Act CCXXII of 2015
on the general rules on electronic administration and trust services

The National Assembly, with a view to facilitating the wide uptake of electronic administration, accelerating procedures, easing administrative burdens, facilitating the use of electronic means in private law relationships and legal relationships between the State and citizens, ensuring cooperation between electronic administration organs, and facilitating the provision of modern and more efficient public services to citizens adopts the following Act:

PART ONE

INTRODUCTORY PROVISIONS

1. Interpretative provisions

Section 1 For the purposes of this Act,

1. *form submission support service* means a service that ensures the filling in by the client, and the submission with electronic identification to the electronic administration organ, of electronic forms complying with technical specifications determined by an organ or service provider designated by law;

2. *archive service* means a service for the long-term preservation of electronic documents, including trust services specified in Article 3(16)(c) of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (hereinafter "eIDAS");

3. *automatic information transfer* means the transfer of information by a cooperating organ transferring information without human intervention;

4. *automatic information transfer interface* means a technical solution for automatic information transfer created and operated by a cooperating organ transferring information;

5. *identification-based document authentication* means a service as part of which a service provider, as specified by law, assigns a statement provided by a client to a certified person, and then confirms that link in an authentic manner;

6. *internal records* means records kept exclusively for the own purposes, tasks, and control activities of the organ keeping those records, without any intent to transfer data to a third party and without qualifying as a source of information for third parties;

7. *trust service* means a service specified in Article 3(16) eIDAS;

8. *trust service policy* means a set of rules adopted by a trust service provider, relying party, or another person laying down the terms of using a trust service for groups of relying parties with certain common security requirements or for specific applications;

9. *trust service client* means a person who enters into a service contract with a trust service provider;

10. *trust service provider* means a trust service provider as defined in Article 3(19) eIDAS;

11. *secure electronic delivery service* means a delivery service that, with regard to the delivery of electronic communications, ensures compliance with all of the following requirements:

a) if a message received from a sender is made available to the addressee in an unaltered form, a confirmation recorded in an electronic document bearing at least an advanced electronic signature is available to the sender,

b) the message or the document confirming delivery cannot be changed undetectably in the course of, or after, delivery,

c) the message can be received only by the addressee or an authorised substitute recipient, and the identity of the actual recipient is confirmed by the receipt confirmation document,

d) documentary evidence (acknowledgement of receipt) is available to the sender even if delivery within a specified time limit is unsuccessful; the confirmation shall indicate the date and time of and, if known, reason for such failure;

12. *simple information transfer* means transfer of information, not qualifying as automatic information transfer, between cooperating organs;

13. *electronic identification* means the process described in Article 3(1) eIDAS;

14. *electronic payment* means

a) transfer from a payment account,

b) transfer made through an electronic payment and clearing system,

c) simplified electronic payment made through an electronic payment and clearing system,

d) payment by card,

e) payment by card made through an electronic payment and clearing system or POS terminal;

15. *electronic payment and clearing system* means a service offering options for electronic payment between payment accounts to member electronic administration organs and parties using their services in a manner specified by a decree by the Government;

16. *electronic information system* means a set of equipment (environmental infrastructure, hardware, network, and data-storage media) and software used for data and information processing;

17. *electronic administration organ* means

a) a state administration organ,

b) a local government,

c) any other legal entity authorised by law or a government decree to exercise administrative authority powers,

d) the National Office for the Judiciary or a court,

e) the Commissioner for Fundamental Rights,

f) the prosecution service,

g) a notary,

h) a bailiff or an independent bailiff's office,

i) a statutory professional body other than a wine community,

j) a public utility service provider,

k) a legal entity that performs or provides a public duty or service and is required by an Act or a government decree to allow for electronic administration, or

l) a legal entity, other than those referred to in subpoints *a)* to *k)*, who or which undertakes voluntarily to administer certain matters by electronic means pursuant to this Act, and ensures in compliance with the requirements set out in this Act, and notifies to the Electronic Administration Supervisory Authority, such administration;

17a. *State organ required to allow for electronic administration* means an organ specified in point 17 *a)*, *b)*, or *d)* to *f)*, or a legal entity at state or local government level referred to in point 17 *c)*, *k)*, or *l)*;

18. *Electronic Administration Supervisory Authority* (hereinafter "Supervisory Authority") means an organ designated by the Government as the entity responsible for the promotion and supervision of electronic administration, the cooperation between and coordination of cooperating organs, and the performance of tasks specified in the government decree issued for the implementation of this Act;

19. *electronic form filling service* means a service as part of which a service provider designated by law ensures the generation of electronic forms with data specified by an electronic administration organ, and allows such forms to be filled in, authenticated and submitted by clients;

20. *validation data* means data referred to in Article 3(40) eIDAS;

21. *validity chain* means a series of linked information relating to an electronic document or its hash (including in particular any certificate, certificate-related information, data used for generating a signature or seal, information on the current status or withdrawal of a certificate, and information on the validity data and withdrawal of such data relating to the service provider that issued the certificate) that can be used to determine if an advanced or qualified electronic signature, seal, or timestamp on an electronic document was valid at the time the signature, seal or timestamp was placed on the document;

22. *advanced electronic signature* means a signature as defined in Article 3(11) eIDAS;

23. *economic operator* means an economic operator, as defined in the Code of Civil Procedure, with its seat in Hungary, with the reservation that, for the purposes of this Act,

a) an association or foundation without a tax number shall not be considered an economic operator,

b) a foundation or association with a tax number shall be considered an economic operator as regards all matters;

24. *certificate policy* means a trust service policy concerning certificates issued as part of a trust service;

25. *information transfer* means the transfer and receipt of information among cooperating organs;

26. *information transfer service* means a service as part of which a cooperating organ transfers data or documents to another cooperating organ by simple or automatic information transfer;

27. *source of information* means a legal entity in possession of a given piece of information;

28. *applicable trust service requirements* means the requirements specified in eIDAS, the EU implementing acts of eIDAS, this Act, laws adopted based on an authorisation by this Act, the service policies and trust service policies of the trust service provider, and decisions passed by the trust service supervisory body regarding the trust service provider;

29. *legal representative* means, unless provided otherwise by law, an attorney-at-law, law office, or registered in-house legal counsel acting on behalf of the client;

30. *government communications service* means an electronic communications service provided to users specified by law through an electronic telecommunications network that is specified by law and qualifies as a government network as defined by the Act on electronic communications;

30a. *central government service* means an information technology, network, and infrastructure service, other than a regulated electronic administration service mandatorily provided by the Government or a central electronic administration service, provided as a central service through a central service provider designated by the State;

31. *central document authentication agent* means a central electronic administration service where a client or an administrator of an electronic administration organ can authenticate a document uploaded by him using an authentication method offered by the service;

32. *organ performing a public duty* means an organ, other than those falling within the scope of point 17, performing a public duty as defined in the Act on public documents, public archives, and the protection of private archival materials;

33. *public utility service provider* means an undertaking obliged by law to sell or provide goods or services, so that it provides, pursuant to this obligation, water utility services, district heating services, regular collection, gathering, removal, and disposal service for municipal solid

and liquid waste, chimney-sweeping services, universal postal services, services under an electricity purchase contract or network access contract to a user entitled to universal electricity service, or services under a natural gas trade agreement or distribution network access contract to a user entitled to universal natural gas service, provided that it issued at least 150 000 invoices per month in average for its services during the year preceding the relevant year;

34. *hash* means a string of bits of specified length linked to an electronic document, which is generated using a procedure (hashing procedure) that meets, at the time of generating the hash, all requirements laid down in the implementing decree to this Act;

35. *classified data* means classified data as defined in the Act on the protection of classified data;

36. *qualified trust service* means a service specified in Article 3(17) eIDAS;

37. *qualified trust service provider* means a service specified in Article 3(20) eIDAS;

38. *qualified electronic signature* means a signature specified in Article 3(12) eIDAS;

39. *data link register* means the data link register regulated under the Act on identification methods replacing personal identification numbers and on the use of identification codes;

40. *customisable electronic administration user interface* means an online application customisable by the client provided by a service provider designated by law, which allows identified parties to make statements and perform procedural acts and other obligations necessary for electronic administration, and use electronic administration services available to the client by way of a single interface;

41. *service policy* means a statement made by a trust service provider regarding the detailed procedural or other operational requirements for certain trust services;

42. *service contract* means a contract by and between a trust service provider and a trust service client establishing the terms and conditions of providing and using a trust service;

43. *certificate subject* means a person the identity or a characteristic of whom is certified by a trust service provider in a certificate, including in particular the signatory in the case of a certificate for electronic signature;

44. *certificate* means a certificate for electronic signature, a certificate for electronic seal, a certificate for website authentication, or an electronic attestation issued by a service provider as part of a trust service, which contains the validation data relating to the certificate and all related data required for using the certificate, and which electronic document is reliably protected against forgery using technology available at the time of issuance and during its validity period;

45. *durable data-storage medium* means a device that allows an addressee to store data addressed to him, and to display the stored data in unaltered form and with unaltered content, during the period corresponding to the purposes of such data. In particular, such devices include USB keys, CD-ROMs, DVDs, memory cards, and computer hard drives;

46. natural person means a natural person, as defined by the Act on the Civil Code, not acting as an economic operator;

47. *natural person certificate subject* means a natural person specified in a certificate, regardless of whether the certificate also certifies his power to represent, an entity other than a natural person; or any other relationship with such entity;

48. *client* means a person or other legal entity, other than an electronic administration organ or a member or employee of a proceeding electronic administration organ, who participates in a matter within the functions and powers of an electronic administration organ as, or as a representative of, a client, party, subject to the proceeding, other participant in the proceeding, or party relying upon the service.

PART TWO

GENERAL RULES ON ELECTRONIC COMMUNICATION BETWEEN ELECTRONIC ADMINISTRATION ORGANS AND CLIENTS

CHAPTER I

GENERAL PROVISIONS

2. The fundamental principles of electronic administration

Section 2 (1) Electronic administration organs shall administer matters within their functions and powers, as well as matters required for the use, cancellation, or modification of services they are required to provide by law (hereinafter jointly for the purposes of this Part "matter"), with their clients by electronic means pursuant to the provisions of this Part.

(2) A legal entity referred to in point 17 *l)* of section 1 may undertake to administer matters, as specified by the Government in a decree, by electronic means pursuant to this Act by notifying the Supervisory Authority.

(3) For the purposes of this Part,

a) an electronic administration organ qualifying as an economic operator, with regard to a private law relationship between that electronic administration organ qualifying as an economic operator and a public utility service provider,

b) an electronic administration organ qualifying as an economic operator, with regard to a private law relationship between that electronic administration organ acting as an economic operator and a legal entity specified in point 17 *k)* or *l)* of section 1,

c) a member or employee, with regard to a private law relationship between a public utility service provider, or a legal entity specified in point 17 *k)* or *l)* of section 1, and its employee or member

shall qualify as a client.

(4) For the purposes of this Part, an electronic administration organ, or a member or employee of such an organ, shall qualify as a client pursuant to this Act if proceeding as

a) a defendant, witness, interpreter, or expert in a criminal proceeding,

b) a party, witness, interpreter, or expert in an authority proceeding,

c) a party, witness, interpreter, or expert in a civil contentious or non-contentious proceeding,

d) an investigated person, witness, interpreter, or expert in an infraction proceeding,

e) a party, witness, interpreter, or expert in an administrative court action or other administrative court proceeding

conducted before the electronic administration organ.

(5) An electronic administration organ may also apply the provisions laid down in this Part to a matter not covered by paragraphs (1) to (4), provided that the given matter is related to its functioning.

Section 3 (1) In Hungary, a client shall be entitled to have his matters administered by an electronic administration organ by electronic means pursuant to this Act.

(2) With regard to persons detained in the course of enforcing a penalty, measure, or coercive measure, the right provided for under paragraph (1) may be restricted in an Act with a view to observing the order of enforcement, maintaining the security of detention, and securing the success of a criminal proceeding. In such a situation, a detained person shall be relieved from any obligation to have his matters administered by electronic means.

(3) It shall be presumed that the means of electronic communication and other technical means specified by law used to submit a document by electronic means are used in a lawful manner.

Section 4 In light of the relative simplicity and cost-efficiency of electronic administration, an organ specified in point 17 *l)* of section 1, when handling a matter by electronic means, may undertake to handle the matter within a time limit shorter than the administrative time limit specified by law or in the general terms and conditions of the organ, provided that doing so does not have a detrimental impact on the average administration time of matters not administered by electronic means.

Section 5 (1) A law relating to electronic administration may not impose any requirement that would oblige a client to use a specific technical implementation or solution, with the exception of a government communications service specified in the government decree on government networks or an information and communication service provided by the State free of charge.

(2)

Section 6 (1) When administering matters by electronic means, electronic administration organs and clients shall proceed in compliance with the requirements of good faith, fair dealing, and mutual cooperation in the course of exercising their rights and performing their obligations.

(2) Electronic administration organs shall develop system processes that support electronic administration and ensure compliance with legal requirements with due regard to the interests of their clients.

(3) Electronic administration organs shall be obliged to conduct in a fully electronic manner all internal functions and processes that are required for the functioning of their electronic administration services and communicating with other associated organs engaged in the administration of matters, and they shall be obliged to provide the necessary electronic information systems.

Section 7 In the course of administering matters by electronic means, the availability of public interest data and data accessible on public interest grounds, and the protection of personal, classified and non-public data shall be ensured.

CHAPTER II

ELECTRONIC ADMINISTRATION

Section 8 (1) Unless provided otherwise by an Act or a government decree adopted by acting within original legislative power, a client may carry out administrative acts and make statements by electronic means before an electronic administration organ in the course administering his matters.

(2) Means of electronic administration may not be used for procedural acts in the context of which a client is required by an Act or a government decree adopted by acting within original legislative power to appear in person or to submit certain documents to the submission of which there is no alternative.

(3) The possibility of using electronic administration may be restricted by an Act or a government decree adopted by acting within original legislative power only if personal appearance by the client or the submission of a document to the submission of which there is no alternative is indispensable.

(4) Electronic administration may not be used for procedural acts that make it impossible by definition.

(5) Electronic administration may not be used in proceedings or for procedural acts where it is prohibited by an international treaty or a directly and generally applicable mandatory legal act of the European Union.

(6) Electronic administration may not be used concerning any document, deed or other submission containing classified data.

3. Mandatory electronic administration

Section 9 (1) Unless provided otherwise by an international treaty or an Act, on the basis of an obligation arising from an international treaty, electronic administration shall be used in all matters referred to in section 2 (1),

a) by, when acting as a client,

aa) economic operators,

ab) the State,

ac) local governments,

ad) budgetary organs,

ae) prosecutors,

af) local government clerks,

ag) statutory professional bodies,

ah) other administrative authorities not covered by subpoints *ac)* to *ag)*, and

b) legal representatives of clients.

(1a) The provisions laid down in section 14 (4) shall apply accordingly to the delivery of documents sent to a client referred to in paragraph (1), a legal representative, a client required by an Act to use electronic administration, or a client using electronic administration voluntarily.

(2) Apart from the situations specified in paragraph (1), a client or his representative shall only be obliged to use electronic administration in situations specified by an Act, provided that doing so is not impossible by definition in light of the given administrative act.

(3) A natural person may be obliged to use electronic administration only by an Act.

(4) A client may not be subject to any disadvantageous legal consequence if

a) he cannot administer a matter by electronic means because an electronic administration organ fails to perform its obligations specified in this Act temporarily or permanently due to any malfunction, outage or other reason,

b) an electronic administration service necessary to administer a given matter by electronic means, a supporting regulated electronic administration service, or any other related service is temporarily or permanently unavailable,

c) he submits a statement in a form other than the form required by law or the relevant electronic administration organ because the electronic administration organ failed to publish the form, pursuant to the rules on electronic communication, in a manner allowing it to be completed and downloaded.

(5) If using electronic communication, or a method of electronic communication, is required by law for submitting a statement, any statement submitted in violation of that requirement shall be considered ineffective, subject to the exceptions specified in an Act or specified in paragraph (4).

(6) Any exemption from disadvantageous legal consequences, as provided for under paragraph (4), shall apply as long as the circumstances or events specified in paragraph (4) remain in, or take, place.

4. Methods of electronic administration

Section 10 A client may make any statement, or perform any procedural act or other obligation required for electronic administration, at his own discretion, by

a) using a uniform customisable electronic administration user interface, regarding all electronic administration organs unless provided otherwise in an Act, or

b) other electronic means provided by an electronic administration organ, if any, pursuant to the relevant information notice published by the electronic administration organ concerned.

5. Automated decision-making procedure

Section 11 (1) An electronic administration organ shall proceed using automated decision-making where the relevant statutory conditions are met. When using automated decision-making, electronic administration organs shall pass, and communicate to clients, their decisions without human intervention on the basis of available data and data obtained through automated information transfer.

(2) In automated decision-making proceedings commenced upon application, clients shall submit their applications, following electronic identification, using an electronic form provided by the electronic administration organ concerned.

(3) Electronic administration organs shall publish the methodology and material rules of the decision-making procedure applied in a manner that they are accessible both on their website and on the customisable electronic administration user interface.

6. Transition to and from paper-based and electronic administration

Section 12 (1) In the course of electronic administration by an electronic administration organ, the organ shall, as necessary,

a) produce, or have produced, an authentic electronic copy of a document received as a paper-based document,

b) produce an authentic paper-based copy of a decision issued by electronic means, or have it converted into an authentic paper-based document.

(2) An electronic document shall have the same probative value as the original paper-based document for

a) an authentic copy produced pursuant to the rules of producing electronic copies of paper-based documents,

b) an authentic copy produced pursuant to the rules of converting electronic documents into authentic paper-based documents.

(3) A document shall have the same probative value as the original electronic document, provided that it was produced in line with the rules on converting electronic documents into authentic paper-based documents or on the central electronic administration service for producing electronic copies of electronic documents in other formats.

6/A Electronic administration by way of electronic administration points

Section 12/A (1) To using an electronic administration point within the meaning of section 34 (6) of Act LXVI of 1992 on the registration of personal data and address of citizens (hereinafter "Nytv.") (hereinafter "electronic administration point"), the provisions of this Act shall apply with the derogations specified in this section.

(2) Electronic administration point is a supplementary service; the operator of an electronic administration point shall inform the Supervisory Authority of the scope of matters that can be administered or initiated through it at least 30 days before offering the service. The Supervisory Authority shall publish, on its website and at least 8 days before offering the service,

a) the geographic location of electronic administration points,

b) services and matters that can be administered at the electronic administration point.

(3) An application submitted at an electronic administration point following electronic identification shall be considered to be submitted by the client by electronic means in compliance with the provisions laid down in this Act.

(4) Even matters to be administered exclusively in person under a law or due to the nature of the matter concerned may be administered at an electronic administration point, provided that the technological requirements are met. In such a situation, the client shall be considered as if he proceeded in person.

(5) Using an electronic administration point shall be without prejudice to the person exercising the relevant powers.

(6) An electronic administration point shall confirm the submission of an application

a) in a paper-based form produced on the spot upon an application to that effect by the client, or

b) in the form of an electronically authenticated document sent to the electronic contact address provided by the client.

(7) If automated decision-making proceedings are conducted in the type of case administered, the electronic administration point shall send of the decision taken in the proceeding

a) a paper-based copy produced on the spot upon an application to that effect by the client, or

b) a copy in the form of an electronically authenticated document sent to the electronic contact address provided by the client.

(8) A paper-based copy of a decision under paragraph (7) *a)* shall be considered served once it is produced. A document recording a decision under paragraph (7) *b)* shall only be sent to a contact address of the client under section 14 or 15.

(9) The following shall be a public deed:

a) a confirmation under paragraph (6) issued by an electronic administration point, and

b) a decision under paragraph (7) served with assistance from an electronic administration point.

(10) To verify the identity of a client when using an electronic administration point, the service specified in section 12/B of Act CLXXXVIII of 2015 on the facial image analysis register and the facial image analysis system may also be used. In such a situation, only a person who is registered in the personal data and home address register may make a juridical act requiring personal identification. Identification offered through this service shall be considered equivalent to electronic identification under this Act.

(11) Biometric identifiers (facial image, fingerprint, signature) recorded with assistance from an electronic administration point shall be considered equivalent to biometric identifiers recorded by the authority entitled to carry out integrated facial image and signature recording.

CHAPTER III

ELECTRONIC COMMUNICATION

Section 13 (1) Communication shall be considered conducted by electronic means where a statement is made by a client, or a statement or decision is made by an electronic administration organ (hereinafter jointly "statement") by electronic means. A procedural act to which appearance in person is mandatory may be permitted by law to be performed by means of electronic communication.

(2) Electronic communication also means communication via electronic means ensuring voice transmission, unless that is impossible by definition.

7. Contact addresses

Section 14 (1) If a client is an economic operator, it shall report its electronic contact address (hereinafter "official contact address") to the register of administrative settings (hereinafter "client settings register") within 8 days, unless provided otherwise in an Act, after its

registration or establishment, where registration in a statutory register is not required for taking up operations; the official contact address may be

a) a secure electronic delivery address, or

b) electronic contact address of a different type as specified by the Government in a decree.

(2) Economic operators shall report to the client settings register any change to their official electronic contact address specifying the date of such change, before the change takes effect.

(3)

(4) An item delivered to an official contact address shall be considered delivered

a) at the time stated in the confirmation of receipt if the service provider providing the official contact address confirms receipt by the client,

b) at the time stated in the confirmation of refusal if the service provider providing the official contact address confirms that the addressee refused receipt of the item, or

c) on the fifth working day following the date of the second notice as stated in the confirmation if the service provider providing the official contact address confirms that the addressee did not accept the item after being notified two times.

(5)

(6) A contact address may not be used as an official contact address only if

a) it can be clearly identified as being used by a given economic operator exclusively,

b) it is capable of clearly identifying, by electronic means, the date and time of sending and receipt, as well as the recipient,

c) it ensures that all documents received are intact,

d) it is capable of handling delivery failures,

e) it is capable of confirming all details specified in paragraph (4).

(7) The Government shall designate in a decree the service provider that provides all organs specified in a Government decree with a contact address mentioned in paragraph (1) *a)* under a separate public service contract free of charge.

(8) If a client is an economic operator without an official contact address, an electronic administration organ may also conduct a proceeding without using electronic communication, with the proviso that the proceeding electronic administration organ shall initiate a supervision of legality proceeding or an administrative audit, as defined in an Act, against the economic operator concerned for failing to meet its obligations.

(9) If an economic operator is recorded in a publicly certified register, the organ keeping the given register shall transfer, by electronic means and without consideration, all recorded public information concerning the economic operator, as necessary to identify the economic operator and its authorised representative, to the organ keeping the client settings register and the service provider providing a secure electronic delivery address, as specified by the economic operator, with a view to registering and operating the official contact address. The technical rules of completing such data transfers shall be drawn up in an agreement by the organs concerned.

(10) Private entrepreneurs shall report their official contact address as required by a decree by the Government.

Section 14/A All data recorded in a register under section 14 (1) regarding an economic operator shall be transferred, without consideration, by the organ keeping the register to the Hungarian Central Statistical Office for the purpose of defining the group of reporting agents, and the Hungarian Central Statistical Office shall be authorised to process such data for statistical purposes.

Section 15 (1) A natural person may specify an official contact address, among his administrative settings, with regard to which he agrees to meet the requirements laid down in section 14. It such an event, the provisions laid down in section 14 shall apply as appropriate to the time or fiction of service.

(2) If a proceeding was initiated by a natural person client by electronic means, the proceeding electronic administration organ may deliver items to the known contact address of the client even in the absence of a statement referred to in paragraph (1), provided that the contact address meets the requirements specified in section 14. It such an event, the provisions laid down in section 14 shall apply as appropriate to the time or fiction of service. Simultaneously with the delivery of an item to an official contact address, the proceeding electronic administration organ shall also notify the client of the delivery to his official contact address through the electronic communication address used by the client to submit his application, provided it is different from his official contact address and doing so is possible from a technical perspective.

(3) If a natural person client does not provide an official contact address pursuant to paragraph (1), the proceeding electronic administration organ may attempt delivery to a known electronic contact address of the client, unless doing so is prohibited by the client through his administrative settings. In such a situation, the provisions laid down in section 14 (4) shall apply, with the proviso that the proceeding electronic administration organ shall attempt to delivery its document or notification by other means following the second failed delivery attempt.

(4) With regard to contact addresses not qualifying as official contact addresses pursuant to section 14 and paragraphs (1) and (2), the fact of delivery may be certified in line with applicable legislation; fiction of service shall not apply to any such situation.

(5) If a client indicates, without applying any other administrative settings, his electronic mail address, his phone number suitable for receiving short text messages, or any other contact address that is suitable for electronic communication in a statement addressed to the proceeding electronic administration organ, the proceeding electronic administration organ may use the provided contact address to communicate information to the client. If the client also has an official contact address, the proceeding electronic administration organ shall communicate with the client using his official contact address primarily, and the contact address referred to in this paragraph shall be used only for notification and information purposes.

(6) If electronic administration is not mandatory, any administrative setting by a natural person client that prohibits electronic administration entirely or with regard to a given procedural act shall also exclude the onset of the legal effects of fictitious service of a given electronic statement, unless provided otherwise in an Act.

(7) Unless provided otherwise by law, a client may configure his administrative settings at an organ designated by the Government.

(8) A contact address provided by a natural person among his administrative settings pursuant to paragraph (7) shall be transferred, without consideration, by the organ designated by the Government to the Hungarian Central Statistical Office (hereinafter “HCSO”) for the purpose of defining the group of reporting agents, and the HCSO shall be authorised to process such data for statistical purposes. The organ designated by the Government may provide data provision by way of direct query. In a proceeding for statistical data generation, the HCSO shall process the data received or queried. Upon the termination of a task, and in particular after a data recording proceeding is closed, the HCSO shall delete data received in connection therewith.

8. Method of communication

Section 16 (1) If using a specific method of communication for making a given statement is not required by law, clients shall be free to choose the method of communicating with an electronic administration organ by electronic means using the contact addresses specified in an information notice published by the given electronic administration organ.

(2) For making statements addressed to clients, if the method of communication to be used is not specified by law, electronic administration organs

a) shall use the communication method indicated among the administrative settings of their clients, or,

b) in the absence of administrative settings, may choose the method of electronic communication freely.

(3) If a method of electronic communication referred to in paragraph (1) or (2) does not ensure, regarding statements made using the given method, that the making or content of that statement can be proven subsequently, or if a conversation conducted via electronic means ensuring voice transmission is not recorded by an electronic administration organ in a form allowing the authenticity of the recording to be proven subsequently, the proceeding electronic administration organ shall produce and send to its client, via electronic means where the electronic contact address of the client is known and in the absence of any other instruction given by the client, a summary of the material circumstances of communication and the statements made.

(4) A summary referred to in paragraph (3) shall be presumed to be an authentic proof of the circumstances of electronic communication and of the statements made, provided that it is not challenged by the client concerned within 3 working days after it is sent. The proceeding electronic administration organ shall make its client aware of this fact in the course of their communication.

Section 17 (1) Where a written statement is required by law for the purpose of non-electronic administration, a juridical act used for electronic communication shall be equivalent to such a statement, provided that

a) the person making the statement is identified by electronic means pursuant to section 18 (2), and

b) it is ensured that the electronic document delivered is identical to the document approved by the person making the statement.

(2) With regard to statements other than those referred to in paragraph (1), an Act or government decree adopted by acting within original legislative power may provide that such a statement shall have the legal effect of a written statement.

(3) Where an electronic delivery service meeting the requirements laid down in this Act and its implementing decrees is used, with regard to an electronic statement referred to in paragraph 1), to

a) send that statement, the act of sending shall have the same legal effect as posting a written non-electronic statement,

b) deliver that statement, the act of delivery shall have the same legal effect as submitting, delivering, or communicating a written non-electronic statement.

(4) Unless provided otherwise by law, a statement made through electronic means ensuring voice transmission by an identified client shall have the same legal effects as a verbal statement made by non-electronic means.

(5) If the use of a given means of communication is not required by law for making a given statement, a statement made by any electronic means meeting the provisions of this Act shall have the same legal effects as a statement made by non-electronic means.

CHAPTER IV

THE RIGHTS AND OBLIGATIONS OF CLIENTS

9. Requirement of electronic identification

Section 18 (1) Subject to the exception specified in section 17 (2), a client may use electronic administration without electronic identification only if no person identification data need to be provided when performing a given procedural or administrative act, or making a statement, by non-electronic means.

(2) In situations not covered by paragraph (1), a client using electronic administration shall identify himself using, at his own discretion,

a) an electronic identification service,

b) an electronic identification means meeting the requirements specified in Article 6(1) eIDAS, or

c) an electronic identification service meeting the requirements laid down in paragraphs (3) to (4) with regard to a given procedure type or procedural act pursuant to the information notice published by the proceeding electronic administration organ.

(3) If permitted by law, when administering matters in a non-electronic manner, a procedural act or statement requiring personal appearance by the client may be performed or made by a client by electronic means, provided that the client identifies himself by using electronic identification that is based on a previous identification of the client in person, according to which the client can be clearly identified as being himself pursuant to paragraph (4).

(4) In a situation described in paragraph (3), a client can be clearly identified as being himself if the data certified during his electronic identification correspond to

a) natural identification data stored, with regard to the client, in the personal data and address register, the central immigration register, or the register of foreign nationals relying upon electronic administration,

b) natural identification data stored, with regard to the client, in the personal data and address register or the central immigration register, or data in the register of foreign nationals relying upon electronic administration that clearly and indirectly correspond pursuant to the data link register,

c) identification data recorded among administrative settings, or

d) person identification data processed in the computer system of an electronic administration organ, provided that the system can confirm that the client corresponds to a given person by comparing such data to data in a publicly certified register.

(5) Subject to the consent of a client, an organ referred to in section 1 (17) *a)* to *i)* may request identification data, which are necessary for administering a given matter and may be processed by the proceeding electronic administration organ, from an organ keeping the client registration records of the electronic identification service specified in section 32 (1) or keeping any other register storing data of the client in relation to an electronic identification means or solution referred to in paragraph (2).

(5a) An electronic administration organ shall become entitled to request and process data pursuant to paragraph (5) when it becomes aware of the intention of the client to engage in the administration of his matter.

(6) In a situation not covered by paragraphs (1) and (3), a client may perform an administrative act or make a possible statement by electronic means, provided that he identifies himself using electronic identification that is based on a previous identification of the client in person and that ensures that the name of the client is available to the proceeding electronic administration organ, and his other data required for his identification are available to the electronic identification service provider.

(7) A client may not be subject to any disadvantageous legal consequence if he fails to use electronic administration as required by law or an electronic administration organ to perform a procedural act or to submit a statement requiring electronic identification because it is not ensured that the client can identify himself pursuant to paragraph (2) *a)* or *b)*.

(8) Unless provided otherwise by law, an electronic administration organ may determine the assurance level of electronic identification, pursuant to Article 8(2) eIDAS, to be used for electronic communication requiring the electronic identification of its client. Unless provided otherwise by law or an electronic administration organ, assurance level low, as specified in Article 8(2)(a) eIDAS, shall be sufficient for electronic identification.

Section 19 (1) An economic operator may perform a procedural act or make a juridical act requiring electronic identification by electronic means after

a) its electronic identification pursuant to section 18 (2), or

b) the electronic identification pursuant to section 18 and verification of the right of representation of its natural person representative.

(2) On behalf of the represented person, a representative of a natural person may perform a procedural act or make a juridical act requiring electronic identification by electronic means after his electronic identification pursuant to section 18 and verification of his right of representation.

(3) An electronic administration organ may not oblige a client, or a representative of a client, to certify the right of representation of the representative if

a) the data certifying the right of representation is required to be kept in a statutory register as publicly certified data,

b) the client granted authorisation among his administrative settings to the representative to perform the procedural act or to make the juridical act.

(4) In a situation described in paragraph (1) *b)*, the proceeding electronic identification service provider shall provide the natural identification data of the natural person acting on behalf of the economic operator to the proceeding electronic administration organ for the purpose of identifying the representative. The electronic administration organ shall be liable for the lawfulness of data processing.

(5) The use of an electronic statement submission service through a machine interface used by an economic operator client regarding a matter where the identification of its representative is either unnecessary or ensured by other means, in particular on the basis of natural identification data provided by the economic operator client or a trust service certificate used by the representative, shall be considered equivalent to the identification of that representative pursuant to paragraph (1) *b)*.

10. Obligation for certifying identifiers and data

Section 20 (1) With the exception of data required for client identification, an electronic administration organ referred to in section 1 (17) *a)* to *i)* may not require a client to certify any data that was published by the organ concerned pursuant to the Act on the right to informational self-determination and on the freedom of information or that needs to be recorded in a statutory publicly certified register.

(2) If any data referred to in paragraph (1) is obtained by an electronic administration organ by way of information transfer, the period of up to 3 working days that is needed to comply with the request for administrative assistance shall not be calculated into the administrative time limit, with the exception of authority proceedings covered by the Act on the Code of General Administrative Procedure.

Section 21 (1) If a client is required by law to certify an identification code, introduced by an official verification card, for which an encrypted connection code is recorded in the data link

register, the client may also perform this obligation by presenting, in the course of electronic or non-electronic administration, to an electronic administration organ any other official verification card suitable for verifying identity that verifies any other such code.

(2) If a client is required by law to provide an identification code, introduced by an official verification card and recorded in the data link register, the client may also perform this obligation by certifying his identification code introduced by an official verification card issued by a specialised system recorded in the data link register in the course of electronic or non-electronic administration before an electronic administration organ.

(3) In a situation described in paragraph (1) or (2), the proceeding electronic administration organ shall obtain an identifier it is entitled by law to process through the data link register.

(4) If a data controller that is connected to the data link register uses, on the basis of statutory authorisation, an identifier other than natural identification data, its client may also certify the identifier and his identity using an identification service instead of a verification card certifying the identifier used by the data controller.

(5) After providing the requested identification code, the proceeding organ and the operator of the data link register shall delete without delay all identification data provided by the client for the purpose of service provision, unless it is authorised by an Act to process such data.

Section 21/A (1) If electronic administration is not excluded regarding a given matter, and the client is required by law to submit an original copy of a paper-based document, deed or other submission (hereinafter for the purposes of this section "submission") to certify a fact or data, the client shall perform this obligation, in case of electronic administration, by submitting an authentic electronic copy of the submission, unless an Act or government decree adopted by acting within original legislative power explicitly provides otherwise. If any doubt arises regarding the authenticity of the original copy of a submission serving as basis for an authentic electronic copy, the client shall present the original copy of his submission upon a reasoned request by the proceeding electronic administration organ.

(2) Paragraph (1) shall not apply where the submission is a verification card or document the withdrawal or return of which was ordered by law or the proceeding electronic administration organ.

(3) If a submission is to be submitted in more than one copies by law, a client using electronic administration shall submit only one electronic copy, unless specifically provided otherwise by an Act or a government decree adopted by acting within original legislative power.

(4) A client may be permitted by law to authenticate an electronic copy of his submission himself, in a manner specified in a decree by the Government, with the proviso that the client concerned shall undertake to retain, and present upon request, the original copy of his submission for a period specified by law. Within a period specified by law, the client concerned shall present the original copy of his submission upon a reasoned request by the proceeding electronic administration organ.

Section 21/B In matters relating to specific types of traffic structures, the law may require certain documents specified by law to be submitted in a paper-based format even if electronic communication is used.

11. The right of disposal of clients

Section 22 (1) A client may make juridical acts within the framework of his administrative settings before an organ designated in a decree by the Government regarding the following matters:

a) opting for electronic or non-electronic means of communication,

b) selecting a method of electronic identification,

c) selecting a method of communication, including any statement by the client to the effect that an electronic administration organ shall consider a message sent via a computer system specified by the client to be a statement made by the client,

d) requiring the encryption of electronic documents,

e) juridical acts concerning representation.

(2) Among his administrative settings, a client may

a) request a service provider specified in a decree by the Government to notify by electronic means, automatically or based on an *ad hoc* instruction by the client, an electronic administration organ specified among the administrative settings about changes to any data specified by the client,

b) grant authorisation, addressed to one, more than one, or all electronic administration organ or organs, to another entity specified by law to act on his behalf regarding certain or all matters before the electronic administration organ concerned,

c) issue instructions as to which of his administrative settings may be accessed by individual electronic administration organs, provided that he also indicates, within this scope, which administrative settings are effective vis-á-vis individual electronic administration organs,

d) require the service provider designated in the decree by the Government to provide information by electronic means on behalf of electronic administration organs specified by the client about administrative acts concerning the client,

e) make any other juridical act specified by law.

(3) Unless provided otherwise by law, administrative settings may be set or modified

a) in person, or

b) by electronic means using an interface or telephone channel operated by a service provider designated by the Government.

(4) If law requires a juridical act to be made in writing or embodied in a private deed of full probative value, a statement made in the administrative settings shall be considered meeting that requirement.

(5) A statement recorded in the client settings register shall be effective in dealings with all electronic administration organs, unless the client concerned applied any other setting among his administrative settings, or the client concerned uses electronic administration without electronic identification.

(6) A setting concerning a matter shall be invalid if it is inconsistent with the laws applicable to the given matter.

(7) An Act or a government decree adopted by acting within original legislative power may require an electronic administration organ to take into account in a pending proceeding any new or modified administrative setting entered into the client settings register after the given proceeding is instituted only if the client concerned notifies it also to the proceeding electronic administration organ.

(8) An Act or a government decree adopted by acting within original legislative power may provide that a juridical act referred to in paragraph (1) *e)* is to be considered invalid until the authorisation is accepted and entered into the client settings register as accepted.

(9) The provision laid down in paragraph (1) *e)* shall not apply to matters other than the duties of the State tax and customs authority as investigating authority, falling within the competence of the State tax and customs authority or the tax authority of a local government (hereinafter jointly “tax matters”), unless the client concerned is a natural person or a private entrepreneur.

12. Right to information by electronic means

Section 23 (1) A client may request and receive information from an electronic administration organ as necessary for

a) handling his matter at a call centre referred to in section 26 (3) or by electronic means,

b) electronic administration also by non-electronic means.

(2) Upon request by a client, an electronic administration organ shall forward any document free of charge, for information, as a non-authentic copy, in electronic form and by electronic means, to the electronic communication address specified by the client and available to the electronic administration organ, provided that the document may be released to the client and is available to the electronic administration organ in electronic form.

13. Electronic payment

Section 24 (1) Unless provided otherwise in an Act or government decree adopted by acting within original legislative power, a natural person client may pay by electronic means any and all administration-related public burdens, administrative charges, fines, and considerations for services.

(2) Unless provided otherwise in an Act or government decree adopted by acting within original legislative power, an economic operator client shall be obliged to pay by electronic means any and all administration-related public burdens, administrative charges, fines, and considerations for services in the course of administration of its matter before an electronic administration organ.

(3) An Act may oblige natural person clients to perform their payment obligations specified in paragraph (1) by electronic means.

CHAPTER V

OBLIGATIONS OF ELECTRONIC ADMINISTRATION ORGANS

14. Provision of electronic administration

Section 25 (1) An electronic administration organ shall ensure the rights of its clients provided for under this Act by way of an information system providing electronic administration pursuant to this Act and its implementing decrees.

(2) In the course of administering matters by electronic means, electronic administration organs specified in a government decree shall use government communications services where such service is available and its use is not impossible by definition.

(3) An electronic administration organ shall operate an information system providing electronic administration that makes it possible, at least,

a) to query the administrative settings of clients,

b) to handle matters through a customisable electronic administration user interface,

c) for clients to use an electronic identification solution offered through the central identification agent service when using a service requiring electronic identification,

d) for messages to be delivered, and received by the addressee, through a secure electronic delivery service as specified in a government decree,

e) to certify, without delay and in a manner specified by law, the receipt of juridical acts made and documents sent by clients by electronic means,

f) to process electronic documents bearing at least advanced electronic signatures or electronic seals that meet public administrative requirements,

g) to produce authenticated documents pursuant to this Act,

h) to deliver documents to clients using any type of service referred to in section 14,

i) to pay by electronic means all burdens relating to a proceeding, with regard to organs referred to in sections 1 (17) *a)* to *i)*, and

j) to process electronic forms created by an electronic form filling service.

(4) The organs referred to in sections 1 (17) *a)*, *b)*, *d)* to *f)*, and *j)* shall ensure that their information system referred to in paragraph (1) is available continuously.

(4a) Electronic administration organs shall create backup of their administration-related data specified in a decree by the Government and unless a more stringent requirement is set by law, at least at a frequency and in an order specified in a decree by the Government, and they shall send such security backups to an organ designated by the Government as responsible for data retention. The organ responsible for data retention may not consult the content of data backups.

(5) An electronic administration organ shall provide electronic administration to the client by way of electronic administration solutions supporting the entire administration process, and, unless prohibited by an Act or the administrative settings of the client, the entire administration process may be completed by using electronic administration solutions.

(6) An electronic administration organ shall make its statements addressed to a client by electronic means, where doing so is not impossible by definition, provided that

a) doing so is required by law,

b) doing so is required by the client, or

c) the application was submitted by the client by electronic means.

(7) If a client is required by law to make a juridical act using an administrative form or electronic form, or if an electronic administration organ is allowed by law to use a standard administrative form or electronic form, the proceeding electronic administration organ may allow its client to make the statements specified by law also using an interactive application made standard for this purpose instead of the administrative form.

(8) A law

a) may designate an electronic administration organ, from among organs with identical competences, to have exclusive authorisation to administer a given matter by electronic means in the country,

b) may provide that, when using electronic administration, either of the organs with identical competences may proceed with territorial jurisdiction over the entire country, and the cases shall be distributed automatically on the basis of objective criteria.

(9) The State shall provide organs referred to in section 1 (17) *a)* to *i)* and *k)*, free of charge, with all regulated electronic administration services mandatorily provided by the Government and central electronic administration services that are necessary for operating an information system providing electronic administration pursuant to paragraph (3).

(10) Except for the occurrence and risk of information security breaches, the electronic administration organ concerned shall publish on its website and report to the Supervisory Authority any change to electronic communication options 30 days before the change. The electronic administration organ concerned shall indicate on its website any change to the method of communication for 14 days after the change.

(11) If an electronic form is changed, paragraph (10) shall apply with the derogation that the change shall be published 14 days in advance, and it need not be reported to the Supervisory Authority.

15. Obligations to provide information

Section 26 (1) An electronic administration organ shall publish, independently or in cooperation with other electronic administration organs, information that is necessary for using, or supports the use of, electronic administration, with the content specified in a decree by the Government, in a manner enabling clients to display and store the information.

(2) An electronic administration organ shall inform its clients, even when using non-electronic administration, about the possibility of using electronic administration at least at the time of first contact.

(3) An electronic administration organ shall operate, independently or in cooperation with other electronic administration organs, a call centre that may be contacted by phone and also by other electronic means pursuant to the provisions laid down in the Act on consumer protection concerning undertakings carrying out public service activities, with the derogation that the call centre shall be available for at least 40 hours per week.

(4) On the basis of a separate agreement, an organ referred to in sections 1 (17) *a)* to *i)* may also carry out their tasks specified in paragraph (3) by operating a national call centre designated in a decree by the Government.

16. Outage, malfunction

Section 27 (1) An entity providing regulated or central electronic administration services, or an electronic administration organ, shall carry out all scheduled technical activities involving the suspension of its services or electronic administration activities at a time when the suspension does not cause any significant disturbance in electronic administration.

(2) An entity providing regulated or central electronic administration services, or an electronic administration organ, shall publish a notice, with the content and at the contact addresses specified in a decree by the Government, regarding any scheduled technical activity involving the suspension or limitation of its services or electronic administration activities at least 3 days before the commencement of that activity.

(3) If electronic administration is suspended for over 1 working day, the electronic administration organ concerned shall ensure that client submissions are received and processed in a non-electronic manner, even if only electronic administration may be used regarding a given type of procedure pursuant to relevant legislation.

(4) The Government shall specify in a decree those electronic administration organs that are unable to meet the requirements laid down in this Act through no fault of their own (hereinafter "no-fault inability"). The provisions laid down in Part Two or Part Three shall not apply to an electronic administration organ affected by no-fault inability.

(5) In a situation of no-fault inability as defined in paragraph (4), electronic communication pursuant to this Act cannot be used, and, for the purpose of electronic communication, a client required to use electronic administration shall be considered not required to use electronic administration.

(6) In its decree under paragraph (4), the Government shall specify the period of no-fault inability, and it may specify a set of matters falling within the functions and powers of the organ concerned with regard to which no-fault inability does not apply.

17. Data provision

Section 28 (1) 30 days before offering the possibility to use electronic administration in a given matter, electronic administration organs shall notify the data specified in a decree by the Government to the Supervisory Authority, in addition to sending the information referred to in section 26 (1), by electronic means using the electronic form used by the Supervisory Authority.

(2) Electronic administration organs shall report, pursuant to paragraph (1), any change to the data or information referred to in paragraph (1) to the Supervisory Authority at least 15 days before the change takes effect.

(3) On the basis of the data provided under this section, the Supervisory Authority may oblige the electronic administration organ concerned to provide further data as required for verifying compliance with the requirements laid down in this Act.

CHAPTER VI

THE PROVISION OF REGULATED ELECTRONIC ADMINISTRATION SERVICES

18. Regulated electronic administration services

Section 29 (1) Regulated electronic administration services shall be the following services:

a) electronic identification services,

b) secure electronic delivery services,

c) services relating to electronic signatures that may be used for electronic administration purposes and meet statutory requirements,

d) services classified as regulated electronic administration services in a government decree adopted based on an authorisation by this Act.

(2) More than one regulated electronic administration service may be implemented and provided as a bundle; in such a scenario, the service provider shall meet all requirements concerning each regulated electronic administration service separately.

(3) The detailed rules concerning the notification of regulated electronic administration services, the keeping of the register of regulated electronic administration services, the activities of the Supervisory Authority, and the provision of regulated electronic administration services shall be determined by the Government in a decree. The provisions laid down in the Act on the general rules on taking up and pursuit of service activities shall apply accordingly, with the derogations laid down in this Subtitle or in a decree by the Government.

(4) The use of a regulated electronic administration service may be made mandatory by an Act or government decree.

19. Electronic identification services

Section 30 (1) An electronic identification service may be used by a person who, in order to use the service, registers and is recorded in the client registration records, within the meaning of section 32 (1), of the electronic identification service provider concerned.

(2) A client may register to use an electronic identification service

a) by electronic means using an electronic signature, an electronic identification means meeting the requirements laid down in Article 6 (1) eIDAS, or another identification service registration for which meets the requirements laid down in this Subtitle, or

b) in person through a proceeding that meets the requirements laid down in this Subtitle.

Section 31 (1) Before registration, a natural person client (for the purposes of this Subtitle, hereinafter "applicant") shall appear in person before the electronic identification service provider, or the organisation carrying out registration on behalf of the electronic identification service provider (hereinafter jointly "client registration organ"). In situations determined by the proceeding electronic identification service provider, personal appearance shall be considered equivalent to a proceeding conducted by the organisation carrying out registration at an external site, provided that the identity of the applicant can be verified as required by this Subtitle under equivalent security circumstances.

(2) The proceeding client registration organ shall identify a natural person who appears in person on the basis of data indicated on an official verification card suitable for verifying identity that is presented by that natural person. The proceeding client registration organ shall compare the natural identification data of the natural person concerned, as indicated on his official verification card, to data recorded in

a) the personal data and address register,

b) the central immigration register, provided that the natural person concerned is a foreign national and is not recorded in the personal data and address register or the register referred to in point *c)*,

c) the register of foreign nationals relying upon electronic administration.

(3) If an applicant is recorded in the register referred to in paragraph (2) *a)*, the client registration organ shall transfer the birth name indicated on the official verification card presented as proof of identity, as well as the identifier and type of the official verification card, to the central register of such documents for the purpose of determining that the verification card is authentic and valid, and the facial image and signature data are identical to those in the register.

(4) The register referred to in paragraph (3) shall transfer to the proceeding client registration organ the natural identification data, the data on nationality, the number and validity of the verification card, and, if requested by the client registration organ, the facial image and signature data. If the electronic identification service is a service mandatorily provided by the Government, the transfer of facial image and signature data shall be mandatory.

(5) If the applicant is registered in the register referred to in paragraph (2) *b)*, the central immigration register shall transfer to the proceeding client registration organ, upon request, the natural identification data and the data on nationality and, if requested by the client registration organ, the facial image and signature data. If the electronic identification service is a service mandatorily provided by the Government, the transfer of facial image and signature data shall be mandatory.

(6) If the applicant is registered in the register referred to in paragraph (2) *c)*, the register of foreign nationals relying upon electronic administration shall transfer to the proceeding client registration organ, upon request, the natural identification data, the data on nationality, the number, type, and validity of the document used for registration in the register of foreign nationals relying upon electronic administration, and, if requested by the client registration organ, the facial image and signature data. If the electronic identification service is a service mandatorily provided by the Government, the transfer of facial image and signature data shall be mandatory.

(7) The client registration organ shall compare the data received to the data indicated on the document presented, and it shall determine whether the facial image fits the person present.

(8) If the data and facial image are confirmed to be matching during a proceeding under paragraph (7), then the client registration organ shall take over the data under section 32 (2) from the register referred to in paragraph (2) for the purpose of entering into the client registration records.

(9) If the data and facial image are not confirmed to be matching during a proceeding under paragraph (7), or the official verification card presented to verify identity is invalid, the client registration organ shall refuse to register the client, and it shall erase all data already recorded, if any.

(10) All facial image and signature data referred to in paragraphs (4) to (6) shall be erased without delay after the verification of identity. The client registration organ may use data not recorded in the client registration records only for the purpose of identification and determining whether the data match.

(11) Only persons recorded in a register referred to in paragraph (2) may use an electronic identification service provided for under this Act.

(12) A person recorded in a register referred to in paragraph (2) *b)* or *c)* may use an electronic identification service only in matters covered by this Act.

Section 32 (1) With a view to ensuring authentic electronic identification and traceability, electronic identification service providers shall keep a register of applicants (hereinafter "client registration records").

(2) The client registration records shall contain

a) natural identification data, nationality, and unique identification number of the applicant,

b) in addition to the data under point *a)*, the number, type, and validity of the document used for registration in the register of foreign nationals relying upon electronic administration, provided that the applicant is included in a register referred to in section 31 (2) *c)*.

Client registration records may contain data specified in the standard contract terms of the electronic identification service provider concerned.

(3) As part of its registration procedure, a client registration organ shall issue a certificate concerning the registered data and, where not impossible by definition, the identifier generated by it. The applicant shall confirm that the data provided by the applicant and indicated in the certificate are correct by signing a printout of the certificate by hand or, where the certificate is generated by electronic means, by using the electronic identification function of his identification card with a storage unit, by using an at least advanced electronic signature, or by way of identification-based document authentication.

(4) An organ keeping client registration records shall be entitled to request data from any register referred to in section 31 (2) for the purpose of verifying data and keeping the data processed up-to-date. The following data may be requested regarding a person registered in the client registration records:

a) natural identification data, nationality, and death of the applicant,

b) in addition to the data under point *a)*, the number, type, and validity of the document used for registration in the register of foreign nationals relying upon electronic administration, provided that the applicant is included in the register referred to in section 31 (2) *c)*.

(5) An organ keeping client registration records shall cancel registration upon

a) request by a user,

b) death of a user,

c) expiry of the document used for registration in the register of foreign nationals relying upon electronic administration, provided that the person concerned is included in the register referred to in section 31 (2) *c)*.

(6) Registration shall also be cancelled, if a registration organ becomes aware that an applicant is not included in any register referred to in section 31 (2).

(7) A client registration organ may disclose client data without the consent of the client concerned to

a) a court for verifying either a statement made in relation to a person involved in a pending proceeding or data indicated on a document presented and for the purpose of conducting a criminal proceeding or enforcing a penalty or measure,

b) an investigating authority for the purpose of preventing or detecting a criminal offence, conducting a criminal proceeding, or enforcing a penalty or measure,

c) the prosecution service for the purpose of carrying out its tasks, as specified in the Act on prosecution service, relating to the protection of public interest and the supervision of legality, and for preventing or detecting a criminal offence, conducting a criminal proceeding, or enforcing a penalty or measure,

d) a national security service for the purpose of detection, national security protection and counter-intelligence, information gathering, national security, industrial security, internal security, and crime prevention and control,

e) a counter-terrorism police organ specified in the Act on the police for the purpose of preventing or interrupting a criminal offence and performing its tasks relating to personal and facility protection within its competence defined in the Act on the police.

(8) A client registration organ shall block data relating to a natural person 5 years after the termination of registration; blocked data may be processed only for the purpose of tracing the authenticity of electronic identification and protecting the rights and legitimate interests of citizens for a period specified in its general terms and conditions, but at least for a period of not less than 10 years, but not more than 20 years after the termination of registration.

(9) After data is blocked pursuant to paragraph (8), a client registration organ shall unblock and provide data to an organ referred to in paragraph (7) for a purpose specified in paragraph (7).

Section 33 (1) With the exception of a situation described in section 18 (5), an electronic identification service provider, following successful electronic identification in the course of electronic administration, may transfer to the proceeding electronic administration organ the name of the identified person, as well as his e-mail address, if available, and the connection code generated for the organ that cannot be deducted from natural identification data.

(2) In a situation under paragraph (1), an electronic identification service provider shall transfer, upon request by the relying party, to the regulated electronic administration service provider the personal data processed by the electronic identification service provider as necessary for registration.

20. Regulated electronic administration services to be mandatorily provided by the Government

Section 34 (1) The Government shall provide the following regulated electronic administration services acting through a designated regulated electronic administration service provider:

a) electronic identification service for natural person clients,

b) secure electronic delivery service,

c) government authentication service, including the following services:

ca) services relating to electronic signatures and electronic seals that meet statutory requirements and may be used for providing electronic administration services, and generation of certificates relating to such services for use by electronic administration organs, as well as regulated electronic administration service providers and central electronic administration service providers within the meaning of this Act,

cb) services relating to electronic timestamps, and generation of identification certificates for use by electronic administration organs, as well as regulated electronic administration service providers and central electronic administration service providers within the meaning of this Act,

cc) services relating to electronic signatures and electronic seals, and generation of certificates relating to such services for persons holding an office subject to protection, as specified by a separate law, or in a legal relationship subject to national security vetting, as well as for organs involved in, or in the authorisation of, secret information gathering or using covert means,

cd) issuing encryption certificates for use by electronic administration organs, as well as regulated electronic administration service providers and central electronic administration service providers within the meaning of this Act, and for persons holding an office subject to protection, as specified by a separate law, or in a legal relationship subject to national security vetting,

ce) verification of the validity of certificates issued pursuant to subpoints *ca)* to *cd)* through a prompt certificate verification service,

d) other regulated electronic administration services to be mandatorily provided by the Government pursuant to a government decree adopted based on an authorisation by this Act.

(2) In addition to the provisions laid down in paragraph (1), a law may also require also other organs to provide certain regulated electronic administration services.

21. Electronic identification service to be mandatorily provided by the Government

Section 35 (1) A client may use the following electronic identification services mandatorily provided by the Government:

a) electronic identification service provided through an identification card with a storage unit,

b) client gate,

c) identification by telephone with a partial code,

d) identification using video technology.

(2) For the purpose of certifying identity in an authentic manner, the organ designated by the Government in a decree shall keep consolidated client registration records (hereinafter "Central Client Registration Records") of the persons who rely upon the electronic identification service mandatorily provided by the Government.

(3) A party relying upon the electronic identification service mandatorily provided by the Government shall be entitled to use, free of charge, a secure electronic delivery service and related storage space consistently connected to the electronic identification service specified in a government decree and referred to in paragraph (1).

(4) To the Central Client Registration Records, the rules on client registration records and registration in such records shall apply with the derogations specified in paragraphs (4a) to (18) and section 35/A.

(4a) Only persons recorded in the register referred to in section 31 (2) *a)* may use the electronic identification service referred to in paragraph (1) *d)*.

(4b) Registration for the electronic identification service referred to in paragraph (1) *d)* and the procedure described in section 31 (7) shall be carried out in the manner specified in section 35/A upon first use of the service.

(5) In a situation described in section 31 (8), the organ keeping a register referred to in section 31 (2) shall generate a connection code, and the organ keeping the Central Client Registration Records shall take over the data specified in section 32 (2) and the connection code from the registers referred to in section 31 (2) for the purpose of entering into the Central Client Registration Records.

(6) A connection code may not contain any personal data, or any part of such data, of the person concerned.

(7) The organ keeping the Central Client Registration Records may request data, pursuant to section 32 (4), from the registers referred to in section 31 (2) through connection codes, provided that data processed by that organ need to be updated, and only with regard to persons the data of whom need to be updated.

(8) In a situation described in section 32 (5) *b)*, the organ keeping a register referred to in section 31 (2) shall provide, through connection code, data to the organ keeping the Central Client Registration Records about the death of the person concerned for the purpose of terminating his registration.

(9) The purpose of the Central Client Registration Records shall be to process data and technical identifiers required for identifying a person in a publicly certified manner in relation to electronic identification services mandatorily provided by the Government in the interest of providing authentic electronic identification services and protecting the rights and legitimate interests of others.

(10) In addition to the connection code and data specified in section 32 (2), the Central Client Registration Records shall contain the following data concerning each person concerned:

a) for the purpose of identification services provided through an identification card with a storage unit, the number and validity data of the document, the undecryptable hash of the registration code assigned to the identification card, and, if provided by the person concerned, his electronic mail address,

b) for the purpose of a client gate, the user name, the undecryptable hash of the password associated with the user name, and the electronic mail address of the person concerned,

c) for the purpose of identification by telephone with a partial code, the phone number provided by the person concerned, his electronic mail address, user identifier, the undecryptable hash of the password associated with the user identifier, and the responses of the client to security questions,

d) for the purpose of identification using video technology, the number, type, and validity data of the document, and, if provided by the person concerned, his electronic mail address.

(11) In the course of using an electronic identification service mandatorily provided by the Government, the technological solution used for

a) verifying data,

b) obtaining data

requested by an electronic administration organ and kept in the Central Client Registration Records shall guarantee that the organ keeping the client registration records is informed of the querying of the electronic identification service only, without learning the identity of the addressee of the query. The technological solution shall transfer only the data request of the electronic administration organ and the data covered by the request, and it shall verify the data provided by the electronic administration organ against the data kept in the client registration records.

(12) An electronic identification service referred to in paragraph (1) may be used without registration pursuant to section 31, provided that the client is already registered in the Central Client Registration Records for the purpose of using any electronic identification service referred to in paragraph (1).

(13) By way of derogation from the provisions laid down in section 32 (5), in a situation described in section 32 (5) *a)*, registration in the Central Client Registration Records shall terminate only if the client does not hold an identification card with a storage unit or his identification card with a storage unit is no longer valid. Registration shall also terminate if a client does not hold an identification card with a storage unit, and he has not requested the use of an electronic identification service referred to in paragraph (1) *b)* to *d)*.

(14) The organ keeping the Central Client Registration Records shall block data relating to a natural person 5 years after the termination of registration; blocked data may be processed only for the purpose of tracing the authenticity of electronic identification and protecting the rights and legitimate interests of citizens for a period 20 years after the termination of registration.

(15) A client may also register for using an electronic identification service mentioned in paragraph (1) *b)* by electronic means, using his identification card with a storage unit.

(15a)

(15b)

(15c)

(15d)

(15e)

(16) For the purpose of providing an electronic identification service by way of an identification card with a storage unit, registration procedure means a procedure for filing an application for an identification card with a storage unit.

(17) In a situation described in paragraph (16), the data specified in paragraph (10) *a)* shall be entered into the Central Client Registration Records on the basis of data provided by the organ keeping the personal data and address register upon the identification card with a storage unit becoming valid.

(18) The organ keeping the personal data and address register shall inform the organ keeping the Central Client Registration Records if and when an identification card with a storage unit becomes invalid.

Section 35/A (1) A client may register for using an electronic identification service referred to in section 35 (1) *d)* by electronic means upon first use of the service. For the purpose of registration, the client concerned shall present an official verification card suitable for verifying identity.

(2) In the course of registration pursuant to paragraph (1), the proceeding electronic identification service provider shall verify the natural identification data, read from the document through video signals, nationality, and document number against the natural identification data recorded in the central register keeping a record of the document; it shall also check whether the official verification card suitable for verifying identity is valid; and it shall also check, using automated comparison as provided for in Subtitle 9/B of Act CLXXXVIII of 2015 on the register and system for facial image analysis, whether a facial image of the client, produced by way of video signals, matches the last recorded facial image in the personal data and address register of the person subject to identity verification. Identification shall be considered successful if the data recorded in the register match, the official verification card suitable for verifying identity is valid, and the required threshold of match is reached.

(3) For verifying the identity of a client, an electronic identification service provider may take over, on the basis of a provided document identifier, the family and given name of the person concerned, as well as his family and given name at birth, place and date of birth, and his mother's family and given name at birth from the central register keeping a record of the document.

(4) If identification pursuant to paragraph (2) is successful, the electronic identification service provider shall notify the organ keeping the personal data and address register and the organ keeping the Central Client Registration Records accordingly in order to conduct a proceeding under section 35 (5).

(5) If a client registered using an electronic identification service referred to in section 35 (1) *d)*, the organ keeping the Central Client Registration Records shall be notified by

a) the organ keeping the personal data and address register about the number, as well as the date and fact of expiry of the identification card,

b) the travel document registration organ about the number, as well as the date and fact of expiry of the travel document,

c) the road traffic registration organ about the number, as well as the date and fact of expiry of the driver's licence.

22. Data processing

Section 36 (1) A regulated electronic administration service provider shall choose and operate all devices used to provide its service in a manner that ensures that personal data are processed only if such processing is indispensable for providing its service or achieving any other purpose specified in this Act; even in such a situation, processing shall be limited to the necessary extent and period.

(2) A regulated electronic administration service provider may process natural identification data and address data as necessary to identify the parties relying upon its service for the purpose of concluding, determining the contents of, amending, and monitoring the performance of a contract for the provision of regulated electronic administration services referred to in section 34 (1) *a)* to *c)*, as well as for the purpose of billing charges relating to, and enforcing any claim arising from, such contracts as necessary.

(3) In addition to paragraph (2), a regulated electronic administration service provider may process natural identification data and address data relating to the use of its regulated electronic administration service, as well as data on the time, period, and location of using its service, for the purpose of billing charges arising from contracts for the provision of regulated electronic administration services.

(4) For the purpose of providing a regulated electronic administration service, a regulated electronic administration service provider may process personal data that are technically indispensable for service provision.

(5) Data processed for a purpose specified in paragraphs (2) to (3) shall be erased without delay when the conclusion of a contract fails, or within 5 years after the termination of the contract concerned. Data processed for the purpose specified in paragraph (4) shall be erased without delay when the purpose of processing ceases.

(6) If data is processed as part of a service, the relevant service contract shall be concluded in a manner ensuring that the contents of the contract meet, with regard to personal data, all requirements set out for the contract to be concluded by and between the data controller and the data processor.

Section 37 (1) Upon request from an electronic administration organ using a regulated electronic administration service for electronic administration, a regulated electronic administration service provider shall compare data for the purpose of verifying the identification data of parties relying upon the service, and it shall inform the requesting electronic administration organ whether the data match.

(2) A regulated electronic administration service provider shall ensure that relying parties can receive information, before or at any time while using the service, on the types of data processed by the regulated electronic administration service provider and the purposes of data processing.

(3) Any personal data, trade secret, bank secret, payment secret, insurance secret, securities secret, fund secret, medical secret, or other professional secret processed in the course of providing a regulated electronic administration service may only be stored by the regulated electronic administration service provider concerned as transferred information in an interim and temporary manner. After the completion of its service, all such data shall be erased from its electronic information systems and data-storage media without delay.

(4) With regard to data accessed pursuant to paragraph (1), all employees of a regulated electronic administration service provider shall be subject to an obligation of confidentiality even after the termination of the legal relationship for their employment.

CHAPTER VII

CENTRAL ELECTRONIC ADMINISTRATION SERVICES

Section 38 (1) The Government shall provide the following central electronic administration services acting through a service provider designated by law:

a) a register of the administrative settings of clients,

b) a document validity register,

c) an electronic payment and clearing system,

d) identification-based document authentication,

e) a central filing agent through which a service provider performs various tasks, as specified in a government decree, relating to the receipt, opening, and filing of items sent by electronic means for and on behalf of electronic administration organs,

f) a central delivery agent through which a service provider performs, for and on behalf of electronic administration organs, various tasks, as specified in a government decree, relating to the preparation, determination of the data-storage medium, type, and method of the delivery of electronic documents to be sent out by such organs,

g) periodic notification to clients concerning electronic administrative acts, so that the proceeding service provider provides its clients, at periods and regarding electronic administration organs determined by such clients, with summary information on certain administrative acts specified in a government decree,

h) conversion of paper-based documents to authentic electronic documents,

i) conversion of electronic documents to authentic paper-based documents,

j) a central identification agent,

k) a customisable electronic administration user interface,

l) a form submission support service,

m) a central document authentication agent,

n) a general-purpose electronic application form service,

o) a data link register.

(2) If use of a central electronic administration service is conditional upon registration, only an electronic identification service may be used for such registration, unless provided otherwise by law. In the course of registration, an electronic identification service provider may transfer personal data processed by the electronic identification service provider and necessary for registration to the designated service provider, subject to consent by the relying party.

(3) The use of a central electronic administration service may be made mandatory by an Act or government decree.

(4) The provisions laid down in sections 36 and 37 shall apply as appropriate to the processing of data by a service provider designated by the Government in the context of providing a central electronic administration service.

23. Registration of the administrative settings of clients

Section 39 (1) With a view to facilitating electronic administration and providing various options for and respecting the instructions given by clients in relation to electronic administration, an organ designated by the Government shall keep a register of the data contents of administrative settings used by clients.

(2) When recording the data link entry of a new natural person into its register, the controller of the data link register shall notify by electronic means the organ keeping the administrative settings of the client concerned, with a view to creating an entry in the client settings register for processing the settings of the person concerned.

(3) The organ keeping the client settings register shall generate, on the basis of natural identification data provided pursuant to paragraph (2), an internal identifier and connection code for the data link entry of the person concerned, and then it shall provide for the transfer of the data link entry connection code, encrypted using a method that can be decrypted only by the proceeding organ, to the organ keeping the data link register, and then it shall erase all natural identification data.

(4) In the course of registering a client setting concerning representation, the organ keeping the client settings register shall enter the representative concerned into the register using a service that is based on the data link register, without storing any natural identification data of the representative or any identifier or identification code generated by another authority.

(5) The organ keeping the client settings register shall verify the right of representation.

(6) A client statement shall be kept by the organ keeping the client settings register in an encrypted form, and it may be released only to the client concerned or other authorised persons based on authorisation granted by law or the administrative settings of the client.

(7) The organ keeping the client settings register may inform, using a service based on the data link register, an eligible organ or person about the content of the administrative settings of a client in a manner specified by law, provided that the organ or person concerned provides the data required to identify the client concerned. The organ keeping the client settings register may inform an eligible organ or person only about those client administrative settings that may be disclosed by law or that the client intends, according to his administrative settings, to share with the organ or person concerned.

(8) The organ keeping the client settings register shall provide data on the content of any administrative settings, including any data on authorisations granted by a client, only to electronic administration organs and the providers of regulated or central electronic administration services. Electronic administration organs and other providers of regulated or central electronic administration services shall certify which identification codes or other identifiers they are eligible to use.

(9) When providing information on the contents of administrative settings, the organ keeping the register may disclose, using the data link register, to the requesting organ or service provider only identification codes or other data that the requesting organ or service provider is authorised to process.

(10) An Act or government decree may allow an electronic administration organ or a provider of regulated or central electronic administration services to report, in a manner specified by law, certain client administrative settings specified by law to the organ keeping the client settings register for the purpose of registration.

(11) Unless provided otherwise in an Act, the organ keeping the client settings register or a registration organ of the client settings register shall process personal data provided by a client, another organ, or a service provider referred to in paragraph (10) in the course of registering any client administrative setting only for the purpose of registering the given administrative setting and until registration is completed.

24. The document validity register

Section 40 (1) As part of the document validity register service, the service provider shall allow the relying parties to verify the authenticity and, where relevant data is available, content of authentic paper-based or electronic documents in their possession.

(2) Parties relying upon the document validity register shall record in the document validity register certain data and parts of content, specified by the service provider, of the documents they issue. The document validity register shall be available to the public, and any person may consult the register to verify data relating to a document that is in his possession and is recorded in the register, and, if possible, also the validity of such document.

25. Conversion of paper-based documents to authentic electronic documents

Section 41 A deed produced on the basis of a document by an organ, designated by the Government, pursuant to the rules of the service for conversion of paper-based documents to electronic documents shall have the same probative value as the original document.

26. Conversion of electronic documents to authentic paper-based documents

Section 42 A deed produced on the basis of an electronic document by an organ, designated by the Government, pursuant to the rules of the service for conversion of electronic documents to authentic paper-based documents shall have the same probative value as the original document.

CHAPTER VII/A

USE OF CERTAIN E-ADMINISTRATION SERVICES

Section 42/A (1) Organs that do not provide electronic administration may also request, in a manner specified in a decree by the Government, regulated electronic administration services, central electronic administration services, and central government services, as specified in an Act or government decree.

(2) If a service referred to in paragraph (1) is provided against remuneration by a market operator specified in an implementing decree to this Act, the market operator may not demand any remuneration for the onward provision of services referred to in paragraph (1) in the course of providing its service to other relying parties.

CHAPTER VIII

REGISTRATION OF FOREIGN NATIONALS RELYING UPON ELECTRONIC ADMINISTRATION

27. Registration of foreign nationals relying upon electronic administration

Section 43 (1) With a view to ensuring the security of electronic administration, the authentic electronic identification of users, and the use of certain electronic administration services, the organ designated by the Government shall keep a register of foreign natural persons who habitually reside in another country, do not have a registered domicile or place of residence in Hungary, and apply for registration voluntarily for the purpose of administering matters by electronic means (hereinafter “register of foreign nationals”).

(2) A natural person who resides in another country and does not have a registered domicile or place of residence in Hungary may administer his matters covered by this Act by electronic means, even without registration pursuant to paragraph (1), provided that he

a) is covered by eIDAS and identifies himself using an electronic identification means meeting the requirements specified in Article 6(1), or

b) is entitled to do so under an international treaty.

(3) Natural person clients shall appear in person before the registration organ designated by the Government in order to register. A proceeding conducted by the registration organ at an external site shall be considered equivalent to personal appearance, provided that the identity of the client can be verified as required by this section under the same security circumstances.

(4) When appearing in person, the registration organ shall identify a natural person on the basis of data indicated in a travel document suitable for verifying identity, as specified by law, presented by the person concerned or, if the person concerned is a citizen of a Member State that is party to the Agreement on the European Economic Area, in a document suitable for verifying identity issued by the given Member State. The proceeding registration organ shall verify the natural identification data of the natural person concerned, as indicated on his presented document, against data recorded in

a) the personal data and address register,

b) the central immigration register, and

c) the register of foreign nationals.

(5) The registration organ shall compare data received during the verification process to data indicated on the document presented by the natural person concerned, and it shall determine whether the facial image on the document presented matches the person present.

(6) The registration organ shall verify, on the basis of the document identifier, whether the document presented by the client has already been used for registration in the register of foreign nationals. If it has, registration shall be denied.

Section 44 (1) If a natural person is not included in any of the registers referred to in section 31 (2), and the facial image on the document presented matches the person present, the registration organ shall record the facial image and signature of the natural person applicant pursuant to the relevant government decree, and it shall enter the natural person into the register of foreign nationals.

(2) The registration organ shall deny the registration of a client and it shall erase all recorded data irreversibly if the data of the natural person client are already included in a register referred to in section 31 (2) or the register of foreign nationals, or if the document presented by the client as proof of identity is invalid.

(3) The registration organ may use the data under section 31 (3) only for the purpose of determining whether the data match.

Section 45 (1) Registration in the register of foreign nationals shall be terminated

a) if the natural person concerned dies,

b) if requested by the natural person concerned,

c) on the basis of a notification by the data link register if the data link entry generated for a registered person includes an encrypted data link connection code relating to a personal identifier or to an identifier used in the central immigration register,

d) when the document used during registration to verify identity expires or, if that document does not have a date of expiry, 50 years after registration.

(2) The register of foreign nationals shall contain, for a period of 5 years after the termination of registration, the facial image and signature of the natural person concerned, as well as

a) his natural identification data if he was identified by way of personal appearance during registration,

b) person identification data that were disclosed during registration and identify him exclusively, in a situation not covered by point *a)*,

c) the issuer, type, and date of expiry of the document or means suitable for verifying identity used for registration,

d) his sex and nationality, and

e) the identifier of the document or means referred to in point *c)*.

(3) Data may be provided from the register of foreign nationals to an electronic identification service provider for the purpose of enabling the electronic identification service provider to

a) determine whether a given person is the same as a person included in its register,

b) verify the identity of a given person toward a person or entity requesting his identification,

c) provide data as necessary to identify a given person to a person or entity requesting his identification.

(4) An organ referred to in paragraph (1) may disclose client data without the consent of the client concerned to

a) a court for the purpose of verifying either a statement made in relation to a person involved in a proceeding pending or data indicated on a document presented, or conducting a criminal proceeding or enforcing a penalty or measure,

b) an investigating authority for the purpose of preventing or detecting a criminal offence, conducting a criminal proceeding, or enforcing a penalty or measure,

c) the prosecution service for the purpose of carrying out its tasks, as specified in the Act on prosecution service, relating to the protection of public interest and the supervision of legality, and for preventing or detecting a criminal offence, conducting a criminal proceeding, or enforcing a penalty or measure,

d) a national security service for the purpose of detection, national security protection and counter-intelligence, information gathering, national security, industrial security, internal security, and crime prevention and control,

e) a counter-terrorism police organ within the meaning of the Act on the police for the purpose of preventing, detecting, and interrupting a terrorist act or any related criminal offence, and performing its tasks relating to priority personal protection.

CHAPTER IX

THE SUPERVISION OF ELECTRONIC ADMINISTRATION

Section 46 (1) The Supervisory Authority designated by the Government in a decree shall supervise the performance of obligations of electronic administration organs as provided for under this Part, and it shall facilitate the enforcement of clients' rights as provided for under this Part.

(2) Upon request from an electronic administration organ, the Supervisory Authority shall participate in the coordination of measures required for ensuring electronic administration.

(3) As for regulated and central electronic administration services, the Supervisory Authority shall be responsible for the administrative supervision of the provision of such services as provided for under the Act on the general rules on taking up and pursuit of service activities.

(4) As part of supervisory reviews, the Supervisory Authority shall verify compliance with the statutory requirements concerning central and regulated electronic administration services by conducting administrative audits.

(5) If the Supervisory Authority establishes that a provider of a central or regulated electronic administration service violated the rules laid down in this Act or an implementing decree to this Act, it

a) shall oblige the service provider concerned to cease its violation and proceed in a lawful manner,

b) may oblige the service provider concerned, with a view to the future and by setting a time limit as necessary, to proceed in a lawful manner,

c) may impose a fine as specified by the Government in a decree.

28. Supervisory review

Section 47 (1) A client may initiate a supervisory review if his rights under this Act are violated or his rights or legitimate interests are affected by a failure of an electronic administration organ to perform its obligations.

(2) The Supervisory Authority shall examine any notification by a client within 15 days, and it shall institute a supervisory review *ex officio*, unless it establishes that

a) the notification falls outside its competence,

b) a legal remedy proceeding is pending concerning the violation underlying the notification, or a final and binding decision has already been passed by an administrative authority or court regarding that violation, unless the final and binding decision confirms that the violation does not constitute a procedural violation affecting the merits of the case,

c) the violation alleged in the notification is insignificant,

d) the notification was filed anonymously,

e) the notification is manifestly unfounded,

f) the notification was filed repeatedly without invoking any new fact or data.

(3) In the course of a supervisory review, the notifier may not exercise the rights of a party as provided for under the Act on the Code of General Administrative Procedure, with the proviso that he shall be informed of the outcome of the supervisory review by the Supervisory Authority.

(4) The Supervisory Authority shall also institute a supervisory review if it seems likely, even on the basis of an anonymous notification, that an electronic administration organ violated its obligations, or the rights of a client, provided for under this Act, provided that the violation affects a large group of clients or causes significant harm to interests or risk of damage.

Section 48 (1) As part of supervisory reviews, the Supervisory Authority shall verify compliance with the requirements laid down in this Part concerning electronic administration by conducting administrative audits.

(2) If the Supervisory Authority establishes that an electronic administration organ violated the rules laid down in this Part or an implementing decree to this Act, it

a) shall oblige the electronic administration organ concerned to cease its violation and proceed in a lawful manner,

b) may oblige the electronic administration organ concerned, with a view to the future and by setting a time limit as necessary, to proceed in a lawful manner,

c) may, in addition to establishing the fact of violation, oblige the electronic administration organ concerned to prepare an action plan within a time limit set,

d) may erase an organ referred to in point 17. *l)* of section 1 from the register of electronic administration organs,

e) may oblige the manager with the relevant functions of the electronic administration organ to attend a training on electronic administration,

f) may impose a fine as specified by the Government in a decree,

g) may order its decision to be published, provided that doing so is justified for facilitating electronic administration or protecting the rights of a significant number of clients as provided for under this Act.

(3) A legal consequence under paragraph (2) *d)* may be applied only in combination with a legal consequence under paragraph (2) *g)*; other legal consequences under paragraph (2) may also be applied in combination with each other.

29. Coordination proceedings

Section 49 (1) The Supervisory Authority shall conduct a coordination proceeding *ex officio* or upon request from an electronic administration organ. A coordination proceeding shall aim to implement or modify electronic administration pursuant to the provisions of this Act.

(2) In the course of a coordination proceeding, the Supervisory Authority

a) shall provide professional assistance in implementing or modifying electronic administration,

b) shall engage in consultations with the regulated electronic administration service provider and the electronic administration organ,

c) may make recommendations regarding the use of specific services or solutions.

30. Database of matters administrable by electronic means

Section 50 (1) The Supervisory Authority shall maintain and make publicly available a database of

a) matters that may be administered by electronic means, and

b) electronic administration organs

with the contents specified by the Government in a decree.

(2) Any person may consult the database of matters administrable by electronic means free of charge and without registration or being identified by electronic means.

(3) If an organisation undertakes to apply this Act voluntarily regarding specific matters, it shall notify its intent to the Supervisory Authority by way of provision of data.

(4) The Supervisory Authority shall examine the notice received, and, in addition to notifying the organisation concerned accordingly, it shall enter the organisation and its matters administrable by electronic means into the database of matters administrable by electronic means, provided that the provision of data meets all statutory requirements.

(5) If a notification, notice, or administration method undertaken by an organisation fails to meet all statutory requirements, the Supervisory Authority shall notify the organisation concerned accordingly, pointing out any and all shortfalls.

(6) If an organisation that undertook voluntarily to provide electronic administration pursuant to this Act intends to cease the provision of electronic administration pursuant to this Act regarding any matter, it shall notify its intent 15 days prior to that change.

PART THREE

COOPERATION IN THE FIELD OF INFORMATION TECHNOLOGY BETWEEN ELECTRONIC ADMINISTRATION ORGANS AND OTHER ORGANS

CHAPTER X

THE FUNDAMENTAL REQUIREMENTS OF COOPERATION

31. Application of the rules on cooperation

Section 51 (1) With the exception provided for under paragraph (1a), the rules laid down in this Part shall apply to communication and information transfers between, and administration of matters, and cooperation in the field of information technology as provided for by this Act in proceedings, involving any information transfer between electronic administration organs and organs performing a public duty designated by the Government (hereinafter jointly "cooperating organs"), in their capacity as such, as required or permitted by this Act or any other law.

(1a) The rules relating to joining and operating the single digital gateway and required for implementing Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012 shall be laid down in a government decree.

(2) The provisions laid down in this Part shall not apply to

a) legislative procedures,

b) preparation of decisions by the Government,

c) election procedures, the preparation and holding of referendums,

d) transfer of data or documents, or provision of data from the records of, and procedures conducted by, national security services or the National Security Authority,

e) internal records and draft decisions of cooperating organs,

f) procedures for granting access to non-public data and documents containing non-public data, within the meaning of the Act on the right to informational self-determination and on the freedom of information, of cooperating organs used for supporting decision-making, subject to the exceptions provided for under this Act,

g) transfers of classified data and documents containing classified data, unless provided otherwise in an Act,

h) relations governed by civil law between cooperating organs,

i) transfers of public documents to archives, or

j) handover-acceptance procedures relating to legal succession of cooperating organs under public or private law.

(3) The provisions laid down in this Part shall not apply to any communication, information transfer, or administration of matters regulated by, and as regulated in, directly and generally applicable mandatory legal acts of the European Union. A law may derogate from the provisions of this Act to an extent and in a way that is necessary to implement a mandatory legal act of the European Union.

32. The fundamental principles of cooperation

Section 52 (1) In situations specified in this Act, a cooperating organ shall obtain from another cooperating organ by electronic means information that is necessary for administering a matter under section 2 (1) (for the purposes of this Part, hereinafter "matter") or performing its task and that was generated at or has already been acquired by the other cooperating organ, or a decision or statement of the other cooperating organ that is necessary for administering a matter.

(2) Cooperating organs shall communicate with each other by electronic means, unless doing so is prohibited by an Act.

(3) Cooperating organs shall implement their electronic information systems and develop their existing electronic information systems in such a manner that it is suitable, in line with the requirements laid down in this Act, for the purposes of their cooperation in the field of information technology as required under this Act (hereinafter "IT cooperation").

(4) As part of their IT cooperation, cooperating organs shall use solutions that meet all relevant electronic information security requirements, are related to the given form of their cooperation and are proportionate to the risks and costs of the cooperating organs concerned.

(5) A cooperating organ may not make any form of IT cooperation conditional upon the payment of any duty, fee, or other remuneration, other than compensation for certified costs specified by law.

(6)

33. Data processing

Section 53 A cooperating organ shall transfer to an electronic administration organ proceeding in a matter commenced upon request or initiative by a client any personal data that is available to the cooperating organ and necessary for administering the given matter; such data shall be processed by the proceeding electronic administration organ to the extent necessary and sufficient for administering that matter, provided that the electronic administration organ informed the client, in a manner meeting applicable requirements, about all material circumstances of processing such data.

34. Data transfer register

Section 54 With regard to personal data transferred under this Act, a cooperating organ providing personal data shall keep its records on data processing activities in a manner enabling clients to obtain information, by electronic means and within no more than 3 days, on their data transferred, the receiving cooperating organ, and the purpose and date of transfer.

35. The fundamental technical requirements of IT cooperation

Section 55 (1) In the course of their IT cooperation implemented for the purpose of administering matters and performing their tasks, cooperating organs shall primarily use solutions that support the entire cooperation process, unless doing so is prohibited by an Act.

(2) A cooperating organ may not require unreasonably a specific telecommunication service or technical implementation or solution to be used for IT cooperation, unless doing so would not result in any direct or indirect expenditure on the side of any organ engaging in cooperation with the organ concerned.

(3) A cooperating organ shall implement, develop, and operate its electronic information system, as specified in section 52 (3), in compliance with the requirements specified in paragraphs (1) and (2), ensuring that, as necessary for the purposes of IT cooperation,

a) it meets the technological security requirements laid down in the Act on the electronic information security of state and local government organs, as well as the requirements laid down in its implementing decree on requirements concerning secure information devices and products, and assignment to security classes and security levels,

b) it is based on standards and technical solutions that are available also to other cooperating organs,

c) it is suitable for cooperating with regulated and central electronic administration services,

d) it can ensure that its services meet the availability requirements laid down in an implementing decree to this Act,

e) it does not hinder modifications or developments, and

f) it allows other organs performing a public duty to reuse technical solutions without prejudice to any of the above-specified requirements.

(4) A cooperating organ shall also perform its publication obligations provided for under this Act using the publication interface specified in a decree by the Government.

(5) The cooperating organ shall ensure that each person concerned is informed about the source and transfer of his personal data.

(6) State organs relying upon a central electronic administration service referred to in section 74 (3) *d) da)* shall perform their obligation to provide information to a person concerned regarding the transfer of his data, as provided for under paragraph (5), in line with section 74 (3) *d) db)*.

Section 56 (1) A cooperating organ shall schedule any predictable technical activity that restricts or interrupts its IT cooperation to a time when the impact of such interruption on the administration of matters and the performance of public duties is minimal.

(2) A cooperating organ shall notify all cooperating organs and the Supervisory Authority at least 5 days in advance about any upcoming scheduled technical activity that restricts or interrupts its IT cooperation.

(3) Any malfunction that restricts or interrupts IT cooperation shall be reported to cooperating organs, and eliminated, without delay, and cooperating organs shall be provided with, and notified simultaneously about, other means of cooperation.

CHAPTER XI

ELECTRONIC COMMUNICATION BETWEEN COOPERATING ORGANS

36. Contact addresses

Section 57 (1) Cooperating organs shall publish, pursuant this Subtitle, their secure electronic contact addresses and electronic mail addresses.

(2) A secure electronic contact address may be

a) a secure electronic delivery service address,

b) an electronic mail address with regard to which the addressee undertakes to confirm receipt of any information, or

c) a contact address as specified by the Government in a decree.

(3) A cooperating organ shall publish at least one contact address referred to in paragraph (2) *a)* or *b)* and it may also publish one or more secure electronic contact addresses and the provisions on the use of such addresses, provided that the cooperating organ ensures compliance with all requirements provided for under this Subtitle with regard to also such additional addresses.

(4) A cooperating organ shall check at least once every working day and confirm within one working day the delivery of items to its contact addresses under paragraph (1).

(5) A cooperating organ shall publish in advance any change to its electronic contact addresses.

37. Method of communication

Section 58 (1) Cooperating organs communicating by electronic means may do so only in a manner specified in this Act; in the course of such communication, the cooperating organs shall ensure that a person who made a statement included in a delivered item can be identified by electronic means, that each delivered item is intact, that delivery of each item is confirmed, and that the date and time of each delivery can be established (hereinafter "secure electronic communication").

(2) Secure electronic communication may be conducted by

a) service to a published secure electronic contact address, or

b) using a document transfer service between document management systems.

(3) An item shall be considered delivered

a) on the next working day after sending, in a situation described in paragraph (2) *a)*,

b) at the date and time of a successful document transfer as confirmed by the service provider, in a situation described in paragraph (2) *b)*.

(4) A cooperating organ initiating electronic communication shall select a contact address of the other organ to be contacted by electronic means from among the published secure electronic contact addresses, with due regard to any additional information published by the cooperating organ concerned.

(5) Automatic information transfer shall also constitute secure electronic communication, provided that the *ex-post* identifiability of any information transferred is ensured by tracking changes or by any other means.

(6) In a situation described in paragraph (5), any information shall be considered delivered at the date and time specified in the relevant information transfer policy or agreement.

Section 59 (1) Cooperating organs may also communicate with each other by electronic means that do not qualify as secure electronic communication, provided that no legal consequence is attached to service by law, or communication is merely for informational purposes.

(2) With a view to establishing cooperation or providing internal processes, a cooperating organ may use regulated electronic administration services and central electronic administration services as provided for under Part Two.

(3) When engaging in cooperation under this Act, a cooperating organ shall, as necessary, produce or have produced, using a central electronic administration service within the meaning of the Act on electronic administration, an authentic electronic copy pursuant to the provisions of this Act of documents that are available in a paper-based format only.

CHAPTER XII

GENERAL RULES OF COOPERATION IN THE FIELD OF INFORMATION TECHNOLOGY

38. Sources of information

Section 60 (1) If a cooperating organ is aware that a piece of information it is not in possession of but needs for administering a pending matter or carrying out a task is available from a primary source of information referred to in paragraph (3), it shall obtain the relevant piece of information from the primary source of information by electronic means, provided that the cooperating organ is authorised by an Act to process that piece of information if it constitutes personal or classified data, and that it is not prohibited from doing so by an Act.

(2) A cooperating organ shall obtain a piece of information referred to in paragraph (1) from a primary source of information by way of automatic information transfer, provided that an automated information access interface is available for that purpose, and doing so is not prohibited by an Act.

(3) A piece of information shall be considered available from a primary source of information if

a) it is recorded in a publicly certified register,

b) it is not recorded in a publicly certified register, but it was generated by a cooperating organ, or

c) it is identified as such by law with reference to the primary source of information.

(4) A cooperating organ shall be presumed, for the purposes of paragraph (1), to be aware of a piece of information being available from a primary source of information

a) in a situation described in paragraph (3) *a)* or *c)*,

b) if that piece of information was generated by a cooperating organ based on the register of sources of information,

c) if the client concerned or the cooperating organ proceeding in the given matter informed it accordingly, with reference to the given piece of information and the primary source of information.

(5) Unless prohibited by an Act, a cooperating organ shall obtain a piece of information from a primary source of information by electronic means if it has any doubt regarding the correctness or reality of a piece of information at its disposal.

(6) A law may specify circumstances under which, or periods calculated from the recording of the data or generation of the document concerned after the expiry of which, it shall be presumed that the data or the content of a document held by the cooperating organ is not in line with reality.

Section 61 (1) If a piece of information a cooperating organ is not in possession of but needs for administering a pending matter or carrying out a task is not available from a primary source of information, but the cooperating organ concerned knows that it is available from a secondary source of information, it shall obtain the relevant piece of information from the secondary source of information by electronic means, provided that the cooperating organ is authorised by an Act to process that piece of information if it constitutes personal or classified data, and that a law does not provide for otherwise.

(2) A piece of information shall be considered available from a secondary source of information if

a) it was obtained by a cooperating organ from a primary source of information, or

b) it was not generated by a cooperating organ, and it was obtained by a cooperating organ from not a cooperating organ.

(3) A cooperating organ shall be presumed to be aware of a piece of information being available from a secondary source of information if

a) the given piece of information was obtained, according to paragraph (2), by a secondary source of information on the basis of a statutory provision or pursuant to the register of sources of information, or

b) the client concerned informed the cooperating organ proceeding in the given matter accordingly, with reference to the given piece of information and the secondary source of information.

(4) A cooperating organ may obtain from a secondary source of information a piece of information that is available from a primary source of information also if it is ensured by way of automatic information transfer that the information available from the secondary source of information is identical to information available from the primary source of information, provided that all the other conditions specified in this section are met.

(5) A cooperating organ transferring information that is available from a secondary source of information shall inform the cooperating organ that initiated the information transfer about

a) the date on, and source of information from, the given piece of information was obtained, subject to the exception specified in paragraph (4), and

b) all other known circumstances that may influence any judgment regarding the reality, correctness, or usability of the piece of information concerned.

Section 62 (1) A cooperating organ possessing a piece of information referred to in section 61 (2) *a)* shall verify before using or transmitting the given piece of information that it is identical to information available from a primary source of information, unless provided otherwise by an Act, and unless it is ensured by way of automatic information transfer that the information available from the secondary source of information is identical to information available from the primary source of information.

(2) A cooperating organ shall transmit by electronic means a piece of information that is available from a primary or secondary source of information within 3 days after receipt of a corresponding electronic request for information transfer, or, if the statutory conditions for such an information transfer are not met, it shall refuse the request and inform the initiating cooperating organ accordingly, with reference to the underlying reasons.

(3) If a cooperating organ that requested an information transmission does not accept the refusal of its request under paragraph (2), the cooperating organs shall consult about the situation within 3 days.

Section 63 (1) If a cooperating organ has any doubt regarding the reality or correctness of any data or content of a document that is available from a primary or secondary source of information, it shall notify the cooperating organ that is the source of information accordingly and without delay, on the working day after becoming aware thereof at the latest; the notified cooperating organ shall conduct its own review proceeding and inform the other cooperating organ about its result.

(2) If a given piece of information changes, the primary source of information concerned shall initiate an information transfer from the cooperating organ that took over and entered the given piece of information into its statutory register.

(3) A cooperating organ serving as a source of information may also provide services, in addition to the provisions laid down in paragraph (2) and under an information transfer policy or agreement, as part of which it informs any cooperating organ initiating an information transfer about any data change or other event that may have an impact on the reality or correctness of the content of a document.

39. The methods of transmitting information

Section 64 (1) Cooperating organs shall transmit pieces of information under Subtitle 38 by way of

a) simple information transfers, or

b) automatic information transfers.

(2) A cooperating organ specified in a government decree shall set up and make available to other cooperating organs an automatic information transfer interface for the transmission of pieces of information, as specified in a government decree, by automatic information transfer.

(3) A cooperating organ may also set up and make available to other cooperating organs an automatic information transfer interface for the automatic information transfer of data other than personal data, as well as documents not containing any personal data, even in the absence of relevant statutory provisions, and it may also determine the terms and conditions of using such an interface.

(4) A cooperating organ shall receive pieces of information using an automatic information transfer interface that is suitable for such transfers, if available.

(5) Information transfers involving the transmission of personal data between cooperating organs that are connected to the data link register service and use identifiers other than natural identification data may also be carried out using the data link register, provided that the relevant statutory conditions are met.

(6) Instead of using information transfers pursuant to paragraph (1), a cooperating organ may also make pieces of information, which are at its disposal and may or are to be transferred under a law, available to another cooperating organ by electronic means, provided that the necessary information technology conditions are met. If delivery has any legal consequence by law, or if a piece of information is to be provided within a time limit specified by law, the cooperating organ providing the information shall inform the other cooperating organ pursuant to section 58 (2) about the fact of making available the given piece of information.

40. Information transfer policies and agreements

Section 65 (1) A cooperating organ shall adopt an information transfer policy, and publish, and submit it to the Supervisory Authority by electronic means at least 15 days before launching its information transfer service.

(2) An information transfer policy shall specify

a) the scope of information under paragraph (3) available at the given cooperating organ as a primary or secondary source of information,

b) the particulars of any automatic information transfer interface operated by the given cooperating organ, including the information offered through, and the terms and conditions of, using the information transfer interface,

c) the terms and conditions of transferring pieces of information under Subtitle 38 by electronic means pursuant to Subtitle 39, and

d) any other required content element as specified by the Government in a decree.

(3) An information transfer policy shall apply at least to the following information:

a) data kept by the given cooperating organ in a publicly certified manner,

b) decisions passed by the given cooperating organ on the merits of matters,

c) statements of specialist authorities issued by administrative authorities,

d) contracts covered by a statutory obligation to conclude a contract,

e) any other information specified by the Government in a decree.

(4) By submitting a request for information transfer, a cooperating organ shall accept, and agree to be bound by, the provisions laid down in a published information transfer policy.

(5) In justified cases, cooperating organs may deviate from their respective information transfer policies by entering into information transfer agreements, with the proviso that any such information transfer agreement shall be notified to the Supervisory Authority by electronic means before it enters into force.

Section 66 (1) A cooperating organ shall amend its information transfer policy within 30 days after the occurrence of the event necessitating an amendment.

(2) A cooperating organ shall publish and notify to the Supervisory Authority any amendment to, or the termination of, its information transfer policy at least 15 days before the effective date of a given amendment.

(3) A cooperating organ shall notify to the Supervisory Authority any amendment to or the termination of its information transfer agreement before the effective date of the amendment or termination.

(4) An information transfer policy or an amendment to such a policy may not enter into force before the 15th day following its publication.

Section 67 (1) With regard to and covering regional state administration organs with the same material competence, a controlling state administration organ, or with regard to and covering regional chambers, a national chamber may adopt a uniform information transfer policy.

(2) In justified cases, an organ covered by a uniform information transfer policy may adopt its own information transfer policy, or enter into an information transfer agreement, derogating from the applicable uniform information transfer policy.

(3) A uniform information transfer policy and any amendment to such a policy shall be published and notified to the Supervisory Authority at least 30 days before its effective date.

(4) A uniform information transfer policy may not enter into force before the 30th day following its publication.

(5) In situations not regulated under this section, the rules applicable to information transfer policies shall apply to uniform information transfer policies.

41. The register of sources of information

Section 68 (1) The Supervisory Authority shall keep a register of the scope of information available at cooperating organs and of automated information access interfaces operated by cooperating organs (hereinafter "register of sources of information").

(2) The Supervisory Authority shall keep the register of sources of information *ex officio* on the basis of information transfer policies and agreements and any amendments to such policies and agreements.

(3)

(4) The register of sources of information shall be available to any member of the public without identification, free of charge or any fee payment.

(5) The detailed content of the register of sources of information and the procedural rules on its keeping shall be determined by the Government in a decree.

42. List of data and document designations

Section 69 (1) The Supervisory Authority shall keep a list on the scope of information that are relevant for the purpose of ensuring IT cooperation, and on their designations (hereinafter "list of data and document designations"). The list shall include all designations, their explanations, and other information as necessary for the processing of data and documents.

(2) Information transfer policies shall also specify the designations of data, as specified in the list of data and document designations, a given cooperating organ may take over by using an information transfer service.

(3) The list of data and document designations shall be available to any member of the public without identification, free of charge or any fee payment.

(4) The detailed content of the list of data and document designations and the procedural rules on its keeping shall be specified by the Government in a decree.

CHAPTER XIII

SPECIAL FORMS OF COOPERATION

43. Cooperation in the field of making decisions and statements

Section 70 (1) If a cooperating organ knows that it needs a decision passed by another cooperating organ for administering a pending matter or carrying out its task, and the necessary decision can be passed *ex officio* or in a proceeding initiated by the cooperating organ concerned, it may request by electronic means that a decision be passed by the eligible organ, unless provided otherwise by law.

(2) A cooperating organ eligible to pass a decision referred to in paragraph (1) shall communicate its decision to the requesting cooperating organ by electronic means.

Section 71 (1) If a cooperating organ knows that it needs a statement made by another cooperating organ for administering a pending matter or carrying out its task, and it can obtain that statement, it shall invite the cooperating organ concerned by electronic means to make a statement.

(2) A cooperating organ shall make its statement referred to in paragraph (1) by electronic means within 8 days, unless a different time limit for making that statement is set by law.

44. Interoperability of registers containing address data

Section 72 (1) The central address register shall serve to ensure the consistency of address management and to improve the interoperability of registers that are kept by cooperating organs and contain address data.

(2) The central address register shall constitute a central register that improves the interoperability of different registers, and that serves as an authentic data source of address data, through an information transfer service, for registers that are kept by cooperating organs and contain address data.

(3) The detailed procedural rules on keeping and operating the central address register and managing address data in a consistent manner shall be laid down in a government decree adopted based on an authorisation by this Act.

(4) The detailed rules on generating address data in a consistent manner shall be laid down in a government decree adopted based on an authorisation by this Act.

Section 73 (1) With a view to ensuring that entries are made into the address register only by persons authorised by law and in full compliance with applicable legislation, the organ responsible for operating the central address register shall keep a register of persons authorised to record addresses (hereinafter "access authorisation record"). For that purpose, the organ responsible for operating the central address register may process the natural identification data of registered persons.

(2) The access authorisation record shall contain the following:

a) natural identification data of the persons concerned,

b) the area of territorial competence of each organ responsible for generating addresses,

c) the commencement date and period of any access authorisation, and

d) the reason for and date of any change to or cancellation of any access authorisation.

(3) Data entered into the access authorisation record may be obtained only for the purposes of verifying the access authorisation of a person and compliance with statutory provisions by a person with access authorisation.

(4) Data entered into the access authorisation record shall be deleted within 5 years after the termination of access authorisation.

(5) If any address data whose determination falls within the competence of a local government representative body needs to be obtained for the purpose of generating a new address in or modifying or deleting an existing address from the central address register, the representative body concerned shall pass its decision as necessary for generating the address at its next session held after receipt of the corresponding request by the organ responsible for operating the central address register, and it shall notify the organ responsible for operating the central address register accordingly and without delay.

(6) Address data that is recorded in the central address register and is of public interest or is accessible on public interest grounds may be accessed through state or local government registers that are connected to the central address register.

CHAPTER XIII/A

CENTRAL STORAGE OF IMAGE, SOUND, AND AUDIO-VISUAL RECORDINGS

44/A. Central storage of image, sound, and audio-visual recordings

Section 73/A (1) An organ designated by the Government in decree (hereinafter "storage provider") shall ensure the storage of image, sound, and audio-visual recordings (hereinafter "recording") produced by

a) road operators,

b) the police in the course of traffic policing measures,

c) image recorders deployed by the police,

d) image recorders deployed by a public space supervisory authority,

e) entities pursuing personal and property protection activities for the protection of private areas open to public of entities providing financial services or supplementary financial services that are necessary for their tasks,

f) service providers within the meaning of section 8 (1) of Act XLI of 2012 on passenger transport services,

g) toll collectors within the meaning of the Act on toll to be paid for using highways, motorways and main roads proportionate to the distance travelled (hereinafter jointly "mandatory central storage user")

by providing information technology applications and central storage space.

(2) The storage provider shall ensure the storage of data recorded by the service provider referred to in section 16/A *e)* of the Act on the local governments of Hungary by means of providing information technology applications and central storage space.

(3) The activities of the storage provider shall be limited to storing recordings and data at its central storage space and providing the information technology application specified in section 73/B; it may not access or perform any data processing operation with any recording or data stored at its central storage space.

(4) Mandatory central storage users shall cooperate with the storage provider as required under a government decree, and, where the conditions laid down in a government decree are met, they shall use the central storage space provided.

(5) Mandatory central storage users may use the central storage space under the terms and conditions laid down in the government decree referred to in paragraph (4).

Section 73/B (1) If the police, a national security service, professional disaster management organ, and, in a criminal proceeding, the court, prosecution service, investigating authority, or organ conducting preparatory proceedings (hereinafter jointly "eligible data recipient") is authorised to take over any recording or data produced by a mandatory central storage user as laid down in an Act; the mandatory central storage user concerned shall ensure the transmission of relevant data using the information technology application operated by the storage provider, provided that it in fact uses the central storage space.

(2) No recording or data produced by a mandatory central storage user may be requested from the storage provider; to the transfer of such data, the data transfer rules laid down in the applicable sectoral Act shall apply.

44/B. Registration of mandatory central storage users and eligible data recipients

Section 73/C (1) A register of mandatory central storage users and eligible data recipients shall be kept for the purpose of storing data of the storage provider, mandatory central storage users, and eligible data recipients that is required for access, and of ensuring the verification of the legality of data processing.

(2) The register of mandatory central storage users and eligible data recipients shall contain the following data concerning each mandatory central storage user and eligible data recipient:

a) name,

b) postal address,

c) phone number,

d) fax number,

e) electronic mail address,

f) type of access authorisation, and the fact and date of granting or cancelling any such access authorisation,

g) with regard to any person authorised to access on behalf of the organisation concerned (hereinafter "person with access authorisation"):

ga) family and given name,

gb) position,

gc) organisational unit,

gd) scope and extent of access authorisation, and the fact and date of granting or cancelling any such access authorisation,

ge) unique identifier.

44/C. The conditions for recording data at the central storage space and accessing data stored at the central storage space by electronic means using an information technology application

Section 73/D (1) Mandatory central storage users and eligible data recipients shall request, by submitting an application to the storage provider (hereinafter "application for unique identifier"), unique identifiers as necessary for recording data in the central storage space and accessing data stored in the central storage space by electronic means and using an information technology application.

(2) An application for a unique identifier shall contain all data specified in section 73/C (2) *a)* to *f)* and *g) ga)* to *gd)*.

(3) Mandatory central storage users and eligible data recipients shall notify the storage provider about any change to the data specified in paragraph (2) within three working days of the change.

(4) Within eight days of receipt of an application for a unique identifier, the storage provider shall inform

a) the mandatory central storage user concerned of the unique identifier of the person with access authorisation, as well as the technical information required for using the central storage space and the information technology application,

b) the eligible data recipient concerned of the unique identifier of the person with access authorisation, as well as the technical information required for using the information technology application.

(5) Recordings and data recorded in the central storage space may be processed only by electronic means and using an information technology application.

44/D. Data access register

Section 73/E (1) The storage provider shall keep a data access register for the purpose of verifying the legality of data requests sent to and data transmissions from the central storage space by electronic means and using an information technology application.

(2) The data access register shall contain:

a) identification data of the recording concerned,

b) the unique identifier of the person with access authorisation,

c) the date and time of data transmission,

d) the statutory provision authorising the eligible data recipient to process data in its proceeding or in the course of pursuing its control activities or exercising its control functions,

e) designation of the data transmitted.

(3) Data may be requested from the data access register by

a) the National Authority for Data Protection and Freedom of Information,

b) the court, prosecution service, investigating authority, or organ conducting preparatory proceedings with a view to preventing, detecting, and conducting criminal proceedings regarding criminal offences indicating the abuse of data,

c) a national security service or law enforcement organ with a view to performing its statutory tasks.

CHAPTER XIV

REGULATED AND CENTRAL ELECTRONIC ADMINISTRATION SERVICES USED IN THE COURSE OF COOPERATION

Section 74 (1) With a view to facilitating cooperation, a cooperating organ may use regulated and central electronic administration services, as specified in Chapters VI and VII and the implementing decree to this Act, in the course of cooperation and its internal electronic administration processes.

(2) In the course of any use referred to in paragraph (1), provisions laid down in Chapters VI and VII shall apply as appropriate, in line with the rules on data processing.

(3) In addition to services referred to in section 38, the Government shall provide the following central electronic administration services acting through a service provider designated by law:

a) a central filing system ensuring that certain phases of document processing are carried out using a central service,

b) an electronic document storage service ensuring that electronic documents stored using the service remain authentic and permanently readable and understandable,

c) a document transfer service between document management systems ensuring that documents and sets of documents recorded in an electronic filing book are transferred between cooperating organs in a documented manner,

d) a central government service bus under the framework of which

da) the service provider ensures a secure environment for automatic information transfer by connecting to the automatic information transfer interfaces of information systems used by cooperating organs and other organisations connecting to the service voluntarily or, in the absence of such interfaces, as an information transfer service, and

db) the service provider, with regard to the data transfer registers of connected cooperating organs' information systems containing personal data, provides one-stop-shop information services in order to support the provision of information to persons concerned regarding the transmission of their personal data.

(4) An Act or government decree may make mandatory the use of a central electronic administration service also in the course of such cooperation.

(5) The Government shall provide legal entities referred to in section 1 (17) *a)* to *i)* and *k)*, free of charge, with all regulated electronic administration services and central electronic administration services that are necessary for the purposes of cooperation and internal electronic administration processes.

CHAPTER XV

THE COORDINATION AND SUPERVISION OF COOPERATION

45. The supervision of cooperation

Section 75 (1) Acting within its functions and powers provided for under this Part, the Supervisory Authority shall

a) keep the register of sources of information,

b) receive notifications regarding information transfer policies and information transfer agreements,

c) keep the list of data and document designations,

d) adopt technical guidelines, and

e) carry out the supervision of the activities of cooperating organs as regulated under this Act, with the exception of the supervision or facilitation of the enforcement of rights to the protection of personal data and rights to access public interest data and data accessible on public interest grounds.

(2) Acting within its functions and powers provided for under paragraph (1) *e)*, the Supervisory Authority

a) shall verify, by conducting supervisory reviews, that the activities of cooperating organs meet the requirements laid down in this Act and its implementing decrees,

b) shall review, by conducting supervisory reviews, all notified information transfer policies and agreements,

c) may file an objection to any notified information transfer policy,

d) shall review any complaint or recommendation submitted against a cooperating organ regarding its obligations provided for under this Act, and it may make recommendations, on the basis of such complaints or recommendations, to the competent authority or an organ or person with power to initiate legislation,

e) shall formulate proposals for action to cooperating organs to facilitate the application of this Act,

f) shall develop annual review plans for conducting supervisory reviews and comprehensive supervisory reviews.

(3) If invited by the Supervisory Authority to do so, a cooperating organ shall disclose all data required for keeping its register of sources of information up to date. If no data is provided or the provided data is false, the Supervisory Authority shall institute a supervisory review.

(4) In the context of issues affecting information security, the Supervisory Authority shall involve the authority responsible for supervising the security of electronic information systems in the performance of its tasks referred to in paragraph (2) *a)*, *b)*, or *e)*.

46. Supervisory review

Section 76 (1) If an information transfer policy, information transfer agreement, any change to such a policy or agreement is notified to the Supervisory Authority, it shall conduct a supervisory review to establish whether the activities of the cooperating organ concerned are consistent with the provisions laid down in this Act, its implementing decrees, related laws, and the information transfer policy or information transfer agreement concerned.

(2) In the course of a supervisory review, the Supervisory Authority may access the information transfer agreement concerned, with the proviso that the Supervisory Authority shall handle in a confidential manner and may not publish any information disclosed to it in the course of the supervisory review.

(3) The Supervisory Authority shall compare the information transfer policy concerned to the content of the technical guidelines referred to in section 78 (1) and the national standards on cooperation, as specified in this Act.

(4) A supervisory review shall not constitute an administrative case, and the provisions laid down in the Act on the Code of General Administrative Procedure concerning administrative audits shall apply to it, with the following derogations and other derogations specified in a government decree:

a) a supervisory report shall be produced as the result of a supervisory review,

b) the provisions of section 78 of Act CL of 2016 on the Code of General Administrative Procedure shall apply to a supervisory report, with the proviso that it shall not contain any personal data that may not be published.

(5) If the Supervisory Authority obtains any information during its supervisory review that may pose an information security risk, it shall notify the authority responsible for supervising the security of electronic information systems without delay.

(6) The Supervisory Authority may carry out a review under paragraph (1) as part of a comprehensive and consolidated supervisory review on the basis of an annual supervisory audit plan.

47. Coordination of cooperation

Section 77 (1) The Supervisory Authority shall conduct a coordination proceeding *ex officio* or upon request from a cooperating organ. A coordination proceeding shall aim to implement or change, pursuant to the provisions of this Act, the method of cooperation under this Act.

(2) In the course of a coordination proceeding, the Supervisory Authority

a) shall provide professional assistance in developing or modifying a method of cooperation,

b) shall hold consultations with cooperating organs,

c) may make recommendations regarding the use of specific services or solutions.

48. Technical guidelines

Section 78 (1) With regard to issues specified in this Act or a decree adopted based on an authorisation granted by this Act, the Supervisory Authority may adopt and make available to the public, free of charge or restriction, non-binding technical guidelines on

a) facilitating and improving the efficiency and security of IT cooperation,

b) the method of information transfer services, and

c) the development of information transfer policies.

(2) The Supervisory Authority shall review its technical guidelines, and modify or replace such guidelines as necessary, on the basis of supervisory reviews and coordination proceedings conducted by the Supervisory Authority as necessary, but at least once every two years.

PART FOUR

TRUST SERVICES

Section 79 (1) The provisions laid down in this Part shall apply to

a) trust service providers established in Hungary and trust services provided by them, within the meaning of the eIDAS,

b) parties relying upon the trust services referred to in point *a)*.

(2) The provisions laid down in this Part shall not apply to trust services that are used exclusively within closed systems pursuant to Article 2(2) eIDAS.

CHAPTER XVI

GENERAL CONDITIONS FOR PROVIDING TRUST SERVICES

49. Taking up the provision of trust services

Section 80 (1) Trust service providers established in Hungary shall notify their intent to take up the provision of trust services to the trust service supervisory body using the standard electronic form of the trust service supervisory body.

(2) Before launching a qualified trust service, the notification under paragraph (1) shall be submitted by the trust service provider concerned at least 30 days before taking up the provision of the trust service.

(3) The documents specified in an implementing decree to this Act shall be attached to the notification by the trust service provider concerned.

(4) A notification made under paragraph (1) shall be reviewed and the trust service provider submitting the notification shall be registered by the trust service supervisory body, provided that it meets applicable statutory requirements.

(5) A trust service provider shall notify the trust service supervisory body of any change, as compared to data entered into the register based on notifications, concerning its operation or the provision of trust services.

(6) A trust service provider providing qualified trust services shall notify the trust service supervisory body at least 30 days in advance about any planned change, as compared to data entered into the register based on notifications, concerning its operation or the provision of trust services.

(7) Notifications and applications relating to trust services may be submitted to the trust service supervisory body directly.

50. Service contracts and requirements concerning the provision of trust services

Section 81 (1) A trust service provider and a trust service client shall enter into a service contract regarding the provision of trust services.

(2) Before contracting and in addition to providing all information required under eIDAS, trust service providers shall inform relying parties about whether their trust services qualify as qualified trust services.

(3) In addition to those under paragraph (2), a trust service provider shall also provide its trust service clients with information required by any implementing decree to this Act, and it shall also make accessible to them any data or document specified in such a decree.

(4) Only persons without a criminal record and who are not subject to disqualification from a profession excluding them from providing trust services may serve as a qualified trust service provider natural person or as an executive officer, manager, or employee of a legal person or organisation without a legal personality operating as a qualified trust service provider.

(5) Detailed provisions concerning service contracts and other terms and conditions of providing trust services (in particular trust service policies and service policies) shall be laid down in an implementing decree to this Act.

(6) A trust service provider shall be entitled to provide its trust services subject to various terms and conditions (including, in particular, different rules on liability or applying different trust service policies).

(7) After concluding a contract, the trust service provider concerned shall provide its trust service client with a copy of the service contract, as well as the relevant trust service policy and service policy on a durable data-storage medium or in a downloadable format.

51. Verification concerning certificates issued through trust services

Section 82 (1) Any data contained in a certificate issued by a trust service provider shall be true, unless it is clear from the certificate itself that the data included was not verified by the issuing trust service provider (in particular when a pseudonym is used). To this end, a trust service provider shall verify all data to be included in a certificate; in particular and depending on the content of a certificate, the trust service provider concerned shall verify the identity of the certificate subject, the authenticity of any identification data used to verify identity, including the verification of that data against relevant data, if any, recorded in a publicly certified or other central register, the right of representation of the representative acting for the certificate subject before the trust service provider, the subsistence of the right of representation to be recorded in the certificate, the right to dispose of the domain to be indicated in the certificate, the right to dispose of the IP address to be indicated in the certificate, the existence of the organisational unit to be indicated in the certificate, and the right to exercise the regulated profession to be indicated in the certificate, if any.

(2) With regard to qualified trust services, a trust service provider shall verify identity pursuant to Article 24(1) eIDAS, with the proviso that the obligations provided for under paragraphs (3) to (8) shall be considered requirements under national law as referred to in the same paragraph of eIDAS. With regard to non-qualified trust services, a trust service provider shall verify identity in a manner specified in Article 24(1) eIDAS and according to the obligations provided for under paragraphs (3) to (8), with the proviso that, in addition to a certificate of a qualified electronic signature or of a qualified electronic seal referred to in Article 24(1)(c), it may also accept an advanced electronic signature or electronic seal.

(3) If a trust service provider intends to verify the identity of a natural person certificate subject by physical presence or equivalent means of identification, it shall do so on the basis of an official verification card suitable for verifying identity within the meaning of the Nytv., provided that the natural person concerned falls within the scope of the Nytv.

(4) If a trust service provider intends to verify the identity of a natural person certificate subject not covered by the Nytv. by physical presence or equivalent means of identification, it shall do so primarily on the basis of a travel document within the meaning of the Act on the entry and residence of persons having the right of free movement and residence or the Act on the entry and residence of third-country nationals.

(5) If a trust service provider verifies the identity of a person pursuant to paragraph (4) by physical presence or equivalent means of identification outside the territory of Hungary, and the natural person certificate subject concerned does not hold any of the travel documents specified in the laws referred to in paragraph (4), the trust service provider may verify his identity only on the basis of such reliable official documents or other documents, as specified

in its authentication policy, with regard to which the trust service provider is able to demonstrate toward the trust service supervisory body that, for the purpose of establishing and verifying the identity of a person, the given reliable official document or other document specified in its authentication policy affords the same degree of certainty as the means referred to in paragraph (4).

(6) If a trust service provider verified the identity of a natural person certificate subject pursuant to paragraph (3), it shall be obliged also to verify the validity of and all data indicated on the official verification card used to verify identity against the appropriate publicly certified official register.

(7) If a trust service provider verified the identity of a natural person certificate subject pursuant to paragraph (4) or (5), it shall also verify against the appropriate central registers the validity (authenticity) of and all data indicated on the official or other document referred to in paragraph (4) or (5) that is used as proof of identity. If such a register is not available or is not accessible by the trust service provider concerned, or if the costs of access and verification is disproportionately high, the trust service provider concerned shall record that fact, and it shall decide based on other available evidence whether it issues the given certificate to the certificate subject.

(8) If a certificate subject is an entity other than a natural person, the trust service provider concerned shall verify at least the full name and unique identifier, as indicated in the certificate, of the certificate subject. If a certificate subject is a person incorporated in Hungary, the trust service provider concerned shall verify the correctness and currency of such data on the basis of a relevant publicly certified register; if such a publicly certified register does not exist, the verification shall be carried out on the basis of the public deed of incorporation, and, in other respects, the provisions laid down in paragraph (5) shall apply as appropriate.

(9) If a representative acts on behalf of a certificate subject in front of a trust service provider, or if the certificate includes any partial or full right of representation, or any legal relationship that may also be construed as such (hereinafter jointly "right of representation"), the trust service provider concerned shall verify the subsistence and scope, as indicated in the certificate, of the right of representation against a law, publicly certified register, instrument of incorporation or, in the absence of such, an authorisation, and it shall record the result of the verification.

Section 82/A (1) The Government shall determine in a decree the other identification methods recognised at national level which provide equivalent assurance in terms of reliability to physical presence.

(2) If an other identification method under paragraph (1) is based on audio-visual recording, the trust service provider shall record in a retrievable way and in the form of a non-deteriorating audio-visual recording, and retain for ten years from recording, the entirety of the communication between the trust service provider and the natural person during identification by way of video technology, the provision of detailed information to the natural person about identification by way of video technology, and the express consent of the natural person.

(3) In a situation under paragraph (2), a trust service provider shall be entitled to store the image recording of the document verifying the identity of the natural person for the period specified in paragraph (2).

52. General obligations concerning certificates issued through trust services

Section 83 If a certificate issued by a trust service provider through a trust service also certifies any right of representation,

a) the trust service provider concerned shall notify the represented person without delay about the issuance of the certificate,

b) the trust service provider concerned shall withdraw, upon termination of the right of representation and if requested by the representative or the represented person, the certificate indicating the subsistence of the right of representation,

c) the trust service provider concerned may not indicate any pseudonym in the certificate without the consent of the represented person.

Section 84 (1) A trust service provider shall retain all available information relating to individual certificates, including information on the generation of each certificate, as well as all related personal data for at least ten years from the expiry of each certificate. If a relying party, authority, or court notifies a trust service provider of a legal dispute launched concerning the correctness or validity of any data included in a certificate, the trust service provider concerned shall be obliged to fulfil its retention obligation until the legal dispute is resolved with final and binding force, even if such resolution takes place more than ten years after the expiry of the certificate concerned. Until the expiry of the retention period, a trust service provider shall also provide means to determine the content of a certificate issued.

(2) A trust service provider may also perform its retention obligation by using a qualified archive service.

(3) In addition to the records referred to in Article 24(4) eIDAS, a trust service provider shall also keep information on the suspension of certificates issued by it continuously available, provided that the trust service provider concerned makes it possible to suspend a certificate in the context of its given trust service.

Section 85 (1) A trust service client shall notify the trust service provider concerned without delay about

a) any change to the following data: personal identification data that is necessary for identification and is indicated in the certificate; if the certificate was issued in relation to the representation of another person, data of the authorised representative and the represented person, and other data indicated in the certificate,

b) any irregularity noticed regarding the trust service or certificate concerned, as defined in a separate law, a service contract, or a service policy, or any other event affecting the trust service concerned, including in particular any possibility of use by an unauthorised person of a cryptographic or other security device provided by the trust service provider that is required for the use of the trust service,

c) the launch of any legal dispute concerning the trust service.

(2) A trust service client or a relying party certified in a certificate pursuant to section 82 may request a certificate to be revoked or, if the trust service provider concerned makes it possible to suspend a certificate in the context of its given trust service, suspended.

53. Suspension and revocation of certificates issued through trust services

Section 86 (1) With regard to a certificate issued by a trust service provider through a trust service, the trust service provider concerned may decide to make it possible to suspend the validity of its certificate in situations specified in its authentication policy, service policy, or service contract.

(2) If a trust service provider makes it possible to suspend a certificate, it shall suspend the validity of the certificate, and it shall publish the suspension, including the exact period of suspension, in its register without delay if

a) suspension is requested by a person referred to in section 85 (2),

b) the trust service provider becomes aware of any irregularity concerning its service, as defined by law, its service policy, or a service contract,

c) there is reason to believe that the data included in the certificate is incorrect,

d) ordered by the trust service supervisory body in a decision with administrative finality.

Section 87 (1) A trust service provider shall revoke a certificate and publish the revocation in its register without delay if

a) revocation is requested by a person referred to in section 85 (2),

b) the trust service provider becomes aware of any irregularity concerning its service, as defined by law, its service policy, or a service contract, that may not be remedied by suspending the certificate concerned, or the service provider does not make it possible to suspend a certificate,

c) the trust service provider learns that the data included in the certificate is incorrect,

d) ordered by the trust service supervisory body with a decision with administrative finality,

e) the given trust service is discontinued.

(2) The revocation of a certificate by a trust service provider may not concern a period before the date of the publication of the revocation.

(3) The trust service provider concerned shall specify in its service policy or service contracts the legal consequences of revoking a certificate before expiry.

(4) If a certificate not covered by Article 28(4) eIDAS is revoked, it also shall lose its validity from the moment of its revocation.

CHAPTER XVII

DISCONTINUATION OF TRUST SERVICES

Section 88 (1) If a trust service provider intends to discontinue a trust service, it shall notify accordingly the trust service supervisory body, its trust service clients, and all relying parties (other than trust service clients) indicated in its issued and yet unrevoked electronic signature and seal certificates at the time of discontinuing the trust service at the latest; if the trust service provider is a qualified trust service provider, such notification shall be given at least sixty days before discontinuing the trust service.

(2) If a trust service provider continues to provide any other trust service, it shall keep continuously available its registers that are already available to the public and related to the trust service to be discontinued; in particular, it shall ensure access to its registers referred to in section 84 (3).

(3) If a trust service provider discontinues all of its trust services, the notification under paragraph (1) shall specify a trust service provider (hereinafter "substitute trust service provider") that is to ensure access to the registers referred to in paragraph (2) even following the discontinuation of such trust services.

(4) If a qualified trust service is to be discontinued, only a trust service provider registered with the trust service supervisory body as a qualified trust service provider providing identical trust services may act as substitute trust service provider.

(5) Once a notification under paragraph (1) is given, the trust service provider concerned may not issue any new certificate through the trust service concerned, and it shall revoke all certificates issued and not yet revoked at least twenty days before it discontinues its relevant activity.

(6) A trust service provider shall hand over to its substitute trust service provider all registered data to which access is to be ensured, as well as all data relating to its revoked certificates (including relevant personal data).

Section 89 (1) If a trust service provider fails to perform an obligation provided for under section 88 (2) or (3), the trust service supervisory body shall order all certificates issued by the trust service provider concerned to be revoked, it shall have the revocation published, and it shall designate a substitute trust service provider. All costs incurred by the trust service supervisory body in this context shall be reimbursed by the trust service provider discontinuing

its trust service within 15 days after receipt of a corresponding notice from the trust service supervisory body. If a trust service provider discontinuing its trust services fails to reimburse such costs within the above time limit, the trust service supervisory body may use the financial collateral provided by law for such purposes by the trust service provider concerned to recover its expenditures.

(2) Where a qualified trust service is concerned, the trust service supervisory body shall designate primarily a qualified trust service provider as a substitute trust service provider.

(3) If no suitable trust service provider is registered with the trust service supervisory body at the time a trust service is discontinued, the trust service supervisory body itself shall perform the tasks of a substitute trust service provider.

(4) If a liquidation, winding-up, or compulsory strike-off proceeding is instituted against a trust service provider, the trust service provider concerned shall notify without delay the trust service supervisory body about the proceeding and the identity of the liquidator or administrator. During the period of the proceeding, the trust service supervisory body may request information from the liquidator, administrator, or the company registration court conducting the compulsory strike-off proceeding about the progress of the liquidation, winding-up, or compulsory strike-off proceeding. If the trust service provider concerned fails to perform its obligations provided for under section 88 (1) and (2) before submitting its closing balance sheet, the trust service supervisory body shall designate a substitute trust service provider.

(5) If a trust service is discontinued, the trust service supervisory body shall deregister the trust service concerned; if a trust service provider is terminated, the supervisory body shall deregister all registered trust services provided by the trust service provider concerned.

CHAPTER XVIII

THE OBLIGATION OF TRUST SERVICE PROVIDERS TO PROVIDE DATA

Section 90 (1) With regard to data confirming the identity of the person concerned or data verified pursuant to section 82 and for the purposes of a criminal proceeding conducted with regard to a criminal offence committed by abusing a trust service provided by a trust service provider or in the interest of national security, the trust service provider concerned shall provide investigating authorities, the prosecution service, the court, and national security services with data free of charge, provided that the conditions laid down in a separate Act concerning data requests are met. The data transfer shall be recorded, and the trust service provider may not inform the relying party about the data transfer.

(2) A trust service provider shall perform its obligations provided for under paragraph (1) without delay, and it may not apply any further condition regarding the data transfer; in particular, such data transfer may not be conditional on reaching any agreement on the costs of the transfer, or on advancing any such cost.

(3) In the course of a civil action or a non-contentious proceeding concerning the validity of a certificate, data confirming the identity of the signatory or the person who placed the seal, provided that his involvement is certified, as well as data verified pursuant to section 82 may be disclosed by the trust service provider to the party with opposing interests or his representative, or the requesting court.

(4) If a relying party is indicated in a certificate under a pseudonym, data concerning the real identity of the relying party indicated in the certificate may be disclosed by the trust service provider only with the consent of the relying party concerned, the trust service client, or another person represented by the relying party indicated in the certificate, or otherwise in a situation specified in paragraphs (1) to (3).

CHAPTER XIX

SUPERVISION OF TRUST SERVICES, AND PUBLICATION OF A TRUSTED LIST

54. Designation, tasks, and competence of a trust service supervisory body

Section 91 (1) The body supervising trust services pursuant to Article 17(1) eIDAS shall be the National Media and Infocommunications Authority.

(2) The trust service supervisory body shall be responsible for publishing a trusted list specified in Article 22 eIDAS.

Section 92 (1) In addition to the tasks provided for under eIDAS, the trust service supervisory body shall

a) keep the registers specified in this Act and its implementing decrees, and keep such registers continuously available to anyone,

b) monitor the development of technologies and cryptographic algorithms concerning trust services, and identify in its decisions the secure cryptographic algorithms trust service providers may use for their services, including requirements concerning the use of such algorithms with defined parameters,

c) with regard to trust services, carry out the tasks of service supervisory body within the meaning of the Act on the general rules on taking up and pursuit of service activities.

(2) For the purposes of paragraph (1) *b)*, a cryptographic algorithm shall be considered secure if it is not possible, using certain parameters, to deduct the data used to generate a signature or seal from the validation data of the given electronic signature or seal, and it also meets the conditions laid down in an implementing decree to this Act with regard to hash strings.

Section 93 (1) The trust service supervisory body may not conduct its proceedings as summary proceedings; it may invite a client more than one time to remedy any deficiency, and it may not communicate its decisions orally.

(2) The authority shall observe an administrative time limit of two months, unless provided otherwise by eIDAS or a directly applicable Union implementing act thereof.

(3) The Office of the National Media and Infocommunications Authority shall proceed as trust service supervisory body at first instance; appeals against its decisions may be submitted to the President of the National Media and Infocommunications Authority.

(4) An administrative service fee, as specified in an implementing decree to this Act, shall be paid for the registration-related activities of the trust service supervisory body, and such fees shall form part of the revenue of the trust service supervisory body.

(5) For the purpose of producing assessments, analyses, and evaluations as necessary to carry out the tasks falling within the competence of the trust service supervisory body, the trust service supervisory body may oblige trust service providers pursuing activities covered by this Act to provide data within a set time limit. Trust service providers shall provide such true and complete data within the time limit set, and in the form required, by the trust service supervisory body. If a service provider fails to meet its obligation to provide data, the trust service supervisory body may impose a fine pursuant to section 95 (3) *e)*.

(6) The trust service supervisory body shall inform each trust service provider providing data about the processing and use of data specified by the trust service supervisory body, as well as the statutory purpose of data processing, at the time of imposing a data provision obligation or issuing a notice requesting optional data provision. If data provision is ordered by way of a binding decision under paragraph (5), the trust service supervisory body shall inform each data provider concerned about the legal consequences of any failure to provide complete and true data within the set time limit and in the appropriate form; otherwise, the notice shall indicate that providing data is optional.

(7) to (8)

(9) The trust service supervisory body shall check, as part of administrative audits conducted during the period of providing any trust service, whether the persons serving as qualified trust service provider natural persons or as executive officers, managers, or employees of legal persons or organisations without a legal personality operating as qualified trust service providers have a criminal record or are subject to disqualification form a profession excluding them from providing trust services. For the purposes of conducting administrative audits, the trust service supervisory body may request data from the criminal records system. Such data requests shall be limited to data indicating whether a person serving as a qualified trust service provider natural person or as an executive officer, manager, or employee of a legal person or organisation without a legal personality operating as a qualified trust service provider has a criminal record or is subject to disqualification form a profession excluding him from providing trust services.

(10) Personal data obtained under paragraph (9) shall be processed by the trust service supervisory body until the trust service concerned is discontinued or, where the trust service provider is a legal person or an organisation without a legal personality, the legal relationship between the organisation and its executive officer, manager, or employee concerned is terminated.

(11) A client may not request the trust service supervisory body to conduct an administrative audit. In the course of conducting an administrative audit *ex officio*, the trust service supervisory body shall proceed pursuant to section 95.

55. Registers concerning trust services

Section 94 (1) In addition to the provisions of eIDAS, the trust service supervisory body shall also keep a register of

a) notified trust service providers and trust services provided by them,

b) notified qualified electronic signature and qualified electronic seal creation devices,

c) designated organisations certifying the suitability of devices referred to in point *b)*,

d) substitute trust service providers within the meaning of sections 88 and 89, and

e) qualified archive services referred to in section 84 (2) that are used by trust service providers to perform their retention obligations.

(2) The name, address, seat, and registration number of a trust service provider, the description of its service, the place and commencement date of service provision, and the relevant trust service policy, service policy, service extract, and general terms and conditions may be published in a register referred to in paragraph (1) as public data or documents. A register published by trust service the supervisory body shall be considered a publicly certified register.

56. Audits conducted at trust service providers, and measures available to the trust service supervisory body

Section 95 (1) Within thirty days after taking up a service, the trust service supervisory body shall carry out a supervisory audit at any trust service provider that notified a qualified trust service to verify compliance with applicable trust service requirements.

(2) At least once per year, the trust service supervisory body shall carry out a comprehensive on-site audit at trust service providers that provide qualified trust services.

(3) With a view to ensuring compliance with applicable requirements and eliminating violations and shortfalls in light of facts and pieces of evidence discovered during an audit, the trust service supervisory body may take the following measures:

a) instructing a trust service provider to comply with applicable trust service requirements,

b) prohibiting the use of certain technologies and procedures,

c) suspending, as a provisional measure, the provision of a service aimed at issuing new certificates, and publishing the suspension in its register,

d) ordering the revocation of any qualified certificate issued earlier,

e) imposing a fine,

f) deleting the fact, with regard to a trust service provided by a trust service provider, that a given trust service is a qualified trust service,

g) removing a trust service provider from the register of trust service providers.

(4) Regarding a qualified trust service, the trust service supervisory body may, in addition to the situations specified in paragraph (3), take any measure specified in paragraph (3) also in order to prevent any violation or shortfall concerning any applicable requirement.

(5) When passing a decision on a measure specified in paragraph (3), the trust service supervisory body shall take into account the gravity and frequency of violation, the extent of damages that were or could be caused, if the entity subject to the measure is a qualified trust service provider, and whether any measure has already been taken against the trust service provider concerned. Such measures may also be applied in any combination.

(6) The trust service supervisory body shall deregister a trust service provider, if compliance with the applicable trust service requirements cannot be ensured by any other means. Deregistration may be applied only if other measures fail to be effective.

(7) If a measure specified in paragraph (3) *f)* or *g)* is applied against a trust service provider that issues qualified certificates, the trust service supervisory body shall, at the same time, also prohibit the trust service provider concerned from referring to its certificates as qualified certificates, and it shall also make arrangements to have any qualified certificate already issued revoked.

(8) The trust service supervisory body may order a qualified certificate to be revoked if it seems likely that the qualified certificate concerned includes any incorrect data, has been falsified, or that the device used by the trust service provider concerned to sign or seal its qualified certificates is unsecure.

(9) If the trust service supervisory body prohibits the provision of a trust service, the trust service provider concerned shall be obliged to proceed pursuant to section 88; if the trust service provider concerned fails to fulfil this obligation, the supervisory body shall proceed pursuant to section 89.

57. The amount of fines imposed by the trust service supervisory body

Section 96 (1) The trust service supervisory body may impose a fine on a trust service provider that fails to meet the applicable trust service requirements.

(2) If a violation is repeated or a trust service provider fails to comply with a decision by the trust service supervisory body, the supervisory body may also impose a fine on the executive officer of the trust service provider concerned, in addition to any fine imposed on the trust service provider.

(3) The trust service supervisory body may not impose a fine if more than two years passed after the trust service supervisory body became aware of the violation, or if more than three years passed after such violation was committed. If a given omission or breach of obligation constitutes a criminal offence, the trust service supervisory fine may be imposed within one year after the perpetration of the criminal offence is established with final and binding effect.

(4) When determining the amount of a fine, the trust service supervisory body shall take into account

a) the extent of risks or damages caused by the violation or omission,

b) the willingness of responsible persons to cooperate with the trust service supervisory body (in particular, granting access to documents and registers, and presenting the technologies used and their technical characteristics),

c) any actual or attempted concealment of any data, fact, or information that serves as grounds for a measure,

d) the repetition or frequency of violations, if any.

(5) The amount of the fine shall range from HUF 200 000 to HUF 20 000 000 if

a) a violation is related to a qualified trust service of a trust service provider,

b) a trust service provider claims to be a qualified trust service provider in a certificate issued by it, or implies such a status directly or indirectly in any other way, without being eligible to do so,

c) any data or document that is related to the issuance of a certificate is not retained for a period required by law or a service contract, and the safekeeping of such data or documents is not ensured by any other way.

(6) In a situation not mentioned in paragraph (5), the amount of the fine shall range from HUF 50 000 to HUF 10 000 000.

(7) The amount of the fine imposed on an executive officer shall range from HUF 50 000 to HUF 2 000 000.

CHAPTER XX

SPECIAL PROVISIONS ON CERTAIN TRUST SERVICES

58. Special provisions on trust services relating to electronic signatures and seals

Section 97 (1) If an electronic document is signed or sealed with a qualified electronic signature or seal, or a timestamp, the content of the document shall be presumed not to have changed since it was signed or sealed or the timestamp was applied, unless the verification of the signature, seal, or timestamp indicates otherwise.

(2) The certificate subject may use any data used to generate an electronic signature or seal for the sole purpose of generating electronic signatures and seals; other restrictions indicated in the certificate shall also be observed, if any.

(3) A qualified electronic signature or seal certificate may also be used to generate advanced electronic signatures and seals.

(4) If any data used to generate electronic signatures or seals is lost or obtained by an unauthorised person, the trust service client concerned shall notify the trust service provider without delay.

(5) If a trust service provider learns that any data used to generate electronic signatures or seals has been lost or obtained by an unauthorised person, it shall revoke the certificate concerned and publish the fact of revocation in its register without delay.

(6) If a trust service provider learns that any data used to generate electronic signatures or seals has likely been lost, or such data may have been, or there is a risk that such data could be, obtained by an unauthorised person, it shall suspend the certificate concerned and publish the fact of suspension in its register without delay, provided that the trust service provider concerned makes it possible to suspend a certificate.

Section 98 A fine under section 96 (5) may also be imposed if a trust service provider that provides a trust service regarding electronic signatures or seals fails to take measures as necessary to protect its own data used to generate electronic signatures or seals.

Section 99 (1) In the context of legal relationships regulated by family law or the law of succession, electronic signatures or seals may not be used and electronic documents bearing an electronic signature or seal may not be generated in an exclusive manner and without relying on documents in non-electronic formats.

(2) Unless provided otherwise explicitly, any reference in a law to electronic signatures or documents signed by electronic means shall be construed as referring to electronic seals or documents sealed by electronic means as well.

59. Special provisions on archive services

Section 100 If an electronic document bearing an electronic signature or seal is archived by a qualified trust service provider, it shall be presumed until proven otherwise that the electronic signature, seal, or timestamp on the electronic document, and any related certificate, was valid when the signature, stamp, or timestamp was applied.

PART FIVE

CERTAIN RESIDUAL RULES CONCERNING ELECTRONIC ADMINISTRATION

Section 101 (1) Unless provided otherwise by an Act or government decree in derogation from sections 101 to 103, the provisions laid down in this Part shall apply to electronic communication

a) between two organs referred to in section 1 (17) *a)* to *i)*, and

b) between an organ referred to in section 1 (17) *a)* to *i)* and a natural person or economic operator.

(2) The provisions laid down in sections 14 to 15 shall apply as appropriate to the electronic delivery of documents and juridical acts.

(3) If electronic delivery fails for any reason and the statutory conditions of fictitious service are not met, an authentic paper-based copy of the electronic document concerned shall be delivered to the addressee.

Section 102 (1) An authentic paper-based copy of an authentic electronic document may be produced by the issuer of the document concerned, or its legal successor, by attaching a clause to a printed copy of the document. In the context of administrative organs, an organ shall be considered a legal successor if issuing the document concerned would be the task of the organ concerned under the legislation in force.

(2) If a natural person issued or signed an electronic document by electronic means, he may attach a clause under his own name to a paper-based copy of the document.

(3) On behalf of an entity other than a natural person issuing an electronic document, the person

a) specified in the organisational and operational regulations,

b) specified in the instrument of incorporation,

c) authorised to represent the legal person concerned

may attach a clause to a paper-based copy of the document.

(4) A clause shall contain a signature from the person authorised to attach a clause, the date of attaching the clause, and a text referring to the fact that the paper-based copy is identical to the underlying electronically authenticated document.

(5) Where a natural person is concerned, the clause shall contain, in addition to the requirements under paragraph (4), signatures from two witnesses, and a text referring to the fact that the clause was signed by the natural person concerned in front of the witnesses, or he acknowledged that the signature on the clause is written in his own hand.

(6) A paper-based copy of a juridical act consisting of more than one pages shall be considered authentic if a clause was attached to it by all signatories or their legal successors pursuant to this section.

(7) The probative value of a paper-based copy produced pursuant to this section shall be the same as that of the underlying electronic document.

Section 103 (1) The issuer of a paper-based document, or his legal successor, may produce an electronically authenticated document of the paper-based document concerned by digitising the document and attaching a clause to it.

(2) In the course of converting a paper-based document into an electronically authenticated document, the signatory may be a person referred to in section 102 (2) or (3).

(3) A clause shall contain an at least advanced electronic signature from the person authorised to attach a clause, and a text referring to the fact that the electronic copy is identical to the underlying paper-based document.

(4) An electronic copy of a juridical act of more than one pages shall be considered authentic if the clause attached to the scanned document includes at least advanced electronic signatures of all signatories or their legal successors.

(5) If a juridical act of more than one pages is signed by at least one signatory by electronic means, the copy reflecting the concurrence of wills in an authentic manner shall be

a) the electronic copy that bears the at least advanced electronic signatures of all signatories, as well as paper-based copies of that document if produced pursuant to section 102, or

b) the paper-based copy of the electronic document that bears the at least advanced electronic signature of all signatories who signed the document by electronic means, as well as

ba) a clause under section 102, and

bb) the signature of all signatories who signed the document by non-electronic means

simultaneously.

(6) The probative value of an electronic copy produced pursuant to this section shall be the same as that of the underlying paper-based document.

Section 104

Section 104/A (1) The central service provider designated in the government decree on centralised computer and electronic communications services, and the government communications service provider designated in the government decree on government networks (hereinafter jointly “central service providers”) shall provide organs performing a public duty not under the direction or supervision of the Government with

a) the development and operation of an information technology system specified in a decree passed by the minister responsible for electronic administration, or support for such activities,

b) centralised computer and communications services specified in the government decree on centralised computer and electronic communications services,

c) the use of government networks specified in the government decree on government networks, as well as government communications activities, and government communications services

as public service, provided that the head of such an organ performing a public duty not under the direction or supervision of the Government applies for the use of such services to the minister responsible for electronic administration.

(2) Financing for the use of services referred to in paragraph (1) and for the provision of public services by the central service provider shall be provided for, depending on the outcome of negotiations between the minister responsible for electronic administration and the head of the respective organ performing a public duty not under the direction or supervision of the Government,

a) in the budget of the ministry headed by the minister responsible for electronic administration, directly or by way of a transfer from the budget of the respective organ performing a public duty not under the direction or supervision of the Government, or

b) by the respective organ performing a public duty not under the direction or supervision of the Government if it enters into a contract with the central service provider directly.

PART SIX

FINAL PROVISIONS

60. Authorising provisions

Section 105 (1) Authorisation shall be given to the Government to determine in a decree

a) the detailed rules of electronic administration and electronic communication,

b) the conditions for the use of electronic administration services and central electronic administration services by non-electronic administration organs, the tasks and procedures of the Supervisory Authority concerning such use, and the method of determining the fee that may be imposed for using such services,

c) the detailed requirements of regulated electronic administration services and central electronic administration services, the detailed procedural rules of providing such services, the detailed rules of using such services, the organisational, personnel-related and financial conditions for service providers for providing regulated electronic administration services, the provisions relating to the notification of regulated electronic administration services and to the imposition of fines by the Supervisory Authority, including the amount of such fines,

d) the detailed requirements concerning the identification of electronic administration organs,

e) the detailed rules concerning the methods of electronic communication,

f) the detailed rules of applying and registering administrative settings,

g) the special requirements concerning electronic signatures used for electronic administration, certificates relating to electronic signatures, and services relating to electronic signatures provided in connection with such purposes,

h) the detailed rules of registering electronic administration service providers,

i) the detailed rules of operating the data link register and providing data from the data link register,

j) the detailed rules on electronic payments and settlements,

k) the detailed rules of procedures of the Supervisory Authority,

l) the range of legal entities referred to in section 14 (7),

m) the detailed rules of operating a national call centre,

n) the detailed rules on producing electronic copies of paper-based documents, and converting electronic documents into authentic paper-based documents,

o) the order and frequency of backing up data concerning matters administered by electronic administration organs, as well as the organ responsible for safekeeping such data,

p) the requirements concerning the content of the register kept by the trust service supervisory body, and the requirements concerning notifications relating to the provision of trust services,

q) the method of determining the fee that may be imposed for the use of electronic administration services and central electronic administration services on by legal entities referred to in section 1 (17) *j)* and *l)*,

r) the rules of cooperation between mandatory central storage users and the storage provider, and the rules of using the central storage space,

s) the detailed rules of connecting to and operating the Single Digital Gateway,

t) in the context of trust services, the other identification methods recognised at national level which provide equivalent assurance in terms of reliability to physical presence.

(2) Authorisation shall be given to the Government to designate in a decree

a) the Supervisory Authority,

b) the organ keeping the register of foreign nationals relying upon electronic administration,

c) the providers of regulated electronic administration services mandatorily provided by the Government, and the providers of central electronic administration services,

d) the organ keeping the Central Client Registration Records, and the registration organs of electronic identification services mandatorily provided by the Government and the client settings registers,

e) the organ operating the national call centre,

f) the storage provider,

g) the organ under section 35 (15a),

h) the operator of the electronic administration point.

(3) Authorisation shall be given to the Government to determine in a decree

a) the rules concerning the availability of IT cooperation services, and the certification of such availability,

b) the rules concerning the publication interface to be used by cooperating organs to perform their publication obligations,

c) the detailed rules of procedure to be followed in case of any outage or malfunction that restricts or hinders IT cooperation,

d) the detailed rules on adopting and publishing technical guidelines,

e) the cooperating organs that are obliged to use automatic information transfer, the scope of information to be transmitted in such a manner, and the requirements concerning automatic information transfer interfaces,

f) the detailed requirements concerning the content of information transfer policies, and the scope of information to be regulated under information transfer policies,

g) the rules concerning the notification of information transfer policies and agreements,

h) the detailed rules concerning the data content and keeping of the register of sources of information,

i) the detailed rules concerning the data content and keeping of the list of data and document designations,

j) the rules on keeping and operating the central address register and generating addresses in a consistent manner, and the detailed procedural rules of managing addresses in a consistent manner,

k) the rules concerning central electronic administration services specified in this Act, and the scope of mandatory central electronic administration services,

l)

m) the detailed rules of supervisory reviews, and

n) the detailed rules of coordination proceedings.

(4) Authorisation shall be given to the Government to determine in a decree the types and range of

a) contact addresses used for electronic communication,

b) information available from primary sources of information

that are not specified in this Act.

(5) Authorisation shall be given to the Government to designate in a decree

a) the organ responsible for operating the central address register,

b) the organs performing a public duty that are designated for cooperation pursuant to Part Three, and

c)

(5a) Authorisation shall be given to the Government to determine in a decree

a) electronic administration organs with no-fault inability,

b) matters falling within the functions and powers of an organ referred to in point *a)* with regard to which no-fault inability does not apply, and

c) the period of no-fault inability.

(6) Authorisation shall be given to the minister responsible for electronic administration to determine in a decree, in agreement with the minister responsible for taxation policy, the administrative service fee payable for the notification of regulated electronic administration services and for the notification of changes to regulated electronic administration services, and the rules concerning the payment, management, and registration of such fees.

Section 106 Authorisation shall be given to the minister responsible for electronic administration to determine in a decree

a) the detailed requirements concerning trust services, including, in particular, requirements concerning the financial and personnel-related suitability and activities of, and devices used by, trust service providers, requirements on contracting with relying parties and providing information in relation to contracting, and detailed conditions for service contracts and other conditions for providing trust services (such as trust service policies and service policies),

b)

*c)*in agreement with the minister responsible for taxation policy, the administrative service fee payable to the trust service supervisory body, as well as the detailed rules concerning the payment, management, registration, and reimbursement of any such fee,

d) the computer systems developed or operated by the central service provider under section 104/A (1) *a)*, and rules on the use of centralised computer and communications services by organs performing a public duty not under the direction or supervision of the Government and on the use of government networks and network services.

61. Provisions on entry into force

Section 107 (1) With the exceptions specified in paragraphs (2) to (4), this Act shall enter into force on 1 January 2016.

(2) Section 114 (1), 114 (4) to (9), and 114 (10) *a)* to *d)* shall enter into force on 2 January 2016.

(3) Part Four and sections 104, 105 (1) *g)*, 105 (3) *l)*, 105 (5) *c)*, 106, 113 (1) to (6), 118, 121 (1) *a)*, and 121 (2) and (3) shall enter into force on 1 July 2016.

(4) Parts Two and Three and sections 105 (1) *a)* to *f)*, *h)*, and *j)* to *l)*, 105 (2) *a)* to *d)*, 105 (3) *a)* to *k)*, *m)*, and *n)*, 105 (4), 105 (5) *a)* and *b)*, 105 (6), 108 (1) to (6), 109, 113 (7), and 121 (1) *b)* shall enter into force on 1 January 2017.

62. Transitional provisions

Section 108 (1) The entities referred to in section 1 (17) *a)* to *k)* shall be obliged to ensure the administration of matters by electronic means pursuant to this Act as of 1 January 2018.

(2)

(2a)

(2b)

(2c)

(3)

(4)

(4a)

(5) Unless provided otherwise by an Act, a client or legal representative shall perform his obligation under section 9 (1) as of 1 January 2018.

(6)

(6a) Until 31 December 2018 and for the purpose of communicating with an electronic administration organ by electronic means in tax matters, an economic operator client may also use the storage space specified in section 35 (3) of the natural person acting on behalf of the economic operator concerned [for the purposes of paragraphs (6a) and (6b) hereinafter "natural person"], while also identifying such natural person, instead of using the official contact address of the economic operator.

(6b) Until the time limit specified in paragraph (6a) and unless instructed otherwise by its client or his representative, an electronic administration organ proceeding in a matter under paragraph (6a) may, instead of using the official contact address of the economic operator client, send its items addressed to an economic operator client to the storage space specified in section 35 (3) of the natural person acting on behalf of the economic operator client, provided that such storage space is known to the proceeding electronic administration organ. An economic operator client shall be considered to have issued a different instruction if it used its official contact address for the purpose of communicating with the electronic administration organ concerned in a given matter.

(6c) If delivery is made at a storage space referred to in paragraph (6b), the rules on delivery laid down in section 14 (4) shall apply.

(6d) Until 31 December 2022, a natural person or private entrepreneur may not record any instruction under section 22 (1) *e)* in his client settings register regarding tax matters falling within the competence of the national tax and customs authority.

(7) After this Act enters into force, an electronic administration organ may only deploy new computer systems for the purpose of electronic administration that are suitable for the purpose of electronic administration as required under this Act.

(8)

(9)

(10)

(11)

(12)

(13)

(14)

(15)

(16)

Section 108/A Until 31 December 2019, if the size of a statement or annex (for the purposes of this section hereinafter jointly "statement") a client seeking to submit by electronic means exceeds the size limit set by the electronic administration organ concerned, communication shall be considered conducted by electronic means, even if the client concerned uses a durable data-storage medium to submit his statement, provided that the statement complies with the provisions laid down in section 17 (1) *b)*.

(2) If a statement is submitted on a durable data-storage medium and unless provided otherwise by law, the client shall notify the electronic administration organ, by way of electronic communication conducted by means other than that under paragraph (1), about the submission of his statement on a durable data-storage medium. Unless provided otherwise by law, the client shall submit the durable data-storage medium in person or by post within 3 working days after receipt of a confirmation of his notification.

(3) Unless provided otherwise by law and in a situation described in paragraph (1), a statement shall be deemed as submitted at the time a notification is received from the client concerned pursuant to paragraph (2) and, for the purpose of calculating the applicable administrative time limit, the statement shall be deemed as received at the time of receipt of the data-storage medium under paragraph (1).

(4) Unless provided otherwise by law and if a size limit referred to in paragraph (1) is exceeded, the electronic administration organ may transmit the statement concerned using a durable data-storage medium by applying the provisions laid down in paragraphs (1) to (3) appropriately.

Section 108/B (1) Until 31 December 2019, it shall constitute an exemption to the rule of electronic communication if a document, deed, or other paper-based submission (for the purpose of this section hereinafter "submission") needs to be presented or inspected in a paper-based form because the digitisation of the original paper-based submission would cause disproportionate difficulties due to its significant volume or unusual shape.

Section 109 (1) Cooperating organs shall be obliged to engage in IT cooperation as provided for under this Act as of 1 January 2018.

(2)

(3)

Section 110 (1) Service providers who provide electronic signature-related services within the meaning of Act XXXV of 2001 on electronic signatures (hereinafter "Eat."), and were already registered with the National Media and Infocommunications Authority on 30 June 2016 as registered service providers shall discontinue their electronic signature-related services within the meaning of the Eat. on 1 July 2017 at the latest, unless they notify their trust services within the meaning of this Act; the provisions laid down in sections 16 and 16/N of the Eat. shall apply to the performance of this obligation, with the proviso that, with regard to their obligations relating to such discontinuation, the trust service supervisory body shall proceed in line with sections 89, 95, and 96 as of 2 July 2017.

(2) Service providers who provide electronic signature-related services within the meaning of the Eat. and were already registered with the National Media and Infocommunications Authority on 30 June 2016 as qualified service providers concerning any of their electronic signature-related services, other than qualified certificates issued to natural persons, (such services hereinafter jointly "Eat. qualified service") may provide such Eat. qualified services until their Eat. qualified services are included on the trusted list referred to in Article 22 eIDAS or until 30 June 2017 at the latest.

(3) During the transitional period under paragraph (2), Eat. qualified services and certificates issued through such services, as well as electronic signatures and timestamps based on such certificates shall continue to have the same statutory legal effects as they had on 30 June 2016 in Hungary, provided that they continue to meet the requirements provided for under the Eat. as of 30 June 2016 during the transitional period.

(4) During the transitional period, administrative supervision of Eat. qualified services shall be carried out by the National Media and Infocommunications Authority within its competence concerning trust services pursuant to the rules applicable to trust services.

(5) During the transitional period, an Eat. qualified service under paragraph (2) shall be considered only a qualified trust service recognised at national level, as provided for under eIDAS; in other respects, such a service shall not have the legal effects of a qualified trust service within the meaning of eIDAS.

(6) With the exception of Part Four, statutory references to qualified trust services within the meaning of Part Four shall also cover Eat. qualified services during the transitional period specified in paragraph (2).

(7) With the exception of Part Four, statutory references to qualified electronic seals shall be considered equivalent to qualified organisational electronic signatures within the meaning of the Eat. during the transitional period specified in paragraph (2).

Section 110/A

Section 110/B

63. Compliance with the law of the European Union

Section 111 This Act contains provisions for the implementation of Chapter III of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

Section 111/A This Act contains provisions for the implementation of Regulation (EC) No 223/2009 of the European Parliament and of the Council of 11 March 2009 on European statistics and repealing Regulation (EC, Euratom) No 1101/2008 of the European Parliament and of the Council on the transmission of data subject to statistical confidentiality to the Statistical Office of the European Communities, Council Regulation (EC) No 322/97 on Community Statistics, and Council Decision 89/382/EEC, Euratom establishing a Committee on the Statistical Programmes of the European Communities.

Section 111/B This Act contains provisions for the implementation of Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012.

Section 112 (1) This Act serves the purpose of compliance with Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market.

(2) The draft of this Act was notified in advance pursuant to Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market.

64. Amending and repealing provisions

Section 113 (1) to (6)

(7)

(8)

Section 114 (1)

(2) to (3)

(4) to (9)

(10)

a) to *d)*

e)

Sections 115 to 117

Section 118

Sections 119 to 120

Section 121 (1) The following shall be repealed:

a)

b)

(2) to (3)