comply with a data request, along with information as to the reasons therefor and the legal remedies available to the requesting party under this Act, shall be notified to the requesting party in writing or, if the requesting party has provided an electronic mail address in the request, by electronic mail within 15 days of the receipt of the request. The controller shall keep records on the requests refused and the reasons for refusing them.

(4) Compliance with a request for access to data of public interest shall not be refused on the grounds that the requesting party whose mother tongue is not Hungarian uses his mother tongue or another language he understands to state his request.

(5) If an Act allows the controller discretion as to whether to refuse compliance with requests for access to data of public interest, the grounds for refusal shall be interpreted in a restrictive way, and compliance with the request for access to data of public interest may be refused only if the public interest in refusal outweighs the public interest in compliance with the request for access to the data of public interest.

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

(7) Access to data for the purpose of comprehensively checking, on invoice level or systematically, the financial management of organs performing public duties shall be governed by the provisions of separate Acts. With reference to this, the controller may comply with the data request also by indicating the subjects of the legal relationship, the type of the legal relationship, the object of the legal relationship and the volume and amount of service and consideration as well as the date of their performance, instead of providing a copy of the document requested.

21/A. Court action to be brought in respect of requests for access to data of public interest

Section 31 (1) If a request for access to data of public interest is refused, or the time limit open for compliance or the time limit extended by the controller pursuant to section 29 (2) expires with no result, and for the review of the amount of the fee charged for compliance with the data request, the requesting party may bring proceedings before the court (for the purposes of this subtitle, hereinafter the "action"), with the proviso that the provisions of Act CXXX of 2016 on the Code of Civil Procedure (hereinafter the "Civil Procedure Code") shall apply to such an action with the derogations laid down in this subtitle.

(2) It shall be for the controller to prove the lawfulness of, and the reasons for, refusal as well as the reasons on the basis of which the amount of the fee payable for compliance with the data request has been determined.

(3) The action shall be brought against the organ performing public duties that refused the request within thirty days from the communication of refusal, the expiry of the time limit with no result, or the expiry of the time limit for the payment of the fee. If regarding the refusal of, or non-compliance with, the request, or the amount of the fee charged for compliance with the data request the requesting party makes a notification to the Authority to initiate the Authority's inquiry, the action shall be brought within thirty days from the receipt of the notice of the refusal to examine the notification on its merits or of the termination or conclusion under section 55 (1) b) of the inquiry, or of the notice 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 otherwise does not have the capacity to be a party to a court action may be a party to the action. The Authority may intervene in the action in order to facilitate the success of the requesting party, and the holder of trade secret or another secret specified in an Act may intervene in the action in order to facilitate the success of the controller.

(5) With the exception of actions brought against organs performing public duties with national territorial competence, the district court shall have subject-matter jurisdiction over the action and territorial jurisdiction shall lie with the district court operating at the seat of the regional court or, in Budapest, with the Pest Central District Court. The court with territorial jurisdiction shall be determined on the basis of the seat of the defendant organ performing public duties.

(6) The court shall act in all stages of such actions, including review procedure, as a matter of priority.

(6a) If the controller refuses to comply with the request for access to data of public interest on the basis of section 27 (1), and the requesting party brings proceedings before the court for the review of the refusal of the request for access to data of public interest in accordance with paragraph (1), the court shall apply to the Authority for the initiation of an authority proceeding for the supervision of data classification and shall simultaneously suspend the court proceedings. No separate appeal shall be available against the order aimed at initiating the authority proceeding for the supervision of data classification or suspending proceedings.

(7) If the court grants the request for access to data of public interest, it shall in its decision require the controller to communicate the requested data of public interest and set a time limit for compliance with the data request. The court may modify the amount of the fee charged for compliance with the data request or may order the organ performing public duties to commence new proceedings with respect to determining the amount of the fee.

Section 31/A (1) If the statement of claim is suitable for litigation, the court shall set, and summon the parties to, the preparatory hearing for a date not more than fifteen days after the submission of the statement of claim. If the statement of claim becomes suitable for hearing only after a measure by the court, the time limit to set a hearing date shall be calculated from that date. The summons period shall be at least three working days.

(2) Simultaneously with summoning him to the preparatory hearing, the court shall communicate the statement of claim to the defendant, and call upon the parties to bring to the hearing all documents and other means of evidence pertaining to the case, in addition, it shall call upon the defendant to make his statement reflecting to the statement of claim during the hearing, with a content that meets the requirements for a written statement of defence.

(3) The defendant may submit a written statement of defence within three working days from the service of the statement of claim, but not later than three days before the due date of the preparatory hearing. Simultaneously, the defendant shall send the written statement of defence also to the electronic mail address of the plaintiff, if known to him, for information and shall substantiate the fact of sending before the court. Procedural acts performed in violation of these provisions shall be ineffective.

(4) If the defendant misses the preparatory hearing and does not submit a written statement of defence, the action shall be deemed undisputed, and the court shall close the preparatory hearing and find against the defendant in a judgment, unless the proceeding is to be terminated. If the defendant present did not submit a written statement of defence earlier, he shall present it orally at the preparatory hearing at the latest.

(5) The continuation of the preparatory stage may be ordered during the preparatory hearing if closing the preparatory stage is prevented by an unavertable procedural obstacle or an objective obstacle pertaining to the circumstances or operation of the court or a party. The continued preparatory hearing shall be set for a date within fifteen days.

Section 31/B (1) The court shall hold the main hearing immediately after adopting the order closing the preparatory stage. The taking of evidence shall be limited to evidence that is available at the hearing or had been proposed by the parties before the order closing the preparatory stage was adopted. Subsequent taking of evidence shall not be permitted in the action.

(2) The main hearing may be postponed if

a) a party so requests, while substantiating, through already discovered evidence or by other means, that the evidence offered by him would be suitable for and successful in confirming or refuting the statements made in the statement of claim or in the defence, or

b) the taking of evidence ordered is prevented by an obstacle beyond the party's control, and the party who moved that evidence be taken maintains his request for the taking of evidence; the hearing shall not be postponed in order to obtain such a statement from an absent party.

(3) If the conditions specified in paragraph (2) are not met, the court shall refrain from ordering and performing the taking of evidence.

(4) If the main hearing is postponed, the continued main hearing shall be set for a due date within fifteen days following the date of the postponed hearing, unless it is not possible under the circumstances of the case.

(5) If all parties miss the continued main hearing, or the party not missing the hearing does not request the hearing to be held, and the party on whose part the omission arose did not request the hearing to be held in his absence in either case, then the proceedings may not be suspended and the court shall terminate the proceeding *ex officio*.

Section 31/C (1) In the course of the action, the following shall not be permitted:

a) application for excuse, apart from the case referred to in section 31 (3),

b) counter-claim,

c) stay agreed upon by the parties,

d) suspension, apart from the cases referred to in section 31 (6a) and in section 126 of the Civil Procedure Code,

e) issuing a court injunction,

f) extending the action, and

g) intervening, apart from the case referred to in section 31 (4).

(2) In the action, in the cases specified in section 121 (1) c) to f) of Act CXXX of 2016 on the Code of Civil Procedure, the period of stay shall not exceed one month.

(3) The court shall put its judgment in writing within fifteen days after delivering and announcing it; the delivery and announcement of the judgment may be postponed for up to fifteen days.

(4) The appeal shall be adjudicated by the court of second instance within fifteen days after receipt of the documents at the latest. The opposing party of the appellant may request a hearing within three days after the service of the appeal, and shall submit the counter-appeal and the cross-appeal, if any, in writing within five days.

(5) The review application shall be adjudicated by the Curia within sixty days after receipt of the documents at the latest.

Chapter IV

PUBLICATION OF DATA OF PUBLIC INTEREST

22. Information obligation regarding data of public interest

Section 32 The organs performing public duties shall promote and ensure that the general public is promptly provided with accurate information with regard to matters falling within their functions, such as the state and local government budgets and their implementation, the management of state and local government assets, the use of public funds and contracts concluded in connection therewith, and special and exclusive rights conferred upon market actors, private organisations and individuals.

23. Obligation of electronic publication

Section 33 (1) Data of public interest whose publication is rendered mandatory under this Act shall be made available to the general public on an internet website in digital format, without restriction, without personal identification, in a form capable of being printed and copied without loss or distortion of data even in parts, and free of charge in respect of inspecting, downloading, printing, copying and transmitting through network (hereinafter "electronic publication"). Access to the 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 on their websites the data specified in the publication schemes referred to in section 37:

a) the Sándor Palace, 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 government committees, as well as the national chambers; and

d) capital and county government offices.

(3) Organs performing public duties other than those listed in paragraph (2) may, at their choice, fulfil their obligation of electronic publication under section 37 on their own website or on another website operated jointly with their associations or maintained by other organs responsible for their supervision, professional direction or operational coordination, or a central website set up for this purpose.

(4) Public upbringing institutions and vocational training institutions shall fulfil their 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, in accordance with section 35, transfer the data to be published to the data publisher, which shall ensure that the data are published on the website, and that it is made clear from which organ individual published data of public interest originate or to which they pertain.

(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 a continuous operation of the website, recovery from breakdowns and the updating of data.

(3) The website used for publication shall offer comprehensible information about 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 schemes, other data of public interest and data accessible on public interest grounds may also be published electronically on the website used for publication.

Section 35 (1) The head of the data source organ subject to electronic publication obligation shall ensure that the data included in the publication schemes specified in section 37 are accurate, kept up to date, published on an ongoing basis, and sent to the data publisher.

(2) The data publisher shall be responsible for the electronic publication, continuous availability, authenticity and keeping up to date of the data sent.

(3) The data source and the data publisher shall determine in internal regulations the detailed rules for fulfilling their obligations 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 publication obligation shall lie with the legal successor of that organ.

Section 36 The publication of data specified in the publication schemes referred to in section 37 shall be without prejudice to the obligations 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 "organ subject to publication obligation") shall, with the exception set out in paragraphs (4) and (4a), publish the data pertaining to their activities as specified in the general publication scheme referred to in Annex 1 in the way defined in Annex 1.

(2) For certain 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 sets of data may be rendered mandatory by the head of the organ subject to publication obligation after seeking the opinion of 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 parts of such agencies (hereinafter "organ-specific publication schemes").

(4) The Government, after seeking the opinion of the Authority, shall determine in a decree the set of data to be published by the national security services.

(4a) Entities publishing on the platform within the meaning of section 37/C may publish their data specified in points 3, 4 and 6 of the table "III. Financial management data" in Annex 1 also using the platform.

(5) Where the organ subject to publication obligation operates as a collegiate organ, that collegiate organ shall be competent to determine or amend the organ-specific publication schemes after seeking the opinion of the Authority.

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

(7) The publication scheme may also determine the frequency of publication, considering the type of data to be published.

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

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

Section 37/A (1) For the purpose of providing fast and easy access to data published electronically, a central electronic register published on a website created for this specific purpose and operated by the Minister responsible for the implementation of infrastructure requirements for administrative information technology systems shall contain cumulatively all data concerning the websites containing data of public interest of organs that are obliged under this Act to electronically publish data of public interest, as well as concerning the databases and records maintained by such organs.

(2) Electronic access based on uniform criteria to the data of public interest of organs referred to in paragraph (1) and the capability of retrieving data of public interest shall be ensured by the integrated public data retrieval system 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 containing data of public interest that are handled by it be transferred to the Minister responsible for the implementation of infrastructure requirements for administrative information technology systems, and the data of public interest thus transferred be 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 public data retrieval system as well as for having such data updated on a regular basis.

(2) Maintaining a register of databases and records containing data of public interest and linking up with the integrated public data retrieval system shall not exempt the data source from the obligation of electronic publication.

24/B. Central Information Register of Public Data

Section 37/C (1) To ensure transparency in the use of public funds, budgetary organs under the Act on public finances not including national security services (hereinafter "entities publishing on the platform") shall publish, on a bi-monthly basis and in a manner ensuring availability for at least ten years from publication, data specified in paragraph (2) broken down as specified in paragraph (3) on the platform of the Central Information Register of Public Data (hereinafter the "platform") maintained by an organ designated in a decree by the Government and available to everyone in accordance with the requirements set out in section 33 (1), which allows for machine readability, bulk download and the data to be sorted, searched, extracted and compared.

(2) Entities publishing on the platform shall publish on the platform data relating to

a) budgetary support provided pursuant to the Act on public finances, except if before publication the budgetary support is withdrawn or the beneficiary renounces budgetary support;

b) contracts on supplies, works, services, sale and exploitation of assets, transfer of assets or rights of pecuniary value and granting concession, with the exception of data on procurements for defence and security purposes and classified data as well as data on procurements under section 9 (1) b) of Act CXLIII of 2015 on public procurement (hereinafter the "Public Procurement Act") and the resulting contracts;

c) payments made for purposes other than the performance of their core tasks, and in particular, payments made to support associations, to professional and employees' representative organs of their employees, to support organisations facilitating educational, cultural, social and sports activities of their employees and care recipients, and related to tasks performed by foundations,

provided that their extent exceeds five million forints and they are implemented by them from national or European Union funds.

(3) The entities publishing on the platform shall publish the data specified in paragraph (2) with the following breakdown, also indicating the ratio of the national and European Union funds used:

a) in a situation under paragraph (2) a) or c),

aa) designation (type) of contract, name or, for persons other than natural persons, designation and seat of beneficiary, tax number, subject of support, place and start and end date of implementation of the support programme, and, where applicable, date of payment, amount and currency of support, and

ab) for State aid covered by a binding legal act of the European Union specified in Annex 2, in addition to the data specified in subpoint aa), classification of beneficiary, classification of sector of the activity in which the aid is used or, where no such activity can be identified, the sectoral classification of the beneficiary's main activity, specification of the form of the aid, the date of award of the aid, specification of the category of aid under the government decree on state aid procedure within the meaning of EU competition law and the regional aid map, and reference number issued by the European Commission of the aid;

b) in a situation under paragraph (2) b),

ba) designation (type) of contract, subject-matter, name(s) or, for persons other than natural persons, designation(s), seat(s) of the contracting party (parties), tax number, subject-matter and value of contract, place and start and, for contracts concluded for a definite period, end date of the performance of the contract; and

bb) for a public procurement or procurement procedure, in addition to the data specified in subpoint ba), name(s) of tenderer(s), individual reference number recorded in the Electronic Public Procurement System under the Public Procurement Act (EPPS identifier) with the relevant link, name(s) of named subcontractor(s) and, where its (their) fee is set, the fee amount(s) and a reference if the public procurement or the procurement, including procurements not exceeding the national threshold under the Public Procurement Act, is financed in whole or in part from EU funds.

(4) For the purposes of paragraph (2) b), value of contract means the consideration, calculated without value added tax, agreed upon for the subject-matter of the contract or, for transactions free of charge, the market or book value of the asset, whichever is higher. As regards periodically recurring contracts concluded for a period exceeding one year, the calculation of value shall be based on the amount of consideration for one year. The values of contracts concerning the same subject-matter concluded with the same contracting party in the same financial year shall be counted together.

(5) Detailed rules on the maintenance and operation of the platform and on publications on the platform shall be determined by the Government in a decree.

Chapter V

NATIONAL AUTHORITY FOR DATA PROTECTION AND FREEDOM OF INFORMATION

25. 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 implementation of the right to personal data protection and the right of access to data of public interest and data accessible on public interest grounds, as well as for 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 in accordance with the provisions of the General Data Protection Regulation and of this Act.

(2b) In contentious and non-contentious proceedings intended to lead to 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 processing operations performed by the court in accordance with the relevant provisions.

(2c) For natural persons and legal entities under the jurisdiction of Hungary, the tasks and powers specified in the Data Governance Act for the competent authority for data intermediation services and the competent authority for the registration of data altruism organisations shall be exercised by the Authority in accordance with the provisions of the Data Governance Act and of this Act.

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

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

b) shall conduct authority proceedings for data protection on the application of the data subject and *ex officio*;

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

d) may bring proceedings before the court in connection with any infringement concerning data of public interest and data accessible on public interest grounds;

e) may intervene in actions brought by others;

f) shall conduct authority proceedings for transparency upon notification and *ex officio*;

g) shall conduct proceedings for the authorisation of processing upon application;

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 as well as other tasks provided for in Acts;

i) shall perform the tasks of the competent authority for the registration and supervision of data intermediation services providers and the competent authority for the registration and supervision of data altruism organisations specified in the Data Governance Act.

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

a) may make recommendations with respect to the adoption and 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 opinions with respect to draft laws affecting its functions;

b) shall make public an account on its activities each year by 31 March, and shall submit this account to the National Assembly;

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

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

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

f) shall organise the conference of data protection officers;

g)

h)

(5) The Authority shall be an independent organ subject to the law only; it may not be instructed in its functions and shall carry out its responsibilities 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 heading-related powers, and its budget shall form a separate title within the budget heading of the National Assembly.

(2) The total expenditure and total revenue in the annual budget of the Authority may be reduced by the National Assembly only, with the exception of temporary measures adopted to prevent natural disasters endangering life and property and the consequences of such disasters as defined in the Act on public finances, and of measures adopted by the Authority within its own subject-matter competence or in its subject-matter competence as a governing organ.

(3) A fine imposed by the Authority shall constitute revenue for the central budget.

(4) The Authority may use the remainder of its revenues from the previous year in the following years to carry out its tasks.

27. President of the Authority

Section 40 (1) The Authority shall be led by a president. The president of the Authority shall be appointed by the President of the Republic on a proposal from the Prime Minister from among Hungarian citizens with a law degree who have the right to stand as candidate at the election of Members of the National Assembly, and have at least ten years' professional experience in auditing procedures related to data protection or freedom of information, or hold an academic degree in either of those fields.

(2) A person may not be appointed as president of the Authority if in the four-year period before the proposal for appointment is put forward he served as Member of the National Assembly, national minority advocate, Member of the European Parliament, President of the Republic, member of the Government, political director of the Prime Minister, state secretary, local government representative, mayor or deputy mayor, mayor or a deputy mayor of the capital, president or vice-president of a county assembly, member of a national minority self-government, or officer or employee of a political party.

(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 the oath before the President of the Republic, reciting the wording laid down in the Act on the oath and affirmation of certain public law officers.

Section 41 (1) The president of the Authority may not be a member of a political party, may not engage in political activity, and his mandate shall be incompatible with any other state and local government office or mandate.

(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, lecturing and artistic activities, activities falling under copyright protection, reviewer and editorial activities, and the activities performed in an employment relationship as foster parent.

(3) The president of the Authority may not be an executive officer and supervisory board member of a company, nor may he be a member of a company who is required to provide personal assistance.

Section 42 (1) The president of the Authority shall make a declaration of assets within thirty days of his appointment. The rules relating to the declaration of assets of the Members of the National Assembly shall apply accordingly to that declaration of assets, with the derogations provided for in this Act.

(2) Should the president of the Authority fail to make the declaration of assets, he shall not be allowed to exercise his office and shall not receive remuneration until his declaration of assets is submitted.

(3) A public, page-for-page copy of the declaration of assets of the president of the Authority shall be published on the website of the Authority without delay. The declaration of 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.

(3a)

(4) Anyone may apply to the Prime Minister for the initiation of proceedings regarding the declaration of assets of the president of the Authority by making a statement of facts concerning the specific content of the declaration that clearly identifies the contested part and content of the declaration. If the application does not meet the requirements specified in this paragraph or is manifestly unfounded, or if a repeatedly submitted application does not indicate new facts or data, the Prime Minister shall reject the application without conducting a proceeding. The Prime Minister shall assess the veracity of the information supplied in the declaration of assets.

(5) Upon a call by the Prime Minister in the proceeding regarding the declaration of assets, the president of the Authority shall supply in writing the data supporting the circumstances as regards assets, income and economic interests indicated in the declaration of assets to the Prime Minister without delay. The Prime Minister shall send the data to the President of the

Republic to inform him of the outcome of the verification. Only the Prime Minister and the President of the Republic may inspect the data.

(6) The supporting data submitted by the president of the Authority shall be erased on the thirtieth day following the conclusion of the proceeding regarding the declaration of assets.

Section 43 (1) The president of the Authority shall be entitled to remuneration equal to two and a half times the amount of the honorarium of a Member of the National Assembly as set out in Act XXXVI of 2012 on the National Assembly.

(1a) In addition to the remuneration set out in paragraph (1), the president of the Authority shall be entitled to the same benefits as a Minister.

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

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

(2) The period of the mandate of the president shall be considered time spent at an administrative organ under a public service relationship.

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 it is established that the conditions for his appointment are not met or the provisions regarding the declaration of assets are violated;

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

f)

g)

(2) The president of the Authority may 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 after the communication of resignation, on the day indicated in the resignation, or, failing this, on the day of communication of the resignation. Acceptance of the resignation shall not be required to make it effective.

(3) If the president of the Authority does not eliminate incompatibility or conflict of interest under section 41 within thirty days from appointment, or if a cause of incompatibility or conflict of interest arises concerning him while in office, the President of the Republic shall, upon a motion from the Prime Minister, decide on the issue of incompatibility or conflict of interest.

(4)

(5)

(6) The President of the Republic, upon a motion from the Prime Minister, shall be responsible for establishing if the requirements for the appointment of the president of the Authority are not met. Where the president of the Authority has knowingly misrepresented substantial data or facts in his declaration of assets, the President of the Republic shall, upon a motion from the Prime Minister, establish the violation of the provisions on the declaration of assets.

(6a) Simultaneously with sending it to the President of the Republic, the Prime Minister shall send the motion made under paragraphs (3) and (6) also to the president of the Authority.

(6b) The president of the Authority may bring an administrative action to have the court establish that the motion is unfounded. No application for excuse shall be accepted for failing to meet the time limit for bringing the action. The court shall act in accordance with the rules governing court proceedings relating to public service relationship, with the proviso that the action shall be brought against the Prime Minister, and fall within the exclusive jurisdiction of the court of the place where the work is carried out. 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, after an action is brought by the president of the Authority under paragraph (6b), the court finds in its final and binding judgment that the motion made by the Prime Minister under paragraphs (3) and (6) is unfounded, the President of the Republic shall not establish the termination of the mandate of the president of the Authority.

(6d) The President of the Republic shall decide on the motion made by the Prime Minister 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 as at the time of termination.

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

Section 45/A The president of the Authority may attend and address the sittings of the committees the National Assembly.

28. Vice-president of the Authority

Section 46 (1) The president of the Authority shall be assisted by two vice-presidents appointed by the president of the Authority for an indefinite term. The president of the Authority shall exercise the employer's rights in respect of the vice-presidents.

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

(3) The provisions of section 41 shall apply accordingly to the incompatibility and conflict of interest of the vice-president.

(4) If the president is prevented from acting or if the office of the president is vacant, the vice-presidents shall exercise the powers and perform the duties of the president in a manner determined by the president.

Section 47 The provisions of section 42 shall accordingly apply to the obligation of the vice-president to make a declaration of assets and to the proceeding regarding his declaration of assets, with the proviso that in the proceeding regarding the vice-president's declaration of assets, the president of the Authority shall act in place of the Prime Minister and there shall be no need to inform the President of the Republic of the outcome of the proceeding.

Section 48 (1) The vice-president shall be entitled to remuneration equal to that of a deputy state secretary as set out in the Remuneration Table in point I of Annex 1 to Act CXXV of 2018 on government administration, with the amount determined by the president of the Authority.

(1a) In addition to the remuneration set out in paragraph (1), the vice-president shall be entitled to the same benefits as a deputy state secretary.

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

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

(4) The period of the mandate of the vice-president shall be considered time spent at an administrative organ under a public service relationship.

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

a) upon his resignation;

b) upon his death;

c) if it is established that the conditions for his appointment are not met;

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

e) upon his dismissal;

f) upon his removal from office.

(2) The vice-president of the Authority may resign from office at any time by tendering his resignation in writing to the president of the Authority. The mandate of the vice-president of the Authority shall terminate after the communication of resignation, on the day indicated in the resignation, or, failing this, on the day of communication of the resignation. Acceptance of the resignation shall not be required to make it effective.

(3) If the vice-president of the Authority does not eliminate incompatibility or conflict of interest under section 41 within thirty days from appointment, or if a cause of incompatibility or conflict of interest arises concerning him while in office, the president of the Authority shall decide on the issue of incompatibility or conflict of interest.

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

(5) The president of the Authority may dismiss the vice-president of the Authority; at the same time, the vice-president of the Authority shall be offered a public official position and, even if the requirements set out in section 51 (1) are not met, the post of an investigator at the Authority.

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

(7) The fact that the requirements for the appointment of the vice-president of the Authority are not met shall be established by the president of the Authority.

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

29. Personnel 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 may, up to twenty per cent of the core headcount of the Authority, appoint as investigators public officials and employees of the Authority with higher education degree who have been in a public service relationship or an employment relationship with the Authority for at least five years.

(2) Investigators shall be appointed for an indefinite term; the president of the Authority may revoke such appointment at any time, without giving reasons.

(3) The remuneration, additional annual leave and other emoluments to which investigators are entitled shall be determined in accordance with the provisions on the head of a separate department.

Chapter VI

AUTHORITY PROCEDURES

30. Authority inquiries

Section 51/A (1) If the bringing of authority proceedings 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 apply to the Authority for the initiation of an inquiry by making a notification thereto. In the notification, the data subject shall indicate the data that prove that he has sought to exercise his rights under section 14 vis-à-vis the controller.

Section 52 (1) Anyone may apply to the Authority for the initiation of an inquiry by making a notification claiming that an injury has occurred relating to the processing of personal data or the exercise of the right of access to data of public interest or data accessible on public interest grounds, or there is an imminent threat of such an injury.

(1a) Where notification is based on a cause specified in section 31 (1), the inquiry of the Authority may be applied for within one year from the communication of the refusal of the request, or the expiry of the time limit with no result, or the expiry of the time limit for the payment of the fee.

(1b) The Authority shall not commence an inquiry into compliance with the obligation of publication under subtitle 24/B, a notification made to this effect shall be deemed to be a notification for the initiation of authority proceedings for transparency under section 63/A (2).

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

(3) No one shall suffer prejudice on account of having made a notification to the Authority. The Authority shall not reveal the notifier's identity unless the inquiry cannot be carried out otherwise. If so requested by the notifier, the Authority shall not reveal the notifier's identity, even if the inquiry cannot be carried out otherwise. The Authority shall inform the notifier of this consequence.

(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 on the merits the notifications.

(2) The Authority may reject the notification without examining it on its merits if

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

b) the notification is anonymous.

(3) The Authority shall reject 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 manifestly unfounded;

d) the re-submitted notification contains no new substantial facts or data;

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

f) the notification does not meet the requirements set out in section 51/A (2);

g) it is carrying out an administrative audit or an authority proceeding concerning the subject matter of the notification; or

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

(4) If the notification was made by the Commissioner for Fundamental Rights, the Authority may reject it without examination on the merits only 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 inquiry if

a) the request should have been rejected without examination on the merits pursuant to paragraphs (3) to (4), but it acquired knowledge of the cause of rejection only after the commencement of the inquiry;

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

(5a) Upon instituting authority proceedings for transparency under subtitle 33/A *ex officio*, the Authority shall terminate the inquiry or, if it finds during the inquiry that the entity publishing on the platform is likely not to fulfil its obligation of publication under subtitle 24/B, the specific part of the inquiry. The notifier shall be notified of termination accordingly in accordance with section 63/A (2).

(6) The Authority shall notify the notifier of the refusal to examine the notification on the merits, the termination of inquiry, and the reasons for refusal or termination.

(7) Where a notification relates to a case which does not fall within its subject-matter competence and there is sufficient information available to determine the competent organ, the Authority shall transfer the notification to the organ competent to act in the notified case, and shall at the same time notify the notifier thereof. Where, as a result of a notification that relates to a case which does not fall within its subject-matter competence, the Authority finds that court proceedings may be brought in the case, it shall notify the notifier of this.

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

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

a) shall be given access to, and may make copies of, all data processed by the controller under inquiry that are potentially associated with the case under inquiry, and shall have the right to inspect, and request copies of, all these documents, including documents stored in an electronic data-storage medium,

b) shall be given access to any processing operation potentially associated with the case under inquiry, shall be authorised to enter any premises where processing is carried out, and shall have access to any means used for the processing operations,

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

d) shall have the right to request written information from any organisation or person potentially associated with the case under inquiry and copies of any data and documents, including documents stored in an electronic data-storage medium, potentially associated with the case under inquiry, and

e) shall have the right to urge the head of the organ supervising the controller authority to conduct an inquiry.

(2) The controller under inquiry and the organisation or person affected by the procedural act shall be obliged to comply with the request of the Authority under paragraph (1) within the time limit set by the Authority. In a situation referred to in paragraph (1) d) and e), the time limit set by the Authority shall not be shorter than fifteen days.

(3) The requested person may refuse to provide information under paragraph (1) b) and c) if

a) the person affected by the notification giving rise to the inquiry by the Authority is a relative or former spouse of the requested person within the meaning of the Civil Code;

b) by providing information he would incriminate himself, or a relative or former spouse within the meaning of the Civil Code of committing a criminal offence, as regards a related question.

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

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

aa) shall take a measure specified in sections 56 and 57,

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

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

b) shall establish that no injury has occurred and an imminent threat of it does not exist, and shall conclude the inquiry.

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

a) the period between a call for the communication of data necessary for the clarification of the facts of the case and its fulfilment,

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

c) the period of time over which circumstances obstruct or malfunctions or other unavoidable events make impossible the functioning of the Authority for at least a whole day.

(2) The Authority shall notify 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, and the commencement of authority proceedings.

(3) If the Authority concludes, in accordance with paragraph (1) b), its inquiry carried out on the basis of notification under section 51/A (2), it shall inform the notifier, simultaneously with the notification under paragraph (2), of the possibility to exercise the relevant right to legal remedy in court.

Section 56 (1) If the Authority establishes that an injury relating to the processing of personal data or concerning the exercise of the right of access to data of public interest or data accessible on public interest grounds has occurred or that there is an imminent threat of it, it shall call upon the controller to remedy the injury or to eliminate the imminent threat of it.

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

(3) If the call referred to in paragraph (1) produced no result, and the controller authority has a supervisory organ, the Authority may make a recommendation to the controller's supervisory organ, while also informing the controller organ thereof. In the absence of a call referred to in paragraph (1), the Authority may directly make a recommendation to the supervisory organ of

the controller if it is of the opinion that this is a more effective way to remedy the injury or to eliminate the imminent threat of injury.

(4) The supervisory organ shall inform in writing the Authority about its standpoint on the merits of the recommendation and the measures taken within thirty days from receiving the recommendation.

Section 57 If, as a result of its inquiry, the Authority finds that the injury or its imminent threat is attributable to an unnecessary, ambiguous or inappropriate provision of a law or public law regulatory instrument, or the lack or deficiency of the legal regulation of issues related to processing, then, to prevent such injury and its imminent threat in the future, the Authority may make recommendations to the organ authorised to make law or issue public law regulatory instrument or to the entity in charge of the preparation of 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 notify the Authority of its position or the measure taken in conformity with the recommendation within sixty days.

Section 58 (1) If the call or recommendation referred to in section 56 does not result in remedying the injury or eliminating its imminent threat, the Authority shall decide on further necessary measures to be taken within thirty days following the expiry of the time limit for information specified in section 56 (2) or, if a recommendation was made, in section 56 (4).

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

a) shall or may bring authority proceedings for data protection in accordance with section 60;

b) shall or may bring authority proceedings for the supervision of data classification in accordance with section 62;

c) may bring court proceedings in accordance with section 64; or

d) may draw up a report in accordance with section 59.

(3) The Authority shall notify 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) The Authority may draw up a report on the inquiry conducted on the basis of notification if no proceedings have been brought by the Authority or the court in the case.

(2) The report shall contain the facts revealed by 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. A report that contains classified data or secrets protected by an Act shall be published in such a way that the classified data or the secrets protected by an Act cannot be accessed.

(4) The report made by the Authority on its inquiry into the activities of organs authorised to gather information secretly or to use covert means shall not contain any data that may allow for conclusions to be drawn about the secret information gathering or the use of covert means in the given case.

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

32. Authority procedure for data protection

Section 60 (1) To give effect to the right to personal data protection, the Authority shall bring authority proceedings for data protection on the application of the data subject and may bring authority proceedings for data protection *ex officio*.

(2) An application for an authority proceeding for data protection may be submitted in the cases referred to in Article 77 (1) of the General Data Protection Regulation and section 22 b) of this Act.

(3) The Authority shall *ex officio* bring authority proceedings for data protection if

a) as a result of its inquiry it finds that an injury relating to the processing of personal data has occurred or there is an imminent threat of it, and, following the call or recommendation referred to in section 56, the injury has not been remedied or its imminent threat has not been eliminated within the time limit set by the Authority,

b) as a result of its inquiry it finds that an injury relating to the processing of personal data has occurred or there is an imminent threat of it, and a fine may be imposed according to the provisions of the General Data Protection Regulation.

(4) If the authority proceeding for data protection was preceded by an inquiry of the Authority initiated upon notification, the Authority shall notify the notifier of the commencement and conclusion of the authority proceeding for data protection.

(5) In the case referred to 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) specification of the alleged infringement,

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

c) the data available to the applicant 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 evidence of such facts, and

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

(6) In authority proceedings 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 proceedings for data protection shall be one hundred and fifty days; this time limit shall not include the period between a call for the communication of data necessary for the clarification of the facts of the case and its fulfilment.

(2) The Authority shall suspend the authority proceeding 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.

(2a) In addition to the cases specified in the Act on the Code of General Administrative Procedure, the Authority may suspend an authority proceeding conducted by it also if

a) deciding a question that arose in the course of the proceeding falls within the subject-matter competence of another organ or person, or

b) the case in question cannot be reasonably decided in the absence of another decision or proceeding by the Authority that is closely related to the case in question.

(2b) The Authority shall communicate its procedural decision on the suspension of the proceeding to also the other organ or person referred to in paragraph (2a), and shall at the same time request it to provide information on the completion of the proceeding.

(2c) All time limits shall be interrupted by the suspension of the proceedings, and shall start again, with the exception of the administrative time limit, when suspension is terminated.

(3) If the Authority establishes, at any stage of a proceeding instituted upon application, that it has no jurisdiction, it shall reject the application or terminate the proceeding.

(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 procedural decision rejecting the application or terminating the proceeding 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 about how to enforce rights before the supervisory authority with jurisdiction.

(6) If within ninety days of submission of the application the Authority did not terminate the authority proceeding for data protection nor did it make a decision on the merits of the case, it shall notify the applicant of the procedural acts taken up to the date of notification.

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

a) may apply the legal consequences specified in the General Data Protection Regulation concerning the processing operations specified in section 2 (2) and (4) of this Act and, in particular, it may order, on request or *ex officio*, the erasure, in a manner specified by the Authority, of unlawfully processed personal data or it may impose a temporary or definitive limitation on processing in another way,

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

ba) establish that the personal data have been unlawfully processed,

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

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

bd) prohibit the unlawful processing of personal data,

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

bf) order the provision of information to the data subject if the controller unlawfully omitted or refused to do so, and

bg) impose a fine,

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

(2) The Authority may order its decision, including the identification data of the controller or processor, to be published if

a) the decision concerns a wide scope of persons,

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

c) the gravity of the injury justifies publication.

(3) A warning shall not be issued in the proceedings of the Authority if it establishes on the basis of the provisions relating to its discretionary power that a fine needs to be imposed.

(4) The amount of the fine may range from one hundred thousand forints to 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 an authority proceeding for data protection is a budgetary organ.

(5) When deciding whether to impose a fine pursuant to paragraph (1) b) bg) and deciding on 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 any previous infringement concerning the processing of personal data established in respect of the infringer.

(6) The data affected by the processing operation in dispute shall not be erased or destroyed until 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 adoption of the final and binding court decision.

(7) The enforcement of the Authority's decision with regard to the obligation specified in the decision to perform a specific act, to engage in a specific conduct, or of tolerating or discontinuing shall be effectuated by the Authority. Unless otherwise required by the court, prosecution service, or another authority, if a criminal proceeding, another authority proceeding or court proceeding is pending regarding data that are affected by the unlawful processing operation established in a decision with administrative finality of the Authority or in case of an administrative court action, in its decision adjudicated with final and binding effect by the administrative court, those data shall not be erased or destroyed from the date of commencement of the criminal proceeding until the completion of the criminal proceeding with a final and binding conclusive decision of the court or a non-conclusive court order that reached administrative finality or until the decision terminating the proceeding against which no further legal remedy is available is adopted by the prosecution service or investigating authority, or in the case of another authority proceeding or court proceeding, from the date of commencement of this proceeding until its conclusion with administrative finality or final and binding effect.

(8) The payment obligation set forth in the Authority's decision may not be reduced (hereinafter "reduction") at the request of the party subject to the obligation. The party subject to the obligation may request a deferral or performance in instalments of the payment obligation or the obligation referred to in paragraph (7) (hereinafter jointly "performance relief"). The party subject to the obligation shall present evidence in the request that a cause beyond his control makes it impossible for him to perform within the time limit or that it would be disproportionately burdensome for him.

(9) If the party subject to the obligation submits the request under paragraph (8) after the enforcement of the Authority's decision is ordered, the Authority may allow a performance relief only if the cause that made it impossible to perform the obligation within the time limit was beyond the control of the party subject to the obligation.

(10) In assessing a request for reduction or performance relief submitted in respect of a payment obligation established in the Authority's decision, the state tax and customs authority shall act in accordance with section 110 of Act CLIII of 2017 on enforcement procedures to be effectuated by the tax authority.

Section 61/A (1) As a provisional measure to prevent the unlawful processing of personal data, the Authority may require also the hosting service provider or the intermediary service provider providing also hosting services (hereinafter the "party subject to the removal obligation") within the meaning of the Act on certain issues of electronic commerce services and information society services that processes the data published through an electronic communications network (for the purposes of this Act hereinafter "electronic data") to temporarily remove the electronic data the publication of which serves as grounds for an authority proceeding for data protection or administrative audit by the Authority if in the absence thereof, the delay would cause an unavertable and severe violation of the right to personal data protection and

a) the data subject of the published data is a child, or

b) the published data is sensitive data or criminal personal data.

(2) A procedural decision on the temporary removal of electronic data shall be communicated to the party subject to the removal obligation without delay. The party subject to the removal obligation shall be obliged to temporarily remove the electronic data within one working day from the communication of the procedural decision on the provisional measure by the Authority.

(3) The Authority shall end the temporary removal of electronic data and order the electronic data to be restored if the grounds for ordering the temporary removal ceased to exist.

(4) The temporary removal of electronic data shall terminate upon concluding with administrative finality the authority proceeding for data protection of the Authority or closing the administrative audit.

(5) In a situation under paragraph (3) or (4), the Authority shall oblige the party subject to the removal obligation to restore the electronic data.

(6) A procedural decision on the restoration of electronic data shall be communicated to the party subject to the removal obligation without delay. The party subject to the restoration obligation shall be obliged to restore the electronic data within one working day of the procedural decision being communicated to that party.

(7) A procedural decision under paragraph (6) shall be served on the person entitled to dispose of the data only if that person's identity and contact details are known from the data of the proceeding available at that time.

(8) An independent legal remedy shall be available against a decision on the temporary removal of electronic data.

(9) The Authority may impose a procedural fine ranging from one hundred thousand forints to twenty million forints on a party subject to the removal obligation that fails to comply with its obligation set out in this section.

Section 61/B (1) As a provisional measure to prevent the unlawful processing of personal data, the Authority may order that the electronic data the publication of which serves as grounds for an authority proceeding for data protection or administrative audit by the Authority be rendered temporarily inaccessible.

(2) The electronic data may be rendered temporarily inaccessible where in the absence thereof, the delay would cause an unavertable and severe violation of the right to personal data protection, and any other measures, including temporary removal by the Authority under section 61/A (1) remained ineffective, and

a) the data subject of the published data is a child, or

b) the published data is sensitive data or criminal personal data.

(3) The Authority shall communicate a procedural decision ordering the electronic data to be rendered temporarily inaccessible by public notice. The public notice shall be published on the website of the Authority for five days. The day of the communication of the procedural decision shall be the third day following publication on the website.

(4) An obligation imposed by the procedural decision of the Authority under paragraph (1) shall apply to all electronic communications service providers without the need for an explicit provision to that effect.

(5) The National Media and Infocommunications Authority (hereinafter the "NMHH") shall organise and monitor the implementation of rendering the electronic data temporarily inaccessible in compliance with the Act on electronic communications.

(6) The Authority may impose a procedural fine ranging from one hundred thousand forints to twenty million forints on an electronic communications service provider that fails to comply with its obligation set out in this section.

Section 61/C (1) The obligation to render the electronic data temporarily inaccessible shall terminate on the day when

a) the notification referred to in paragraph (2) is published if the authority proceeding for data protection terminates, the Authority terminates the authority proceeding for data protection, or the Authority concludes the administrative audit without launching an authority proceeding for data protection in the case; or

b) the decision of the Authority reaches administrative finality if the Authority, in its decision, obliges the controller or the processor to erase the electronic data.

(2) The Authority shall publish the dates specified in paragraph (1) a) and b) by public notice.

(3) The Authority shall terminate rendering the electronic data temporarily inaccessible by a procedural decision if

a) the reason for ordering it ceased to exist, or

b) the coercive measure of rendering electronic data temporarily inaccessible or the measure of rendering electronic data permanently inaccessible was ordered or is being implemented as regards the electronic data according to information provided by the court, prosecution office or investigating authority proceeding in the criminal case, or the NMHH.

(4) The provisions of section 61/B (3) shall apply accordingly to a procedural decision under this section.

(5) An independent legal remedy shall be available against a decision on rendering electronic data temporarily inaccessible.

Section 61/D (1) In the course of the enforcement referred to in section 61 (7), the Authority may order the temporary removal of electronic data or rendering electronic data temporarily inaccessible also if

a) publishing the electronic data is unlawful pursuant to the provisions of a decision by the Authority that reached administrative finality,

b) the Authority ordered the erasure of data concerning electronic data referred to in point a), and

c) the controller or processor required to erase the electronic data fails to comply with its erasure obligation despite a repeated call by the Authority.

(2) The Authority shall order the electronic data to be temporarily removed or to be rendered temporarily inaccessible pursuant to paragraph (1) for the period until the date of erasure of the electronic data, and shall notify

a) those to whom it communicated its procedural decision ordering the electronic data to be temporarily removed, and

b) by public notice those to whom it communicated its procedural decision ordering the electronic data to be rendered temporarily inaccessible of that date.

(3) The provisions of section 61/A (2), (8) and (9) shall apply accordingly to the temporary removal of electronic data pursuant to paragraph (1), while the provisions of section 61/B (3) to (6) and section 61/C (5) shall apply accordingly to rendering electronic data temporarily inaccessible pursuant to paragraph (1).

(4) The rules set out in the Act on judicial enforcement shall apply accordingly to the temporary removal of electronic data and to rendering electronic data temporarily inaccessible ordered pursuant to paragraph (1).

33. Authority procedure for the supervision of data classification

Section 62 (1) If as a result of an inquiry by the Authority or for other reasons it can be substantiated that the classification of national classified data or repeating the classification marking is unlawful, the Authority may bring an authority proceeding for the supervision of data classification.

(1a) If the court applies to the Authority for the initiation of an authority proceeding for the supervision of data classification in accordance with the provisions of section 31 (6a), the Authority shall bring an authority proceeding for the supervision of data classification.

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

(2)

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

(3) An authority proceeding for the supervision of data classification shall be instituted only *ex officio;* even if it was preceded by an inquiry of the Authority initiated upon notification or it was initiated upon application from the court in accordance with section 31 (6a), an authority proceeding for the supervision of data classification shall not be deemed a proceeding instituted upon application. If, however, the authority proceeding for the supervision of data classification was preceded by an inquiry of the Authority initiated upon notification, the notifier shall be notified of the commencement and conclusion of the authority proceeding for the supervision of data classification.

(4) In authority proceedings for the supervision of data classification, the following shall be considered a party to the proceeding:

a) the classifier where proceedings aim to examine whether classification was unlawful,

b) the entity repeating classification marking where proceedings aim to examine whether repeating the classification marking was unlawful.

(5) For clarifying the facts of the case in an authority proceeding for the supervision of data classification, the witness, the expert and the holder of the object of the inspection may be interviewed, even if that person has not been exempted from the obligation of confidentiality with respect to the national classified data under inquiry.

(6) The administrative time limit in authority proceedings for the supervision of data classification shall be ninety days; this time limit shall not include the period between a call for the communication of data necessary for the clarification of the facts of the case and its fulfilment.

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

a) if it finds that the laws relating to the classification of national classified data have been infringed,

aa) shall instruct the classifier to modify, in accordance with the law, the classification level or date of validity of the national classified data or to have it declassified, or

ab) shall establish that the classification of the national classified data has not been lawfully established and instruct the classifier to take the appropriate measures to eliminate the unlawful situation

b) if it finds that the laws relating to repeating the classification marking of national classified data have been infringed, shall instruct the entity repeating classification marking to repeat the classification marking of the national classified data in accordance with the law or to put an end to the use of the repeated classification marking, or

c) shall establish that the classifier acted in compliance with the laws relating to the classification of national classified data or the entity repeating classification marking acted in compliance with the laws relating to repeating the classification marking.

(2) The classifier may challenge the decision of the Authority under paragraph (1) a) within sixty days of it being communicated, and the entity repeating classification marking may challenge the decision of the Authority under paragraph (1) b) within sixty days of it being communicated. The submission of the statement of claim shall have suspensory effect on the becoming effective of the decision.

(2a) If the classifier does not turn to the court within sixty days of the communication of the decision of the Authority under paragraph (1) a) or the entity repeating classification does not turn to the court within sixty days of the communication of the decision of the Authority under paragraph (1) b),

a) in the case of a decision under paragraph (1) a) aa), the classification of the national classified data shall cease or its classification level or date of validity shall be modified in accordance with the decision on the sixty-first day following the communication of the decision,

b) in the case of a decision under paragraph (1) a) ab), the classification marking of the national classified data shall cease in accordance with the decision from the sixty-first day following the communication of the decision, or

c) in the case of a decision under paragraph (1) b),

ca) the repeated classification marking shall cease in accordance with the decision on the sixty-first day following the communication of the decision, provided that the decision instructs the entity repeating classification marking to put an end to the use of the repeated classification marking of the national classified data, or

cb) the classification level or date of validity of the repeated classification shall be modified in accordance with the decision on the sixty-first day following the communication of the decision, provided that the decision instructs the entity repeating classification marking to repeat the classification marking in accordance with the law.

(2b) The classifier and the entity repeating classification marking shall fulfil the obligation of notification provided for in section 8 (3) and (3a) of Act CLV of 2009 on the protection of classified data by the sixty-first day following the communication of the decision where paragraph (1) a) or b) applies, or without delay after the decision becoming final and binding if the decision is challenged in accordance with paragraph (2).

(2c) In addition to the cases specified in the Act on the Code of General Administrative Procedure, the Authority may suspend an authority proceeding for the supervision of data classification conducted by it also if

a) deciding a question that arose in the course of the proceeding falls within the subject-matter competence of another organ or person, or

b) the case in question cannot be reasonably decided in the absence of another decision or proceeding by the Authority that is closely related to the case in question.

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

(4)

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

(6) Only a judge who had been subjected to national security vetting in accordance with the Act on national security services may act in such an action.

(7) In the course of an action 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 corresponding to the classification level of the data.

33/A. Authority procedure for transparency

Section 63/A (1) To ensure compliance with the obligation of publication under subtitle 24/B, the Authority shall bring authority proceedings for transparency upon application and may bring authority proceedings for transparency *ex officio*. The provisions of the Act on the Code of General Administrative Procedure shall apply to these proceedings in accordance with the provisions of this Act.

(2) Anyone may make a notification for an authority proceeding for transparency. An authority proceeding for transparency shall be deemed a proceeding instituted *ex officio* even if it was preceded by a notification. The Authority shall notify the notifier of the commencement and conclusion of the authority proceeding for transparency.

(3) The Authority shall bring authority proceedings for transparency *ex officio* if it finds during its inquiry relating to the exercise of the rights of access to data of public interest or data accessible on public interest grounds that the entity subject to the obligation of publication under subtitle 24/B is likely not to have fulfilled its obligation of publication.

(4) If the authority proceeding for transparency was preceded by an inquiry initiated upon notification under paragraph (3), the Authority shall notify the notifier of the commencement and conclusion of the authority proceeding for transparency.

(5) In the case referred to in paragraph (2), the notification shall contain the following:

a) specification of the alleged infringement,

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

c) the data available to the notifier necessary for the identification of the controller committing the alleged infringement who is an entity publishing on the platform according to subtitle 24/B,

d) the facts that substantiate the statements related to the alleged infringement.

Section 63/B (1) The administrative time limit in authority proceedings for transparency shall be forty-five days.

(2) In its decision adopted in the authority proceeding for transparency, relating to the obligations of publication under subtitle 24/B, the Authority

a) may establish the existence of infringement relating to the obligation of publication on the part of the controller subject to the obligation of publication, including where publication took place with inaccurate data or was incomplete,

b) shall in the context of point a) order the obligation of publication under subtitle 24/B to be fulfilled as a matter of priority but within no more than 15 days, including the publication of real data and the provision of the data missing from published data.

(3) If the organ subject to the obligation of publication under subtitle 24/B does not comply with the obligation thus established within the time limit set in paragraph (2) b), the Authority may impose a fine. The amount of the fine shall range from one hundred thousand forints to fifty million forints.

(4) When deciding whether to impose a fine pursuant to paragraph (3) and deciding on the amount of the fine, the Authority shall take all circumstances of the case into account, in particular the gravity of the infringement, including the number of data affected by the failure and the period of time of the infringement, as well as any previous infringement established in respect of the infringer concerning the obligation of publication under subtitle 24/B.

(5) The Authority may order its decision to be published together with the data of the controller subject to the obligations of publication under subtitle 24/B if the gravity of the injury justifies publication.

34. Court action brought by the Authority

Section 64 (1) If the controller does not comply with the call under section 56 (1), the Authority may bring an action for infringement in respect of data of public interest and data accessible on public interest grounds within thirty days following the expiry of the time limit for information under section 56 (2), asking the court to require the controller to act in accordance with the call of the Authority.

(2) The subject-matter and territorial jurisdiction of the court shall be established in accordance with to section 31 (5).

(3) It shall be for the controller to prove that the processing complies with the law.

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

(5) Upon request the court may order its judgment to be published together with the identification data of the controller if this is necessary for data protection and the protection of the interests of the freedom of information and the rights protected under this Act of a larger number of data subjects.

34/A. Procedure for the authorisation of processing

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

a) for the approval of the draft codes of conduct, extensions or amendments 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 what is required by the Act on the Code of General Administrative Procedure, the application referred to in

a) paragraph (1) a) shall contain the draft code of conduct, extension or 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 determined in a ministerial decree shall be paid for a proceeding for the authorisation of processing.

Section 64/C (1) The administrative time limit in proceedings for the authorisation of 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 a proceeding for the authorisation of 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 during the period of suspension as well.

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

(4) A summary procedure shall not be applied in a case for authorisation of processing.

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

a) shall

aa) approve the draft code of conduct, extension or 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.

34/B. Procedure for the registration of data intermediation services providers and the issuance of official certificate regarding compliance

Section 64/E (1) The Authority shall register any data intermediation services provider who intends to provide the services referred to in Article 10 of the Data Governance Act in accordance with the provisions laid down in this subtitle. The register of data intermediation services providers shall contain the data referred to in Article 11 (6) of the Data Governance Act. The data processed in the register shall constitute data accessible on public interest grounds.

(2) In addition to what is required by the Act on the Code of General Administrative Procedure, an application for registration referred to in paragraph (1) shall contain the data referred to in Article 11 (6) of the Data Governance Act. In proceedings for registration referred to in paragraph (1), the administrative time limit shall be seven days.

(3) At the request of the data intermediation services provider, the Authority shall issue an official certificate (hereinafter the "compliance certificate") to confirm that the registered data intermediation services provider complies with the conditions laid down in Articles 11 and 12 of the Data Governance Act, with the proviso that notwithstanding the Act on the Code of General Administrative Procedure, the intended use of the compliance certificate need not be indicated in the application. In proceedings for the issuance of compliance certificate, the administrative time limit shall be 150 days.

(4) In conducting a proceeding referred to in paragraph (3), the Authority may, in addition to the cases specified in the Act on the Code of General Administrative Procedure, suspend its authority proceeding also if

a) deciding a question that arose in the course of the proceeding falls within the subject-matter competence of another organ or person, or

b) the case in question cannot be reasonably decided without another decision or proceeding by the Authority that is closely related to the case in question.

(5) The Authority shall communicate its procedural decision on the suspension under paragraph (4) of the proceeding referred to in paragraph (3) to also the other organ or person referred to in paragraph (4), requesting to be informed accordingly once the proceeding is completed.

(6) All time limits shall be interrupted by the suspension under paragraph (4) of the proceeding referred to in paragraph (3) and shall start again, with the exception of the administrative time limit, when suspension is terminated.

(7) An administrative service fee determined in a ministerial decree shall be paid for a proceeding for registration referred to in paragraph (1) and the issuance of compliance certificate.

(8) The data intermediation services providers registered by the Authority shall notify any change in the data referred to in paragraph (1) to the Authority within fourteen days from the change occurring. The rules governing the procedure for registration shall apply to the procedure for notification of change.

(9) Any data intermediation services provider registered by the Authority that ceases its activities shall notify the Authority thereof within fifteen days from the day of the cessation of activities, and the Authority shall remove this data intermediation services provider from the register.

(10) The Authority shall notify the European Commission of each notification, notification of change and removal under this subtitle without delay in accordance with the provisions of the Data Governance Act, in the manner specified in a decree by the Government.

34/C. Procedure for the supervision of data intermediation services providers

Section 64/F (1) If a request to this effect is made, the Authority shall institute a proceeding for the supervision of data intermediation services providers to monitor compliance with the requirements laid down in Chapter III of the Data Governance Act; otherwise it may *ex officio* institute a proceeding for the supervision of data intermediation services

(2) In the case referred to in paragraph (1), the application shall contain, in addition to what is required by the Act on the Code of General Administrative Procedure, the following:

a) specification of the alleged infringement,

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

c) the data available to the applicant necessary for the identification of the data intermediation services provider committing the alleged infringement,

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

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

(3) In proceedings for the supervision of data intermediation services providers, the administrative time limit shall be one hundred and fifty days; this time limit shall not include the period between a call for the communication of data necessary for the clarification of the facts of the case and its fulfilment.

(4) If the Authority establishes, at any stage of a proceeding instituted upon application, that it has no jurisdiction, it shall reject the application or terminate the proceeding.

(5) If within ninety days from the submission of the application the Authority did not terminate the proceeding for the supervision of data intermediation services providers, nor did it make a decision on the merits of the case, it shall notify the applicant of the procedural acts taken up to the date of notification.

(6) In its decision adopted in a proceeding for the supervision of data intermediation services providers, the Authority may apply the legal consequences specified in the Data Governance Act or may impose a fine. The amount of the fine shall range from one hundred thousand forints to fifty million forints.

(7) If in conducting a proceeding for the supervision of data intermediation services providers, the Authority finds that there is no need to terminate the proceeding, and it cannot be established either that the behaviour of the monitored data intermediation services provider is not unlawful, the Authority shall send to the monitored data intermediation services provider its preliminary position on the case, which shall include the established facts of the case, the supporting evidence, an assessment of the facts of the case, as well as a description of the essence of the considerations and conclusions necessary for taking the decision, and of the considerations intended to be taken into account in a possible imposition of a fine. The monitored data intermediation services provider may make a statement or observations as to the preliminary position within thirty days.

(8) In deciding whether it is justified to impose a fine pursuant to paragraph (5) and in determining the amount of the fine, the Authority shall take all circumstances of the case into account, in particular the gravity of the infringement, including the duration of the infringing situation, and whether the infringing party was previously in the proceeding for the supervision of data intermediation services providers found to have committed an infringement in the context of its activities.

(9) The Authority may order its decision, including the identification data of the data intermediation services provider, to be made public if the gravity of the injury justifies publication.

(10) If the Authority applies a legal consequence under Article 14 (4) b) or c) of the Data Governance Act or receives a notification about the rectification of an infringement referred to in paragraph (8), it shall notify the European Commission thereof in the manner specified in a decree by the Government without delay.

(11) The Authority shall cooperate with the supervisory authorities referred to in the Data Governance Act in accordance with the provisions of the Data Governance Act.

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

(13) The provisions of section 61 (7) to (10) shall apply accordingly to proceedings for monitoring data intermediation services providers for compliance.

34/D. Procedure for the registration of data altruism organisations

Section 64/G (1) If the organisation concerned so requests, the Authority shall register an organisation that meets the requirements laid down in Article 18 of the Data Governance Act in accordance with the provisions laid down in this subtitle. The register of data altruism organisations shall contain the data referred to in Article 19 (4) of the Data Governance Act.

(2) In addition to what is required by the Act on the Code of General Administrative Procedure, an application for registration referred to in paragraph (1) shall contain the data referred to in Article 19 (4) of the Data Governance Act. In proceedings for registration, the administrative time limit shall be eighty four days.

(3) An administrative service fee determined in a ministerial decree shall be paid for a proceeding for registration referred to in paragraph (1).

(4) The data altruism organisations registered by the Authority shall notify any change in the data referred to in Article 19 (4) of the Data Governance Act to the Authority within fourteen days from the change occurring. The rules governing the procedure for registration shall apply to the procedure for notification of change.

(5) The Authority shall notify the European Commission of each registration of a data altruism organisation, any subsequent notification of change and its removal from the registration without delay in accordance with the provisions of the Data Governance Act, in the manner specified in a decree by the Government.

(6) To ensure the transparency of the activities of data altruism organisations, the Authority shall make public the information referred to in Article 19 (4) a), b), f), g) and h) of the Data Governance Act until a change in the data is notified. The data made public as such by the Authority as well as the information referred to in Article 19 (4) d) and e) of the Data Governance Act made public on the website of the data altruism organisation in accordance with Article 19 (4) f) of the Data Governance Act shall constitute data accessible on public interest grounds.

(7) A data altruism organisation registered by the Authority shall transmit an annual activity report pursuant to Article 20 (2) of the Data Governance Act to the Authority each year by 31 January. For the purpose of keeping data subjects and controllers informed, the Authority shall make public the activity reports. The data contained in the activity reports made public by the Authority shall constitute data accessible on public interest grounds.

34/E. Procedure for the supervision of data altruism organisations

Section 64/H (1) If a request to this effect is made, the Authority shall institute a proceeding for the supervision of data altruism organisations to monitor compliance with the requirements laid down in Chapter IV of the Data Governance Act; otherwise it may *ex officio* institute a proceeding for the supervision of data altruism organisations.

(2) In the case referred to in paragraph (1), the application shall contain, in addition to what is required by the Act on the Code of General Administrative Procedure, the following:

a) specification of the alleged infringement,

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

c) the data available to the applicant necessary for the identification of the data altruism organisation committing the alleged infringement,

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

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

(3) In proceedings for the supervision of data altruism organisations, the administrative time limit shall be one hundred and fifty days; this time limit shall not include the period between a call for the communication of data necessary for the clarification of the facts of the case and its fulfilment.

(4) If the Authority establishes, at any stage of a proceeding instituted upon application, that it has no jurisdiction, it shall reject the application or terminate the proceeding.

(5) If within ninety days from the submission of the application the Authority did not terminate the proceeding for the supervision of data altruism organisations, nor did it make a decision on the merits of the case, it shall notify the applicant of the procedural acts taken up to the date of notification.

(6) In its decision adopted in a proceeding for the supervision of data altruism organisations, the Authority may apply the legal consequences specified in the Data Governance Act or may impose a fine. The amount of the fine shall range from one hundred thousand forints to fifty million forints.

(7) If in conducting a proceeding for the supervision of data altruism organisations, the Authority finds that there is no need to terminate the proceeding, and it cannot be established either that the behaviour of the monitored data altruism organisation is not unlawful, the Authority shall send to the monitored data altruism organisation its preliminary position on the case, which shall include the established facts of the case, the supporting evidence, an assessment of the facts of the case, as well as a description of the essence of the considerations and conclusions necessary for taking the decision, and of the considerations intended to be taken into account in a possible imposition of a fine. The monitored data altruism organisation may make a statement or observations as to the preliminary position within thirty days.

(8) In deciding whether it is justified to impose a fine pursuant to paragraph (6) and in determining the amount of the fine, the Authority shall take all circumstances of the case into account, in particular the gravity of the infringement, including the duration of the infringing situation, and whether the infringing party was previously in the proceeding for the supervision of data altruism services providers found to have committed an infringement in the context of its activities.

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

(10) The provisions of section 61 (7) to (10) shall apply accordingly to proceedings for the supervision of data altruism organisations.

35. International cooperation

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

(2) In the framework of the cooperation set forth in paragraph (1), the Authority may request the authority of a third country or an international organisation to provide legal assistance, and, with the exception laid down in section 67, shall comply with the requests for legal assistance received from the authority of a third country or an international organisation, provided that this is allowed under an agreement on legal assistance in administrative matters concluded between the third country or international organisation and Hungary, another international treaty, national law or a legal act of the European Union.

Section 66 The Authority shall refuse to comply with a request for legal assistance received from an authority of a third country or an international organisation and shall inform the authority of the third country or the international organisation about the reasons for refusal if complying with the request for legal assistance

a) does not fall within its functions and powers,

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

c) would impair the fundamental right of a 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 Article 50 of Directive (EU) 2016/680.

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

a) the public official or employee member of the personnel of the Authority designated by the president of the Authority to participate in a joint operation shall participate in exercising, in the territory of another EEA State, the tasks and powers conferred 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 participate in 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 in accordance with the law of Hungary.

Section 68 If data or documents need to be acquired or other procedural acts need to be carried out for complying with a request not linked directly to any proceeding pending before the Authority, received from the authority of a third country or an EEA State or from an international organisation, the Authority shall conduct an administrative audit for this purpose. In such a case, the audit shall be concluded with a procedural decision by the Authority on transferring the 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 for concluding the agreement on the conduct of certification, the consideration to be provided for certification, and the process of the conduct of certification, together with the criteria for certification.

(3) The Authority shall determine, in proportion to the volume of activity to be performed, the conditions for concluding the agreement on the conduct of certification and the consideration to be provided. The consideration to be provided for the conduct of certification shall be revenue of the Authority.

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

a) the name of the controller 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) If, in the course of its proceedings, the Authority detects a suspicion of a criminal offence, it shall apply to the competent organ for the initiation of criminal proceedings. If, in the course of its proceedings, the Authority detects a reasonable suspicion of the commission of an infraction or disciplinary offence, it shall apply to the organ competent to conduct infraction or disciplinary proceedings for the initiation of infraction or disciplinary proceedings.

(2) The organ referred to in paragraph (1) shall inform the Authority of its views regarding the initiation of proceedings within thirty days, unless otherwise provided by an Act, and of the outcome of the proceedings within thirty days from the conclusion of the proceedings.

38. Other rules applicable to the proceedings of the Authority; processing and confidentiality

Section 70/A (1) An administrative audit shall not be carried out on an application of the controller or the processor.

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

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

a) regarding the decisions published under section 61 (2):

aa) the identification data of the controller or processor,

ab) specification of the infringement,

ac) specification of the legal consequence applied,

b) regarding the decisions specified in section 64/D a):

ba) the identification data of the applicant,

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

bc) specification of the temporal effect where the Authority's decision is effective for a fixed term,

c) regarding the data protection officer notified to the Authority:

ca) name,

cb) postal and electronic mail address,

cc) name of the controller or processor represented by the data protection officer.

(2) The data under paragraph (1) shall constitute 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 becoming ineffective, or

ab) until the expiry of ten years after the authentic copy of the decision is issued,

b) the data specified in paragraph (1) b) until the date of the decision becoming ineffective,

c) the data specified in paragraph (1) c) until a change in the data is notified.

Section 70/C Data whose publication or disclosure by the Authority is rendered mandatory under a binding legal act of the European Union or this Act shall be made available to the general public on the Authority's website in digital format, without restriction, without personal identification, in a form capable of being printed and copied without loss or distortion of data even in parts, and free of charge in respect of inspecting, downloading, printing, copying and transmitting through network.

Section 71 (1) In the course of its proceedings, the Authority may process, to the extent and for the duration necessary for the conduct of the proceedings, personal data, as well as data classified as secret protected by law and secret related to the exercise of a profession, that are related to the proceedings and the processing of which is necessary for the effective conduct of the proceedings.

(1a) If the controller lawfully restricted, or is entitled to restrict, in accordance with an Act or a binding legal act of the European Union, the data subject's rights under Articles 13 to 18 and 21 of the General Data Protection Regulation and under section 14 of this Act then, in the context of its proceedings, the Authority

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

b) shall perform the notifications that it is required under this Act to make to the data subject in a manner and at a time

that ensures that the interests that may serve as a basis for lawfully restricting the data subject's rights are not impaired.

(1b) At the request of the Authority, the local government clerk of a settlement shall verify the actual circumstances of processing activity carried out in the area of its territorial competence specified by the Authority in its request, in particular the scope of the processed personal data, the operations performed 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 and other means of evidence that it lawfully acquired during its proceedings also for the purposes of its other proceedings.

(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 protected data processed by the Authority during an inquiry or an authority proceeding shall be blocked after the closure of the inquiry or after the decision closing the proceeding has reached administrative finality. Blocked data may be retained until the disposal of the documents of the case or until their handing over to the archives for preservation; with the exception of the use under paragraph (2), they may only be processed for the purpose of enforcing the decision with administrative finality, monitoring the implementation of the decision, or legal remedies or review related to the decision with

administrative finality, and they may only be made accessible to the court, other organ or person entitled to process or access such data in the manner and in the scope specified in an Act.

(3) In its proceedings under this Act, the Authority may access 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 "Commissioner for Fundamental Rights Act") in accordance with section 23 (7) of the Commissioner for Fundamental Rights Act.

(3a) The Authority may without regard to paragraph (3) access the data specified in section 23 (3) e), (4) f), and (5) d) of the Commissioner for Fundamental Rights Act if this is necessary

a) in any inquiry,

b) in any authority proceeding for data protection, or

c) in any authority proceeding for the supervision of data classification

commenced in connection with the protection of the personal data of the participating person.

(3b) The Authority may without regard to paragraph (3) access the data specified in section 23 (3) f) and (4) g) of the Commissioner for Fundamental Rights Act which allow the identification of persons using devices and methods for secret information gathering or the use of covert devices if this is necessary

a) in any inquiry,

b) in any authority proceeding for data protection, or

c) in any authority proceeding for the supervision of data classification

commenced in connection with the protection of the personal data of these persons.

(3c) If a document that the Authority intends to examine contains data which the Authority may access only in accordance with paragraph (3), access to the document shall be granted to the Authority with the data that must not be accessed made unrecognisable.

(4)

(5) With the exception of data provision to other organisations prescribed by an Act, the president and vice-president of the Authority as well as any person who is or was in a public service relationship or another employment-related relationship with the Authority shall, during, and following the termination of, their legal relationship, keep confidential the personal data, classified data and data classified as secret protected by law and secret related to the exercise of a profession which have come to their knowledge in connection with the activities and the performance of the activities of the Authority, as well as all data, facts and circumstances that the Authority is not obliged, by virtue of an Act, to make available to the public.

(6) As a result of their being subject to the confidentiality obligation, the persons referred to in paragraph (5) shall not disclose, use or reveal to third parties data, facts and circumstances which have come to their knowledge in connection with the performance of their activities without being authorised to do so.

Chapter VI/A

MONITORING PROCESSING OPERATIONS OF COURTS

Section 71/A (1) In contentious and non-contentious proceedings intended to lead to a judicial decision (hereinafter the "main case"), the monitoring of the implementation of the right to personal data protection in the context of processing operations performed by the courts in accordance with the relevant provisions shall take place through data protection complaints (hereinafter the "complaint").

(2) In accordance with the procedural rules applicable to the main case, where

a) the rules of the criminal or infraction procedure apply to the main case, section 143 (3) and section 144 (3) and (8) a) of Act XC of 2017 on the Code of Criminal Procedure,

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

c) points a) and b) do not apply, section 157 (3) and section 158 (3) and (6) of Act CXXX of 2016 on the Code of Civil Procedure or, where Act III of 1952 on the Code of Civil Procedure (hereinafter the "1952 Civil Procedure Code") applies to the main case, section 114/A (4) and section 114/B (3) and (6) of the 1952 Civil Procedure Code

shall apply to the adjudication of the complaint with the derogations laid down in this chapter.

(3) The complaint shall be lodged with the court proceeding in the main case in writing, addressed to the court with subject-matter jurisdiction to adjudicate the complaint.

(4) The party, the accused and other participants of the proceedings, in particular the aggrieved party, the private party, the witness and the expert, shall be entitled to lodge a complaint; anyone else may lodge a complaint only if he substantiates his legal interest upon lodging the complaint.

Section 71/B (1) Once a complaint is lodged, the court shall examine whether the proceeding judge, lay judge or judicial employee complied with the provisions of the national and Union law relating to personal data protection during his processing activities.

(2) The data subject may lodge a complaint claiming that

a) an injury relating to the processing of his personal data has occurred or there is an imminent threat of it, or

b) the controller has acted unlawfully with respect to his data subject rights specified in the General Data Protection Regulation or in section 14 of this Act.

(3) In the complaint under paragraph (2) b), the data subject shall indicate the data that prove that he has sought to exercise his data subject rights vis-à-vis the controller.

(4) If the court proceeding in the main case finds the complaint well-founded, it shall take, within eight days, the necessary measures to mitigate the consequences of the injury or to eliminate the threat of the injury, and at the same time it shall notify the complainant thereof and of the measures taken, and inform him that, should he maintain, despite the measures taken, the complaint, he may submit a statement thereon in writing within eight days from the receipt of the notification.

(5) If the court proceeding in the main case has not taken any measure referred to in paragraph (4), or if the data subject has submitted a statement referred to in paragraph (4), the court proceeding in the main case shall, for the adjudication of the complaint, refer the necessary documents, including its statement on the complaint, to the court with subject-matter jurisdiction to adjudicate the complaint within eight days.

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

Section 71/C (1) The court adjudicating the complaint shall, by 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 acquired knowledge of the cause of rejection only after starting to examine the merits of the case.

(2) If the court adjudicating the complaint has not rejected or dismissed the complaint in accordance with paragraph (1), it shall, by reasoned decision, within two months from the date of referral of the complaint and the necessary documents of the case to it,

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

b) establish that point a) applies or there is an imminent threat of it, and

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

bb) shall order the controller to take measures to give effect to the data subject rights guaranteed by the General Data Protection Regulation or this Act, or

c) establish that no injury has occurred or there is no imminent threat of it, and dismiss the complaint.

(3) In proceedings related to the complaint, in the interest of the consistent application of the provisions relating to personal data protection, the court proceeding in the main case and the court adjudicating the complaint may seek the opinion of the Authority.

(4) The time limit open for the court to handle the complaint shall not include the following:

a) the period between a call for the communication of data necessary for the clarification of the facts of the case, or a call for seeking the opinion of the Authority under paragraph (3), and the fulfilment of such a call,

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

c) the day when any circumstances, malfunction or other 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), (2) and (3) shall apply to the procedure of the court adjudicating the complaint with regard to any matter not regulated in this chapter.

Chapter VI/B

MONITORING OF THE TRANSPARENCY OF DATA OF PUBLIC INTEREST AND DATA ACCESSIBLE ON PUBLIC INTEREST GROUNDS AND THE COMPLIANCE WITH THE REQUIREMENTS FOR THEIR ACCESSIBILITY

Section 71/D (1) In addition to exercising its functions and powers under this Act, the Authority shall twice a year monitor compliance with the requirements for transparency of data of public interest and data accessible on public interest grounds and for the accessibility of data of public interest and data accessible on public interest grounds at organs performing public duties, local governments and publicly owned companies (for the purposes of this section hereinafter jointly the "organs") on the basis of the data provided by the organs to the Authority in accordance with the paragraph (4) (for the purposes of this chapter hereinafter the "monitoring").

(2) In case a notification to this effect is made, the Authority shall conduct the monitoring in respect of the organ affected by the notification also separately. Anyone may make a notification for monitoring.

(3) A notification referred to in paragraph (2) shall contain the following:

a) specification of the alleged infringement,

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

c) data necessary for the identification of the organ committing the alleged infringement,

d) facts that support the statements related to the alleged infringement.

(4) The organs shall provide data to the Authority by 31 January of each year regarding the following:

a) number of requests for access to data of public interest and data accessible on public interest grounds complied with and for which compliance was refused as well as the common reasons for refusal,

b) average number of days required for compliance with requests for access to data of public interest and data accessible on public interest grounds, and

c) access to published data of public interest and data accessible on public interest grounds.

(5) The Authority may request data from the monitored organs as necessary for conducting monitoring. The monitored organs shall be required to comply with such requests for data provision within 8 days from receiving the request.

(6) Monitoring by the Authority shall cover the examination of the publication of data of public interest and data accessible on public interest grounds.

(7) The Authority may make recommendations to the monitored organs with a view to promoting compliance with the requirements for transparency of data of public interest and data accessible on public interest grounds and for the accessibility of data of public interest and data accessible on public interest grounds. The head of the organ affected by the recommendation shall draw up an action plan for the implementation of the necessary measures and shall transmit this plan to the Authority within 15 days from the receipt of the recommendation.

(8) The Authority shall, as part of its account referred to in section 38 (4) b), draw up annually a report on the monitoring.

Chapter VII

FINAL PROVISIONS

Section 72 (1) Authorisation shall be given to the Government to determine in a decree

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

b) after seeking the opinion of the Authority, the amount of the fee payable in connection with requests for data of public interest, and the limits for the amounts that can be determined pursuant to section 29 (3);

c) the compilation of sector-specific publication schemes;

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

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

f) the maintainer of the platform and the detailed rules for the operation of, and publication on, the platform;

g) the detailed rules for the notification of the European Commission as specified in the Data Governance Act;

h) after seeking the opinion of the Authority, the detailed procedural rules for the methodology of monitoring under chapter VI/B by the Authority.

(2) Authorisation shall be given to

a) the Minister vested with the relevant functions to determine in a decree sector-specific publication schemes with respect to organs under his control or supervision;

b) the Minister responsible for e-administration 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) Authorisation shall be given to the Minister responsible for justice to determine in a decree, after seeking the opinion of the Authority and in agreement with the Minister responsible for tax policy, the amount of the administrative service fee payable for the procedure for the authorisation of processing, as well as the detailed rules for collecting, managing, registering and refunding such fees.

(4) Authorisation shall be given to the Minister responsible for the consolidation of e-administration and IT developments to determine in a decree, after seeking the opinion of the Authority and in agreement with the Minister responsible for tax policy, the amount of the administrative service fee payable for the registration of data intermediation services providers and data altruism organisations, and for compliance certificates issued for data intermediation services providers, as well as the detailed rules for 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 Section 26 (2) and section 30 (7) of this Act as introduced 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 also to proceedings 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 proposal for the first president of the Authority to the President of the Republic by 15 November 2011. The President of the Republic shall appoint the first president of the Authority with effect from 1 January 2012.

Section 75 (1) Cases pending that are based on a submission filed with the Commissioner for Data Protection before 1 January 2012 shall be dealt with by the Authority in accordance with the provisions of this Act.

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

(3) For processing operations started before 25 May 2018, the review specified in section 5 (5) shall be carried out by 25 May 2021.

(4) Inquiries and authority proceedings for data protection launched by the Authority before the entry into force of Act XXXVIII of 2018 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 amending other connected Acts (hereinafter the "Amending Act") shall be carried out by the Authority by applying the provisions of Chapter VI as in force on the day preceding the day of entry into force of the Amending Act.

(5) The Authority shall block the data that were processed in the data protection register before the entry into force of the Amending Act and may use them only in proceedings launched in relation to processing operations performed prior to the entry into force of the Amending Act.

(6) The controller shall be exempt from the application of the provisions laid down in section 25/F (1) until 31 December 2022 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 performed 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 by taking into account the principle of proportionality, in particular by taking action to remedy an infringement by primarily issuing a warning to the controller or processor in accordance with Article 58 of the General Data Protection Regulation when the personal data processing provisions laid down in the national law or a binding legal act of the European Union are first infringed.

Section 75/B (1) The president and vice-president of the Authority shall, in accordance with section 42 (1) as introduced by Act XVIII of 2022 amending Act XXXVI of 2012 on the National Assembly and certain related Acts, make a declaration of assets by 5 August 2022 reflecting the situation on the day when the declaration of assets is made.

(2) The entity in charge of dealing with the declarations of assets shall retain the declarations of assets of the spouses, cohabitants and children of the president and vice-president of the Authority living in the same household with the president and vice-president of the Authority, respectively, that are kept by the entity in charge of dealing with the declarations of assets on the day of entry into force of Act XVIII of 2022 amending Act XXXVI of 2012 on the National Assembly and certain related Acts until 1 August 2023.

(3) To proceedings related to declarations of assets pending on the day of entry into force of Act XVIII of 2022 amending Act XXXVI of 2012 on the National Assembly and certain related Acts, the rules in force on the day of commencement of the proceeding shall apply.

Section 75/C (1) The president and vice-president of the Authority shall for the first time make a declaration of assets covering the information and in the form set out in Act LVI of 2022 amending, at the request of the European Commission, certain Acts for the successful conclusion of the conditionality mechanism procedure, reflecting the situation on 1 November 2022, by 31 January 2023 in accordance with the provisions introduced by Act XXXI of 2022 amending certain Acts on declaration of assets relating to the control of the use of European Union budget funds, attaching also the declarations of assets of their spouses, cohabitants and children living in the same household with them.

(2) To proceedings relating to declarations of assets pending on the day of entry into force of Act XXXI of 2022 amending certain Acts on declaration of assets relating to the control of the use of European Union budget funds, the rules in force on the day of commencement of the proceeding shall apply.

Section 75/D The maintainer of the platform shall establish the platform and publish the data sheet required for publication on the platform by 31 December 2022 at the latest. Entities publishing on the platform shall publish the data specified in section 37/C (2) on the platform continuously with the first publication taking place by 28 February 2023 at the latest.

Section 75/E With regard to section 37/C (3) b) bb), for procurements not exceeding the national threshold under the Public Procurement Act, the fact that the procurement was financed from EU funds shall be indicated for procurements implemented on or after 31 March 2023.

Section 75/F Section 31 (1), (4) and (6) and sections 31/A to 31/C as introduced by Act XL of 2022 amending Act CXII of 2011 on the right to informational self-determination and on the freedom of information in order to reach an agreement with the European Commission shall apply to requests for access to data of public interest submitted on or after 31 December 2022.

Section 75/G Section 62 (1) and (4) and section 63 (1) to (2c) as introduced by Act XXXII of 2023 amending Act CLV of 2009 on the protection of classified data and Act CXII of 2011 on the right to informational self-determination and on the freedom of information (hereinafter the "Amending Act 2") shall apply also to proceedings pending at the time of the entry into force of Amending Act 2.

Section 76 Chapter V and sections 75/B to 75/C of this Act qualify as cardinal on the basis of Article VI (4) 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) Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA;

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 77/B Subtitles 34/B to E, Chapter V and section 72 contain provisions for the implementation of Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act).

Section 78 (1) to (2)

(3) to (9)

Section 79

Section 80

Section 81

Section 82

Section 83

Section 84

Section 85

Section 86

Section 87

Section 88

Section 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 of each department	Immediately upon the change taking effect	Previous data to be erased
3	Name, position and contact information (telephone and fax number, electronic mail address) of the executive officers of the organ performing public duties as well as the executive officers of its departments	Immediately upon the change taking effect	Previous data to be erased
4	Name and contact information (telephone and fax number, electronic mail address) of the competent senior customer relations officer within the organisation and customer service hours	Immediately upon the change taking effect	Previous data to be erased
5	For a collegiate organ, number and composition, name, position and contact information of the members	Immediately upon the change taking effect	Previous data to be erased
6	Name and the data referred to in point 1 of any other organ performing public duties under the control, supervision or oversight of, or subordinated to, the organ performing public duties	Immediately upon the change taking effect	Previous data to be archived for a period of 1 year
7	Name, seat, contact information (postal address, telephone and fax number, electronic mail address) and scope of activities of any economic operator which is majority-owned by, or operates with the participation of, the organ performing public duties, name of its representative, share of 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, contact information (postal address, telephone and fax number, electronic mail address), deed of foundation and members of the administering organ of any public foundation established by the organ performing public duties	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 established by the organ performing public duties, reference to the law establishing the budgetary organ, or the decision on its establishment, deed of foundation, head, website	Immediately upon the change taking effect	Previous data to be archived for a period of 1 year

	address and operating permit of the budgetary organ		
10	Name of any newspaper founded by the organ performing public duties, name and address of its editor and publisher, 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 referred to in point 1 of the superior or supervisory organ of the organ performing public duties, or the organ competent to adjudicate appeals against its decisions, or, failing this, of the organ exercising legality control 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	Current unabridged text of the fundamental laws and public law regulatory instruments governing the responsibilities, subject-matter competence and core activities of the organ performing public duties, as well as the organisational and operational regulations or rules of procedure and the data protection and data security regulations of the organ	Immediately upon the change taking effect	Previous data to be archived for a period of 1 year
2	For organs with national territorial competence and capital and county government offices, information material in Hungarian and English on the duties and activities of the organ performing public duties	Immediately upon the change taking effect	Previous data to be erased
3	Tasks voluntarily undertaken by the local government	Quarterly	Previous data to be archived for a period of 1 year
4	Name of the organ having subject-matter competence in state administration, local government and other administrative cases, per case type and type of procedure; where powers are delegated, name and area of territorial competence of the organ that actually exercises the power; list of documents and certificates required for administrative procedures, procedural fees (administrative service fees), fundamental procedural rules, place and time for the submission of documents to institute proceedings, customer service hours, time limit for the administrative procedure (administrative time limit and time limit for filing an appeal), guidelines on administrative procedure, information about administration arrangements and the required forms for downloading, access to electronic programmes available for use, appointments, list of the laws linked to case types, information on client rights	Immediately upon the change taking effect	Previous data to be erased

	and obligations		
5	Name and contents of public services rendered by, or financed from the budget of, the organ performing public duties, rules relating to access to public services, amount of fees payable for public services and fee discounts	Immediately upon the change taking effect	Previous data to be archived for a period of 1 year
6	Descriptive information on databases and registers maintained by the organ performing public duties (name, format; purpose, legal basis and duration of processing, data subjects involved, sources of data, questionnaire, where applicable), identification data under this Act of registers to be reported to the data protection register; type of data collected and technically processed by the organ performing public duties as part of its core 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 the publicly available publications of the organ performing public duties, means of access, free of charge availability or price of the publication	Quarterly	Previous data to be archived for a period of 1 year
8	Decision preparation process of the collegiate organ, citizen participation method (public opinion), its procedural rules, place and time as well as publicity and decisions of the meetings of the collegiate organ, minutes or summaries of meetings; information on voting in the collegiate organ unless restricted by law	Immediately upon the change taking effect	Previous data to be archived for a period of 1 year
9	Draft laws and accompanying documents to be published pursuant to an Act; submissions submitted to a public meeting of the local government representative body from the time of submission	Unless otherwise provided by an Act, immediately after the time of submission	Previous data to be archived for a period of 1 year
10	Announcements and notices published by the organ performing public duties	Continuously	Archived for a period of at least 1 year
11	Technical specifications of tenders issued by the organ performing public duties, outcome and 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 core activity of the organ performing public duties	Without delay after consulting the examination report	Previous data to be archived for a period of 1 year
13	Procedure for handling requests for access to data of public interest, name and contact information of the	Quarterly	Previous data to be erased

	competent department, name of the person responsible for information rights		
14	Results of statistical data collection, prescribed by the law, relating to the activities of the organ performing public duties including the developments over time	Quarterly	Previous data to be archived for a period of 1 year
15	Data on the organ concerned resulting from the mandatory statistical data provision concerning data of public interest	Quarterly	Previous data to be archived for a period of 1 year
16	List of contracts for the exploitation of data of public interest to which the organ performing public duties is a party	Quarterly	Previous data to be archived for a period of 1 year
17	Standard contract terms for the use and exploitation of data of public interest processed by the organ performing public duties	Immediately upon the change taking effect	Previous data to be archived for a period of 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	List of public cultural data processed by the organ performing public duties that are available for re-use in accordance with the Act on the re-use of public data, with indication of the available formats, and information on the public data types processed by the organ performing public duties that are available for re-use in accordance with the Act on the re-use of public data, with indication of the available formats	Within 15 days from the change taking effect	Previous data to be archived for a period of 1 year
20	Standard contract terms for the re-use of public data and public cultural data referred to in point 19 in an electronically editable form	Within 15 days from the change taking effect	Previous data to be erased
21	General schedule of fees to be paid for making available for re-use public data and public cultural data referred to in point 19, including the items forming the base for fee calculation	Within 15 days from the change 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 data	Within 15 days from the change taking effect	Previous data to be erased
23	Indication of the parties to the arrangements granting exclusive right concluded by the organ performing public duties in accordance with the Act on the re-use of public data, period and subject of exclusivity, and other important elements of the arrangement	Within 15 days from the change taking effect	Previous data to be erased

24	Text of the arrangements concluded by the organ performing public duties that grant an exclusive right to digitise public cultural data in accordance with the Act on the re-use of public data	Within 15 days from the change taking effect	Previous data to be erased
25	Any law, public law regulatory instrument, public service contract or other binding document referred to in the Act on the re-use of public data (or reference whereby it can be accessed) that requires 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 change taking effect	Previous data to be erased

III. Financial management data

	Data	Updating	Storing
1	Annual budget, annual accounts under the Act on accounting or annual budget report of the organ performing public duties	Immediately upon the change taking effect	For 10 years following the time of publication
2	Consolidated data on the number and personal benefits of the staff employed at the organ performing public duties, and remuneration, wage and regular benefits as well as expenditure allowances of executives and senior officers, in total, type and amount of benefits provided to other employees, in total	Quarterly	Archived for a period defined by a separate law, but for at least 1 year
3	Data relating to the names of beneficiaries of budgetary support granted by the organ performing public duties in accordance with the Act on public finances, purpose and amount of support, as well as the place of implementation of the support scheme, except if before publication the budgetary support is withdrawn or the beneficiary renounces budgetary support	By the sixtieth day following the date of the decision	For 5 years following the time of publication
4	Name (type) and subject-matter of contracts on supplies, works, services, sale and exploitation of assets, transfer of assets or rights of pecuniary value and granting concession worth 5 million forints or more relating to the use of funds from the general government sector or the management of assets of the general government sector, name of the parties to the contract, value of the contract, duration if the contract is concluded for a definite period as well as any change to these data, with the exception of data on procurements for defence and security purposes and classified data as well as data on procurements under section 9 (1) b) of Act CXLIII of 2015 on public	By the sixtieth day following the date of the decision	For 5 years following the time of publication

	procurement and the resulting contracts Value of the contract means the consideration, calculated without value added tax, agreed upon for the subject-matter of the contract or, for gratuitous transactions, the market or book value of the assets, whichever is higher. As regards periodically recurring contracts concluded for a period exceeding one year, the calculation of value is to be based on the amount of consideration for one year. The values of contracts concerning the same subject-matter concluded with the same contracting party in the same financial year are to be counted together.		
5	Data accessible to the public according to the Act on concessions (tender notices, particulars of tenderers, evaluation memos, outcomes of tender procedures)	Quarterly	Archived for a period defined by a separate law, but for at least 1 year
6	Payments of more than five million forints made by the organ performing public duties for purposes other than the performance of its core tasks (in particular, payments made to support associations, to professional and employees' representative organs of their employees, to support organisations facilitating educational, cultural, social and sports activities of their employees and care recipients, and related to tasks performed by foundations)	Quarterly	Archived for a period defined by a separate law, but for at least 1 year
7	Description of developments implemented from European Union funding as well as 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

Annex 2 to Act CXII of 2011

List of the binding legal acts of the European Union in respect of which the data pursuant to section 37/C (3) a) ab) concerning State aids falling within their scope are to be published:

1. Commission Regulation (EU) No 651/2014 of 17 June 2014 declaring certain categories of aid compatible with the internal market in application of Articles 107 and 108 of the Treaty (OJ L 187, 26.6.2014, p. 1);

2. Commission Regulation (EU) 2017/1084 of 14 June 2017 amending Regulation (EU) No 651/2014 as regards aid for port and airport infrastructure, notification thresholds for aid for culture and heritage conservation and for aid for sport and multifunctional recreational infrastructures, and regional operating aid schemes for outermost regions and amending Regulation (EU) No 702/2014 as regards the calculation of eligible costs (OJ L 156, 20.6.2017, p. 1);

3. Commission Regulation (EU) 2020/972 of 2 July 2020 amending Regulation (EU) No 1407/2013 as regards its prolongation and amending Regulation (EU) No 651/2014 as regards its prolongation and relevant adjustments (OJ L 215, 7.7.2020, p. 3–6);

4. Commission Regulation (EU) 2021/1237 amending Regulation (EU) No 651/2014 declaring certain categories of aid compatible with the internal market in application of Articles 107 and 108 of the Treaty (OJ L 270, 29.7.2021, p. 39–75);

5. Commission Regulation (EU) No 702/2014 of 25 June 2014 declaring certain categories of aid in the agricultural and forestry sectors and in rural areas compatible with the internal market in application of Articles 107 and 108 of the Treaty on the Functioning of the European Union (OJ L 193, 1.7.2014);

6. Commission Regulation (EU) No 1388/2014 of 16 December 2014 declaring certain categories of aid to undertakings active in the production, processing and marketing of fishery and aquaculture products compatible with the internal market in application of Articles 107 and 108 of the Treaty on the Functioning of the European Union (OJ L 369, 24.12.2014, p. 37–63);

7. Council Regulation (EU) 2015/1589 of 13 July 2015 laying down detailed rules for the application of Article 108 of the Treaty on the Functioning of the European Union (OJ L 248, 24.9.2015);

8. Binding legal acts adopted by the European Commission in respect of Hungary in individual State aid cases other than those referred to in points 1 to 7.