



Published in Official Gazette no./
Official Gazette publication date/
Constitutional Court no./

LAW ON ELECTRONIC DOCUMENTS, ELECTRONIC IDENTIFICATION AND TRUST SERVICES (*)

(“Official Gazette of the Republic of North Macedonia” No. 101/19 and 275/19)

(*) With this law, the harmonization with 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, with CELEX no. 32014R0910 is made.

I. GENERAL PROVISIONS

Article 1

1) This law shall regulate and prescribe the creation, preservation and processing of electronic documents, electronic identification and trust services.

2) This law shall also determine the manner of use of electronic documents, electronic signatures, electronic seals and electronic trust services in administrative and court proceedings.

3) The subject of regulation of this law shall be the conditions under which the electronic identification devices issued to natural and legal persons falling under registered or recognized electronic identification scheme are recognized.

Purpose

Article 2

1) The purpose of this law is to ensure the security of electronic identification funds and security when providing trust services.

2) The purpose of this law is to regulate legal regime of electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic services recommended delivery, website authentication services, as well as, preservation of the electronic signature or seal and their validation.

Definitions

Article 3

(1) The terms used in this law shall have the following meaning:

1) **data in electronic form** is data created in electronic form, suitable for electronic processing and transmission through electronic communication systems;

- 2) **electronic transaction** is an activity between two or more parties, which is conducted by electronic means;
- 3) **electronic document** is any document stored in electronic form, in particular text or sound, visual or audio-visual recording;
- 4) **product** is hardware, software or relevant components of hardware or software intended to be used for the provision of trust services;
- 5) **interoperability** is the ability of two or more systems, or of the components thereof, to exchange data and enable joint use of data and knowledge;
- 6) **public body** is a state body, a body of state administration, a unit of the local self-government, public enterprises, institutions, organizations and legal entities to which delegated public powers belong in accordance with the legislation of the Republic of the North Macedonia;
- 7) **authentication** is an electronic process that enables the electronic identification of a natural or legal person, or that enables confirmation of origin and integrity of data in electronic form;
- 8) **person identification data** is a set of data pursuant to which it is only possible to identify the identity of a legal entity, natural person or authorised person of a legal entity;
- 9) **electronic identification** is the process of using personal identification data in electronic form uniquely representing either the natural person or legal entity or authorised person of a legal entity;
- 10) **electronic identification devices** are tangible or intangible tools containing personal identification data and are used for authentication in electronic services;
- 11) **issuer of electronic identification devices** is a legal entity that fulfils the conditions set out in this law for issuers of a device of electronic identification;
- 12) **electronic identification scheme** is an electronic identification system according to which electronic identification devices are issued to natural or legal persons or an authorised person of a legal entity;
- 13) **trust service** is an electronic service in electronic transactions, which is consisted of:
- creation, validation and verification of electronic signatures, electronic seals or electronic time stamps, electronic services recommended delivery, and certificates related to these services or
 - creation, validation and verification of websites authentication certificates or
 - preservation of electronic signatures, seals or certificates related to these services.

Trust services may be non-qualified and qualified.

- 14) **trust service provider** is a natural or legal persons who provides one or more trust services;
- 15) **relying party** is a natural or legal persons that has a legal interest in an electronic identification or a trust service;
- 16) **qualified trust service** is a trust service that meets the applicable requirements laid down in this Law that refer to qualified trust service;
- 17) **qualified trust service provider** is a trusted service provider who provides one or more qualified trusted services and whose status of a provider of qualified trust service is assigned by the Minister of Information society and Administration by registration in the Register of Electronic Schemes identification of trusted services;
- 18) **electronic signature** is a set of data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign;
- 19) **electronic seal** is data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the origin and integrity of the attached or logically associated data;
- 20) **electronic signature creation data** is unique data which is used by the signatory to create an electronic signature;
- 21) **validation data** is the data used for electronic validation signature or electronic seal;
- 22) **certificate for electronic signature** is an electronic attestation which links electronic signature validation data to a natural person which confirms at least the name or the pseudonym of that person;
- 23) **certificate for electronic seal** is an electronic attestation that links electronic seal validation data to a legal entity and confirms the name of that legal entity;
- 24) **signatory** is a natural person who creates an electronic signature;
- 25) **creator of a seal** is a person representing the legal entity, who creates an electronic seal;
- 26) **electronic signature and/or seal creation device** is a technical device, or configured software or hardware, used to create an electronic signature or electronic seal;
- 27) **validation** is the process of verifying and confirming that an electronic signature or a seal is valid;
- 28) **advanced electronic signature** is an electronic signature which meets the requirements laid down in this Law that refer to an advanced electronic signature;
- 29) **qualified electronic signature** is an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified electronic signature certificate;
- 30) **qualified electronic signature and/or seal creation devices** are devices that meet the conditions set out in this Law, and which refer to funds for creating a qualified electronic signature or seal;
- 31) **qualified certificate for electronic signature** is a certificate for electronic signature, which is issued by a qualified trust service provider and meets the conditions set out in this Law that refer to a qualified certificate for electronic signature;
- 32) **advanced electronic seal** is an electronic seal, which meets the conditions set out in this Law that refer to an advanced electronic seal;
- 33) **qualified electronic seal** is an advanced electronic seal, which is created by a qualified electronic seal creation device, and that is based on a qualified certificate for electronic seal;
- 34) **electronic seal creation data** is unique data, which is used by the creator of the electronic seal to create an electronic seal;

35) **qualified certificate for electronic seal** is a certificate for an electronic seal that is issued by a qualified trust service provider and meets the conditions set out in this Law that refer to a qualified certificate for electronic seal;

36) **certificate for website authentication** is an attestation that makes it possible to authenticate a website and links the website to the natural or legal entity to whom the certificate for website authentication is issued;

37) **qualified certificate for website authentication** is a certificate for website authentication, which is issued by a qualified trust service provider and meets the conditions set out in this Law that refers to a qualified certificate for website authentication;

38) **electronic time stamp** is a set of data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that particular moment;

39) **qualified electronic time stamp** is an electronic time stamp which meets the conditions set out in this Law that refer to a qualified electronic time stamp;

40) **electronic registered delivery service** is a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and thereby protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations;

41) **qualified electronic registered delivery service** is an electronic registered delivery service which meets the conditions set out in this Law that refer to a qualified electronic registered delivery service;

42) **conversion** is a change to the form or format of the document from one form or format to another form or format, so that the content of the document remains unchanged;

43) **digitalization** is the conversion of a document from a form that is not electronic into an electronic form;

44) **digitalized document** is an electronic document created by means of digitalization of the original document in written form;

45) **electronic preservation of documents** is preservation of documents in electronic form, for which the exact time of preservation of documents is specified, corresponding to the time of preservation of the documents in paper form, for which the time of preservation is confirmed with an electronic time stamp;

46) **qualified electronic preservation of documents** is preservation of electronic documents, which in their preservation are confirmed with a qualified electronic signature and/or seal and a qualified time stamp;

47) **trust mark for trust services** is a sign which is clearly recognizable and which clearly indicates that the trust service is provided by a specific trust service provider;

48) **trust mark for qualified trust services** is a sign which is clearly recognizable and which clearly indicates that the qualified trust service is provided by a specific qualified trust service provider;

49) **conformity assessment body** is a legal entity accredited to carry out conformity assessment of a qualified trust service provider and the qualified trust services it provides;

50) **certification laboratory** is a legal entity accredited to carry out conformity assessment of electronic identification, electronic signatures or electronic seals determined by this law.

(2) Terms used in this law whose meaning is not defined in paragraph (1) of this Article, have a meaning determined by another law.

Application

Article 4

(1)The provisions of this Law shall also apply to the prevention of money laundering, through identifying the user of the trusted services, confirming his identity based on the processing of documents, data or information obtained from reliable and independent source, including devices of electronic identification, appropriate trusted services.

(2)The provisions of this Law that refer to trust services shall not apply within a closed system or a system intended for a limited group of participants, whose use can be determined by an agreement or an internal act, and which does not influence third parties or does not cause liabilities to third parties other than that system.

Processing and protection of personal data

Article 5

(1)A trust service provider shall, when processing personal data to which it has access during the performance of its activity, act in accordance with the regulations governing the protection of personal data.

(2)When conducting an electronic transaction, a user may use a pseudonym if the usage of the relevant pseudonym is not in conflict with the provisions of another law.

II. ELECTRONIC DOCUMENT

Legal effects of electronic document

Article 6

(1)An electronic document shall have equal legal effect and probative force as the written form of the document, in accordance with the law.

(2) An electronic document cannot be denied as evidence in an administrative or court proceeding, solely because it is created in electronic form.

(3)Where the law prescribes a written form of documents or acts, the electronic document shall be considered as a document or act in a written form.

Creating an electronic document

Article 7

(1)An electronic document shall be created using one or more of the available and usable information and communication technologies, unless otherwise provided by law.

- (2) An electronic document representing archival material shall be created in a form that meets the requirements prescribed by this Law and is suitable for reliable preparation for electronic storage.
- (3) Electronic documents contain mandatory elements.
- (4) The mandatory elements of the electronic documents shall be prescribed by the Minister of Information Society and Administration with a rulebook.

Original and copy

Article 8

- (1) Any electronic copy of the electronic document shall be considered as original.
- (2) An electronic document created by digitizing a source document whose original form is not electronic shall be considered as a copy of the original document.
- (3) When the electronic document is reproduced in a paper form, it shall be considered a copy of the original document.

Document digitization

Article 9

(1) A digitized document shall have the same legal effect and probative force as the original document, if:

1) the digitization of the document was carried out under the supervision of or by:

- a natural person or an authorised person of a legal entity that created the document which is the subject of digitization or

- persons who are authorised to handle documents that contain signatures, manuscripts or records, in accordance with the regulations governing the archive and office work or

- persons who are authorised by this or another law to verify a digitized document;

2) the identity of the digitized document with the original document is confirmed with a qualified electronic seal or a qualified electronic signature of the persons referred to in item 1) of this paragraph or the person to whom the competences, under which the document was adopted, were transferred.

Certification of a printed copy of an electronic document

Article 10

An electronic document reproduced on any print media has equal legal and evidentiary force as the original electronic document, if:

1) reproduction of an electronic document is performed under the supervision or by a natural person or an authorised person of a legal entity that created the document and

2) printing of a document is carried out in such a way that the identity of the electronic document with the printed document is confirmed with a personal signature of a natural person or an authorised person of a legal entity.

III ELECTRONIC IDENTIFICATION

1. Electronic identification schemes

Conditions to be met by electronic identification schemes

Article 11

Electronic identification schemes shall comply with the following conditions:

- 1) to include confirmation of the data for identification of entities to whom the electronic identification devices have been issued, which uniquely identify the legal or natural person;
- 2) to ensure that the issuer of the electronic identification devices provides identification data within the electronic identification devices that correspond to the person to whom the electronic identification devices has been issued;
- 3) to meet the conditions for the security level in which the electronic identification scheme is classified, as defined in Article 13 of this Law.

Consent for identification

Article 12

The procedure for issuing an electronic identification may only be conducted after a previous request of a natural or legal entity who is the subject of identification, unless otherwise specified by law.

Security levels of electronic identification schemes

Article 13

Electronic identification schemes shall be classified according to the security level of the electronic identification devices that are issued under that scheme, as follows:

- 1) **security level low** shall provide a limited degree of security in the claimed or asserted identity of a person, and is characterised with reference to technical specifications, standards and procedures, including technical controls, the purpose of which is to decrease the risk of misuse or alteration of the identity;
- 2) **security level substantial** shall provide a substantial degree of security in the claimed or asserted identity of a person, and is characterised with reference to technical specifications, standards and procedures, including technical controls aimed at significantly reducing the risk of abuse or alteration of identity and,
- 3) **security level high** shall provide a higher degree of security in the claimed or asserted identity of a person than electronic identification devices with the security level “substantial”, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to prevent abuse or alteration of the identity.

Register of trusted service providers and electronic identification schemes

Article 14

- (1) A trust service provider shall submit an application to the Ministry of Information Society and Administration for registration in the Register of trust service providers and electronic identification

schemes (herein further: the Register), which is kept by the Ministry of Information Society and Administration.

(2) Electronic identification schemes must be registered in the Register used by public authorities.

(3) In the Register upon a previously submitted request by the public authority or the private legal entity may also register electronic identification schemes which are created by public bodies, and schemes created by private legal entities.

(4) Schemes created by public sector bodies shall be registered in the Register pursuant to a decision for registration issued by the Minister of Information Society and Administration, after a previously submitted application for registration of a scheme by the public sector body.

(5) Schemes created by private legal entities must comply with high security level in order to be registered in the Register.

(6) The Register referred to in paragraph 1 of this Article shall contain the following information about the trust service provider:

- name of the legal entity,
- contact information such as: address, telephone number and e-mail;
- type of service provided by the issuer of electronic identification scheme;
- electronic identification devices used under the scheme;
- security level.

(7) The providers of qualified trust service shall also be registered in the Register.

(8) Trust service providers and electronic identification schemes may be deleted from the Register if:

- cease to meet the conditions set out in this Law,
- the deviations from this law shall not be removed upon prior indication of elimination of deficiencies within the deadline determined in the decision for removal of irregularities issued in accordance with this Law or
- in other cases, determined by law for deletion of legal entities from the records of competent authority.

(9) The Minister of Information Society and Administration shall prescribe the content and manner of keeping the Register referred to in paragraph 1 of this Article, as well as the manner of applying for registration, the necessary documentation required with the application, the application form and the manner of publishing the data from the Register, depending on the type of trust service.

Use of electronic identification schemes in electronic business and in communication with a public sector body

Article 15

(1) The electronic identification scheme registered in the Register referred to in Article 14 of this Law (hereinafter: registered electronic identification scheme) shall be used for electronic identification of the person who is conducting a procedure before a public sector body.

(2) For electronic identification of the person taking actions related to private sector activities, including e-commerce, on their own selection may use a registered scheme or an electronic identification scheme that is not registered in the Register referred to in Article 14 of this Law.

Liability for damage arising from use of registered electronic identification schemes

Article 16

- (1) The issuer of the registered electronic identification scheme shall be liable for the damage that may arise because the scheme does not meet the requirements of Article 18 of this Law.
- (2) The damage caused as a result of the incorrectly conducted validation procedure shall be the responsibility of the party conducting the procedure if the damage was caused intentionally or negligently.
- (3) The burden of proving the damage caused shall lie with the party that is claiming compensation of damages.
- (4) The issuer referred to in paragraph (1) of this Article is obliged to be insured against possible damage which can cause it.
- (5) The lowest amount of insurance against any damage caused by the issuer shall be prescribed by the Minister of Information Society and Administration.

Application for determining the fulfilment of conditions for the security level of schemes

Article 17

- (1) The request for determining the fulfilment of conditions for levels of security of schemes shall be attached to the request for registration in the Register referred to in Article 14 of this Law.
- (2) The request referred to in paragraph (1) of this Article shall contain the following information:
 - (1) the manner of proving and verifying the identity of a natural or legal persons which requires the issuance of a device of electronic identification;
 - (2) the manner of issuing the devices for electronic identification;
 - (3) authentication mechanisms, through which a natural or legal person, using the devices for identification, confirms the identity of the party concerned;
 - (4) the conditions to be met by the other participants involved in the procedure for issuing devices for electronic identification;
 - (5) technical and security features of electronic identification devices issued under the scheme;
 - (6) technical and organizational measures fulfilled by the issuer of electronic identification devices in order to ensure interoperability of electronic identification schemes in accordance with national and international standards in this area;
 - (7) report on the level of security of the electronic identification scheme by the body for conformity assessment and
 - (8) data on the issuer of the electronic identification scheme.

Security conditions to be met by electronic identification service providers

Article 18

(1) The issuer of electronic identification scheme shall undertake the necessary technical, physical and organizational measures to manage risks that could endanger the reliable and secure provision of these services.

(2) The technical and organizational measures shall ensure that the level of security corresponds to the level of risk and the predicted security level of the electronic identification scheme, taking into account the latest available technological solutions, and in particular, the measures to prevent security incidents and to limit the harmful effects of possible incidents, as well as to inform stakeholders about unwanted effects of security incidents.

(3) The requirements to be fulfilled by technical and organizational measures for the security of electronic identification schemes shall be prescribed by the Minister of Information Society and Administration.

(4) The assessment of the level of security of the electronic identification scheme shall be carried out by the conformity body that is accredited to perform the certification in accordance with standards, defined in the corresponding secondary legislation set forth in paragraph 3 of this Article.

2. Cross-border cooperation in the field of electronic identification

Interoperability of technical systems

Article 19

The Ministry of Information Society and Administration shall cooperate with relevant international institutions on issues related to cross-border interoperability of the electronic identification schemes, and shall take measures within its jurisdiction in order to establish the highest level of interoperability of the electronic identification schemes at the national level, in order to ensure their integration and interoperability in the internationally recognized electronic identification schemes.

Registration of an electronic identification scheme issued by a foreign legal person

Article 20

(1) The Ministry of Information Society and Administration may register in the Register of trust service providers and electronic identification schemes foreign legal entities registered as trust service providers or issuers of electronic identification schemes at the European Union level or in a member state of the union.

(2) The Ministry of Information Society and Administration may also register in the Register electronic identification schemes corresponding to a high-level security, if that scheme is used by a member state of the European Union.

(3) The Ministry of Information Society and Administration may register in the Register of trust services providers and electronic identification schemes foreign legal entities registered as providers of trust services or as issuers of electronic identification schemes in another country that is not a member state of the European Union, on the basis of a previously concluded agreement which establishes reciprocity of the electronic identification schemes and / or the providers of trust services between the Republic of North Macedonia and the state where the legal entity is registered.

IV TRUST SERVICES

1. General Provisions

Types of trust services

Article 21

(1) Trust services are services that are defined as trust services in accordance with the provisions of this Law.

(2) Qualified trust services shall be:

- 1) issuance of qualified certificates for electronic signatures,
- 2) issuance of qualified certificates for electronic seals,
- 3) issuance of qualified certificates for website authentication,
- 4) qualified trust service for preservation of qualified electronic signatures,
- 5) qualified trust service for preservation of qualified electronic seals,
- 6) qualified validation of a qualified electronic signature,
- 7) qualified validation of a qualified electronic seal,
- 8) qualified trust service for issuance of a qualified electronic time stamp,
- 9) qualified trust service for electronic registered delivery and
- 10) qualified trust service for electronic document preservation.

(3) A trust service provider or a qualified trust service provider may provide one or more services from paragraph 1 and 2 of this Article.

Liability of trust service providers

Article 22

(1) A trust service provider shall be liable for damage resulting from failure to act in accordance with this Law if the damage was caused intentionally or negligently.

(2) The burden of proving intention or negligence of a trust service provider shall lie with the natural or legal person claiming the damage referred to in paragraph 1 of this Article.

(3) When trust service providers inform users of trust services in relation to restrictions of trust services they provide in advance and properly and when these restrictions are

recognizable to third parties, trust service providers shall not be liable for damages arising from use of services that exceed the stated restrictions.

(4) A qualified trust service provider must be insured against liability or to provide financial resources in a manner and under conditions determined by this law, which apply for liability for damages from the use of electronic identification schemes.

Responsibility of trust service users

Article 23

The trust service user shall be obliged to protect the devices and data for issuance of an electronic signature or seal of unauthorised access and use, and shall be obliged to use them in accordance with the provisions of this Law.

Conditions to be met by trust service providers

Article 24

(1) A non-qualified trust service provider shall be obliged to notify the Ministry of Information Society and Administration on the performance of activity within a period of 15 days from the day of commencement of the activity.

(2) In addition to the basic data about the legal entity, the non-qualified trust service provider shall be obliged to also include in the notification the type of services, the technical standards that it applies and a statement that they will comply with the conditions for the performance of the activity.

(3) The Ministry of Information Society and Administration shall register the trust services and the provider of unqualified service in the Register referred to in paragraph (2) in this article, based on the submitted notification.

(4) A qualified trust service provider, before the commencement of its activity, shall be obliged to apply for registration in the Register.

(5) Trust service providers shall be obliged to undertake the necessary technical and organizational measures to manage risks that could jeopardize the security in the provision of these trust services.

(6) The technical and organizational measures shall ensure that the level of security corresponds to the level of risk, taking into account the latest available technological solutions, and in particular, measures shall be taken to prevent security incidents and to limit the harmful effects of possible incidents, as well as to inform stakeholders about unwanted effects of security incidents.

(7) Trust service providers, without delay, and no later than within 24 hours of becoming aware, shall notify the competent authority of any security breaches or loss of integrity of

the service that have a significant impact on the provision of trust services or the protection of personal data processed within the provision of the service.

(8) In the event that the security breach is related to the protection of personal data, the trust service provider shall also notify the Directorate for Personal Data Protection.

(9) If a breach of security or loss of confidentiality service may adversely affect users of the trust service, the trust service provider shall be obliged, immediately and within 24 hours at the latest, to inform the user of the trusted service.

(10) The Ministry of Information Society and Administration shall inform the public, directly or by request to a trust service provider to do the same, if it finds that with a breach of security or loss of integrity of trust services, the public interest is affected.

(11) The Ministry of Information Society and Administration shall cooperate with competent international institutions regarding the exchange of security information and the integrity of the trust services in accordance with the international agreements ratified in accordance with the Constitution of the Republic of North Macedonia.

Competence of the Ministry of Information Society and Administration for trust services and electronic identification schemes

Article 25

The Ministry of Information Society and Administration, in accordance with this law, shall perform the following tasks:

- 1) maintains the Register of trust service providers and electronic identification schemes;
- 2) follows the recommendations from the reports for checking the fulfilment of the conditions for providing qualified trust service;
- 3) supervises the work of trust service providers and issuers of schemes for electronic identification;
- 4) initiates supervision before a conformity assessment body over the provider of trust service;
- 5) conducts an extraordinary check of the fulfilment of conditions for the provision of qualified trust services and schemes, in accordance with the law;
- 6) cooperates with the competent personal data protection authority and informs it without delay if it finds out that the qualified trust service providers do not comply with the regulations on personal data protection;
- 7) confirms the existence and proper implementation of the plans for termination of activity of trust service provider, including the manner in which the data they issued or received shall remain accessible in order to ensure the continuity of the service or to serve as evidence in a court procedure;

8) cooperates with the supervisory bodies of the European Commission.

Competencies of the Ministry of Information Society and Administration in the framework of cross-border cooperation

Article 26

The Ministry of Information Society and Administration in the framework of the cross-border cooperation shall report to the European Commission on its activities in accordance with the eIDAS Regulation, starting from the date of accession of the Republic of North Macedonia as a state within the competent authorities at the level of European Union or after the accession of the Republic of North Macedonia to the European Union.

Competent accreditation body

Article 27

1) Upon previously issued opinion by the Accreditation Institute of the Republic of North Macedonia, the Ministry of Information Society and Administration shall adopt a methodology for accreditation of conformity assessment bodies and laboratories for testing of devices, which includes the standards set by the Minister of Information Society and Administration.

2) The Ministry of Information Society and Administration shall keep a list of accredited conformity assessment bodies and laboratories in the North Republic Macedonia.

3) The accreditation conducted by a competent accreditation body of a member state of the European Union shall be recognized in the Republic of North Macedonia.

2. General provisions on qualified trust services

Establishing the relationship between the qualified trust service provider and users

Article 28

(1) A qualified trust service is provided pursuant to an agreement concluded between the qualified trust service provider and the user, which is concluded upon prior request of the user.

(2) The qualified trust service provider shall, before concluding the agreement referred to in paragraph 1 of this Article, in a clear and unambiguous way notify the person, who submitted the request for qualified trust service provision, about all important circumstances of the use of the service, in particular:

1) regulations and rules relating to the use of a qualified trust service;

2) any limitations on the use of a qualified trust service;

3) the measures to be implemented by users of a qualified trust service, and the necessary technology for safe use of qualified trust services.

Conditions for provision of qualified trust services

Article 29

(1) The qualified trust service provider shall meet the following conditions:

1) to employ or subcontract staff that possess the necessary expertise, experience, and qualifications to apply administrative and management procedures which correspond to national and international standards, and who have received appropriate training regarding information security;

2) to be insured against professional liability for damages or to maintain sufficient financial resources for compensation of damages resulting from the performance of a qualified trust service;

3) to use trustworthy systems and products that are protected against unauthorised modification and ensure the technical security and reliability of the processes supported by them;

4) to use trustworthy systems to store data provided to it, in a verifiable form, thus:

- the data are publicly available only where the consent of the person to whom the data relates has been obtained,

- only authorised persons can make entries and changes to the stored data,

- the data can be subject to authentication;

5) to take appropriate measures against forgery, theft and unauthorised access to data;

6) to record and keep accessible for an appropriate period of time, including after the activities of the qualified trust service provider have ceased, all relevant information concerning data issued and received by the qualified trust service provider, in particular, for the purpose of providing evidence in legal proceedings and ensuring continuity of the service. Such recording may be done electronically;

7) to keep updated, accurate and well-protected databases of issued qualified electronic certificates, if the provider of qualified trust service issues certificates;

8) to have an up-to-date plan for termination of activity to ensure continuity of provision of qualified trust services for their users;

9) to take technical and organizational measures for the processing of personal data in accordance with the laws of the Republic of North Macedonia.

(2) A qualified trust service provider shall be obliged to adopt the following acts:

- 1) general conditions for the provision of services that are publicly available;
- 2) procedures and methods that the qualified trust service provider uses to ensure the provision of service in accordance with the regulations and the general conditions referred to in item 1) of this paragraph.

(3) A condition for performing an activity of a qualified trust service provider is the entry in the Register of trust services and electronic identification schemes.

Professional liability insurance

Article 30

The Minister of Information Society and Administration shall prescribe the lowest amount or the type of coverage of the insurance against the risk of liability for damages caused by a qualified trust service provider.

Identity verification of a qualified trust service user

Article 31

(1) The qualified trust service provider shall verify the data for natural or legal person before issuing a qualified certificate, in accordance with the law.

(2) The verification of the data referred to in paragraph (1) of this Article shall be performed directly or through an authorised person in accordance with the law by the qualified trust service provider, in the following manner:

1) by physical presence of the natural person or of an authorised representative of the legal person; or

2) remotely, using electronic identification devices for which, prior to the issuance of the qualified certificate, a physical presence of the natural person or of an authorised representative of the legal person was ensured and which meets the requirements set out in Article 13 with regard to the security levels of the electronic identification scheme corresponding to "substantial" or "high"; or

3) by means of a certificate of a qualified electronic signature or of a qualified electronic seal issued in compliance with item 1) or 2) in this paragraph; or

4) by using other identification methods recognised at national level that provide equivalent security in terms of reliability to physical presence. The equivalent security level shall be confirmed by a conformity assessment body;

5) by identification methods used in a member state of the European Union;

(3) In the event of change of the data referred to in paragraph 1 of this Article, the natural or legal person shall be obliged without delay, within 7 days from the date of change at the latest, to notify the qualified trust service provider of the occurrence of the change.

(4) For the identification and use of qualified trust services, the qualified trust service provider and the issuer of electronic identification schemes may verify or integrate their systems in an

interoperable manner for remote verification with the central register of the population, personal identification documents, registers of legal persons and other persons, when necessary.

Assessment of the conditions for providing qualified trust services

Article 32

- 1) Assessment of the fulfilment of requirements for the provision of qualified trust services shall be performed by a conformity assessment body.
- 2) Conformity assessment body is a legal person accredited to assess the conformity of the qualified trust service provider and the qualified trust services they provide, pursuant to an initiative of the Ministry of Information Society and Administration or after a request of the service provider.
- 3) After completing the assessment of the fulfilment of requirements, the conformity assessment body shall make a conformity assessment report.
- 4) Assessment of the fulfilment of requirements shall be made before the beginning of the performance of the activity of the qualified trust service provider, and at least once in 24 months, for each qualified trust service provider.
- 5) Upon completing the report for the performed assessment of the conformity of the applicant or the qualified trust service provider, the conformity assessment body shall submit the report to the Ministry of Information Society and Administration, immediately or within three working days at the latest.
- 6) The Ministry may order an extraordinary reassessment of conformity if irregularities were identified in the provision of qualified trust services or if an incident occurred that significantly jeopardized or violated information security.
- 7) The cost of the conformity assessment, including extraordinary reassessments, shall be borne by the qualified trust service provider.
- 8) The Ministry of Information Society and Administration shall determine the list of standards that should be fulfilled by the conformity assessment body, the mandatory content of the conformity assessment report, the assessment procedure for compliance with the requirements, as well as the list of legal entities authorised in the Republic of North Macedonia or in a member state of the European Union who can perform conformity assessments in the Republic of North Macedonia.

Procedure for entry of a qualified trust service provider in the Register

Article 33

- 1) A legal entity intending to provide qualified trust services shall submit a request to the Ministry of Information Society and Administration for registration in the Register, before commencing the provision of qualified trust services.

2) In addition to the request referred to in paragraph (1) of this Article, the legal entity shall enclose the materials listed as information in the request, including the report on conformity assessment in accordance with Article 32 of this Law.

3) The Ministry of Information Society and Administration shall issue a decision on the registration of the applicant in the Register, granting the status of a qualified trust service provider to the relevant trust service provider, within 60 days from the date of receipt of the request, if it is complete, and based on the claims contained in the conformity assessment report.

4) As an exception to paragraph (3) of this Article, when additional checks are necessary or obtaining additional evidence that requires a longer deadline is required, the Ministry for Information Society and Administration shall extend the deadline for the adoption of the decision for registration in the Register, not longer than 60 days from the determined deadline in paragraph (3) of this Article.

5) In the decision-making process, the Ministry of Information Society and Administration may request the attachment of additional evidence, as well as additional verification of technical and organizational measures and verification of security capacities of the applicant and the services, in accordance with the law.

6) If the applicant or the services listed in the request fail to fulfil the conditions prescribed by this Law, the Ministry of Information Society and Administration shall issue a decision on refusal of the request for registration in the register after the expiration of the deadline determined in paragraph (3) or paragraph (4) of this Article.

Termination of the performance of the activity of a qualified trust service provider

Article 34

1) A qualified trust services provider, that intends to cease its activities, shall be obliged to notify the qualified trust service users and the Ministry of Information Society and Administration, three months before the intended end of the performance of the activities at the latest.

2) The qualified trust service provider, that intends to cease its activities, shall be obliged to provide continuation of the service with another qualified trust service provider for the qualified trust service users, and immediately notify the Ministry of Information Society and Administration of the measures taken, or within the deadline determined in paragraph (1) of this Article.

3) The qualified trust service provider shall be obliged to submit all documentation and necessary technical means in accordance with the law connected with the performance of the trust services to another qualified trust service provider to whom it shall transfer the obligations of performing one or more trust services.

4) If the qualified trust service provider fails to comply with the obligation set out in paragraphs (2) and (3) of this Article, the Ministry of Information Society and Administration

shall request from the qualified trust service provider, without delay, to submit to the Ministry all documentation and equipment, including the procedures for acting upon them.

5) The Ministry shall temporarily keep the documentation and the equipment, until the provision of another qualified trust service provider that will continue to perform these services for the users, at the expense of the qualified trust service provider that ceases to perform this activity.

6) The manner and the procedure for keeping the documentation and the equipment, is prescribed by the Minister of Information Society and Administration.

7) In case of a temporary prohibition of the performance of activity of a qualified trust service provider, the qualified certificates issued before the date of the entry into force of the prohibition shall remain in effect.

List of qualified trust service providers

Article 35

1) The Ministry of Information Society and Administration shall publish a list of qualified trust service providers, as well as a list of qualified trust services they provide on their web site, in an electronic form suitable for automated processing.

2) The list referred to in paragraph (1) of this Article shall be signed or sealed with the electronic signature or electronic seal of the Ministry of Information Society and Administration.

3) The data in the list of qualified trust service providers shall be derived from the Register of trust service providers and electronic identification schemes, as well as data obtained with the use of automated means.

4) The form and manner of publishing the list referred to in paragraph (1) of this Article are determined by the Minister of Information Society and Administration.

Trust mark for qualified trust services

Article 36

1) Trust mark for qualified trust services (hereinafter: trust mark) is a sign that is simple, recognizable and clearly indicates the qualified trust service, whose form, content and logo are determined by paragraph (3) of this Article.

2) The qualified trust service providers have the right to use the trust mark for the qualified trust service for which they are registered and are bound to link it to the list of qualified trust service providers.

3) The Minister of Information Society and Administration shall determine the form, composition, size and design of the trust mark for the qualified trust services.

Cross-border recognition of qualified trust services

Article 37

(1) To a trust service provider registered with a seat in a foreign country, the status of a trust service provider in the Republic of North Macedonia shall be recognized if it is registered in the Register of trust service providers and schemes for electronic identification.

(2) Trust service providers established by a member state of the European Union and are registered in the List of trust services of the European Union, may operate and provide services on the territory of the Republic of North Macedonia, without prior registration in the Register of trust service providers and schemes for electronic identification.

(3) Qualified trust service providers registered in Republic of North Macedonia, which are registered in the Register of providers of trust services and electronic identification schemes are legally equivalent to qualified trust services provided by qualified trust services providers established in the European Union, on the basis of a previously concluded agreement between the Republic of North Macedonia and the European Union.

(4) The agreement referred to in paragraph (3) of this Article shall in particular guarantee that:

(a) the requirements applicable to qualified trust service providers established in the European Union and the qualified trust services they provide, are met by trust service providers in the Republic of North Macedonia and,

(b) qualified trust services provided by qualified trust service providers established in the European Union are recognized as legally equivalent to the trust services provided by the trust service providers in the Republic of North Macedonia.

V. ELECTRONIC SIGNATURE AND ELECTRONIC SEAL

1. Advanced electronic signatures

Requirements for advanced electronic signatures

Article 38

An advanced electronic signature shall meet the following requirements:

- 1) to be uniquely linked to the signatory;
- 2) to be capable of identifying the signatory;
- 3) to be created using electronic signature creation data that the signatory may, with a high level of trust, use under his sole control;
- 4) to be linked to the data signed in such a way that any subsequent change in the data is detectable.

2. Advanced electronic seal

Requirements for advanced electronic seals

Article 39

An advanced electronic seal shall meet the following requirements:

- 1) to be uniquely linked to the creator of the seal;
- 2) to be capable of identifying the creator of the seal;
- 3) to be created using electronic seal creation data that the creator of the seal may, with a high level of trust, use under his sole control;
- 4) to be linked to the data to which it relates in such a way that any subsequent change in the data is detectable.

3. Content of a qualified certificate for electronic signature and seal

Article 40

- 1) The standards that should be contained in the qualified certificates for electronic signature and electronic seal shall be prescribed by the Minister of Information Society and Administration.
- 2) Apart from the standards form paragraph (1) of this Article that should be contained in the qualified certificates for electronic signature and electronic seal, they may also contain additional elements that do not affect the interoperability and the recognition of the qualified electronic signature and electronic seal.

Legal effects and probative force of qualified certificates for electronic signature and seal

Article 41

Qualified certificates for electronic signature and electronic seal issued by qualified trust service providers shall have the same legal effect and probative force as public documents.

Revocation and suspension of a qualified certificate for electronic signature, electronic seal and website authenticity

Article 42

(1) A qualified trust service provider that issues qualified certificates for electronic signatures, electronic seals and website authenticity shall be obligated to revoke the issued qualified certificates when:

- 1) the owner of the certificate for qualified electronic signature, for electronic seal or website authenticity files for revocation of the certificate;
- 2) the owner of the certificate loses their legal capacity, or has ceased to exist, or the circumstances that significantly affect the validity of the certificate have changed;
- 3) it finds that data in the certificate is missing;
- 4) it determines that the data for the creation of the qualified electronic signature, for the qualified electronic seal, or for website authenticity, or the system of the qualified trust service providers are endangered in a manner that affects the security and reliability of the certificate;

- 5) it determines that the data for creation of the electronic signature, for the electronic seal, or for website authenticity, or the system used for performance of the electronic transaction are endangered in a manner that affects the reliability and security of the electronic signature, the electronic seal, or the website and
- 6) the legal person has ceased to exist, under conditions determined by law.
- (2) A trust service provider that issues qualified certificates for electronic signatures, electronic seals or website authenticity shall be obliged to inform the qualified trust service user about the revocation of the certificate within 24 hours of the received request, or of the occurrence of the circumstances pursuant to which the certificate is revoked.
- (3) If the qualified certificate for electronic signature, electronic seal or website authenticity was revoked after its primary issuance, then it shall lose its validity from the moment of revocation and its qualified certificate status may not be returned under any circumstances.
- (4) Qualified trust service providers that issue qualified certificates, provide information for validity, suspension or revocation of issued qualified certificates to each affected party.
- (5) The information referred to in paragraph (4) of this Article shall be made available to every affected party at least for individual certificates, at any time and after the expiration of the period of their validity, in an automatic way that is safe, effective and without fee.
- (6) The user of a qualified trust service is obliged to request revocation of an issued certificate for qualified electronic signature, for qualified electronic seal and for website authenticity from its publisher in case of loss, damage or endangerment of the integrity of the certificate data or if the certificate creation data changes.
- (7) In case of suspension of a certificate for qualified electronic signature, for electronic seal and for website authenticity, it loses its validity for the duration of the period of validity of the suspension.
- (8) Information on suspension and its duration for a qualified certificate for an electronic signature, for an electronic seal or for website authenticity or for their revocation will be entered in the database of issued qualified certificates kept by a qualified trust service provider and they will be visible when checking the validity status of a qualified electronic certificate.

**Records on issued and revoked qualified certificates for qualified electronic signature,
electronic seal and website authenticity**

Article 43

- 1) The issuer of qualified certificates for electronic signature, for electronic seal or for website authenticity shall be obliged to keep the entire documentation for the issued and revoked qualified certificates for electronic signature, for electronic seal or for website authenticity, as well as the devices for electronic identification and verification in administrative, legal and other procedures, at least ten years after the expiration of the term for which the certificate was issued or after its revocation.
- 2) The obligation from paragraph (1) of this Article shall also refer to the suspension of qualified certificates for electronic signature, electronic seal or for website authenticity.
- n 3) The data referred to in paragraph (1) of this Article may also be kept in electronic form.

Qualified electronic signature or qualified seal creation devices

Article 44

The Minister of Information Society and Administration shall prescribe the technical requirements that should be met and the manner of creating qualified electronic signatures or qualified electronic seals by the qualified trust service providers.

Conformity of qualified electronic signature or qualified electronic seal creation devices

Article 45

1) Assessment of the fulfilment of the technical standards as regards the qualified electronic signature or qualified electronic seal creation devices shall be carried out by an accredited laboratory.

2) The laboratory shall issue a certificate of conformity of the devices for creating qualified electronic signatures or qualified electronic seals and shall inform the Ministry of Information Society and Administration within seven days at the latest, beginning from the day of the issued certificate for the funds.

3) The technical standards which should be fulfilled, and which are subject of assessment of the fulfilment of technical requirements by the conformity body shall be prescribed by the act adopted on the basis of Article 44 of this Law.

4) The Ministry keeps a list of qualified electronic signature and qualified electronic seal creation devices, based on the data obtained from the certificates of the laboratory.

5) The laboratory shall, without delay and within 7 days from the day of occurrence of the change at the latest, notify the Ministry of Information Society and Administration of the issued or withdrawn certificate of conformity of the qualified electronic signature and qualified electronic seal creation devices.

6) The Minister of Information Society and Administration shall prescribe the content and the manner of keeping the list of paragraph (4) of this Article, the manner of submitting the application for registration in the list, the required documentation with the application, as well as the manner of applying for registration in the list.

7) The content of the certificate of conformity of the qualified electronic signature or qualified electronic seal creation devices and the method of its issuance shall be prescribed by the Minister of Information Society and Administration.

8) The devices from paragraph (1) of this Article certified in accredited laboratories in a member state of the European Union shall also be recognized in the Republic of North Macedonia.

4. Qualified trust service for validation of a qualified electronic signature or qualified electronic seal

Qualified electronic signature and qualified electronic seal validation process

Article 46

(1) The process for the validation of a qualified electronic signature or a qualified electronic seal shall be carried out in order to determine:

- 1) that the certificate that supports the electronic signature or seal was, at the time of signing or sealing, a qualified electronic certificate;
- 2) that the qualified electronic certificate was issued by a qualified trust service provider and was valid at the time of signing or sealing;
- 3) that the electronic signature or seal validation data correspond to the data provided to the relying party;
- 4) that the unique set of data representing the signatory or the creator of a seal in the qualified certificate is correctly provided to the relying party;
- 5) the use of pseudonym is clearly indicated to the relying party if a pseudonym was used at the time of signing or sealing;
- 6) that the electronic signature or electronic seal was created by a qualified electronic signature or qualified electronic seal creation device;
- 7) that the integrity of the signed or sealed data has not been compromised;
- 8) that the requirements provided for in Articles 38 and 39 of this Law were met at the time of signing or sealing.

(2) The system used for validating the qualified electronic signature or qualified electronic seal shall provide to the relying party the correct result of the validation process and shall allow the relying party to detect any issues related to security.

Requirements for the provision of a qualified validation service for qualified electronic signature or qualified electronic seal

Article 47

(1) A qualified validation service for qualified electronic signature or qualified electronic seal may only be provided by a qualified trust service provider, as follows:

- 1) the procedure for the validation of a qualified electronic signature or qualified electronic seal shall be carried out in accordance with Article 46 of this Law;
- 2) the relying party shall receive the result of the validation process in an automated manner, which is reliable and efficient;
- 3) the certificate of the validation process from item 2) of this paragraph shall bear an advanced electronic seal or advanced electronic signature of the qualified trust service provider.

(2) A validation certificate of a qualified electronic signature or qualified electronic seal issued by a qualified trust service provider shall have the same legal effect and probative force as a public document.

(3) The standards to be contained in the validation certificates of a qualified electronic signature or qualified electronic seal shall be prescribed by the Minister of Information Society and Administration.

5. Qualified preservation service for qualified electronic signatures or qualified electronic seals

Requirements for the provision of qualified preservation service for qualified electronic signatures or qualified electronic seals

Article 48

1) A qualified preservation service for qualified electronic signatures or qualified electronic seals may only be provided by a qualified trust service provider that uses procedures and technologies capable of extending the trustworthiness of the qualified electronic signature or qualified electronic seal beyond the technological validity period.

2) The standards for the qualified preservation service for qualified electronic signatures or qualified electronic seals shall be prescribed by the Minister of Information Society and Administration by a rulebook.

Legal effect of the electronic signature

Article 49

1) An electronic signature shall not be denied probative force solely on the grounds that it has an electronic form or because it meets the requirements for qualified electronic signatures.

2) A qualified electronic signature shall have the equivalent legal effect and probative force of a handwritten signature.

Legal effect of the electronic seal

Article 50

1) An electronic seal shall not be denied probative force solely on the grounds that it has an electronic form or that it meets the requirements for qualified electronic seal.

2) A qualified electronic seal shall enjoy the presumption of integrity of the data and of correctness of the origin of that data to which the qualified electronic seal is linked.

6. Electronic Time Stamp

Requirements for qualified electronic time stamps

Article 51

(1) A qualified electronic time stamp shall meet the following requirements:

- 1) it binds the date and time to data in such a manner as to reasonably preclude the possibility of the data being changed undetectably;
- 2) it is based on an accurate time source linked to an established international time standard;
- 3) it is signed using an advanced electronic signature or sealed with an advanced electronic seal of the qualified trust service provider.

(2) The standards to be met by the qualified electronic time stamps shall be prescribed by the Minister of Information Society and Administration.

Legal effect of the electronic time stamps

Article 52

1) An electronic time stamp shall not be denied probative force solely on the grounds that it has an electronic form or that it meets the requirements of the qualified electronic time stamp.

2) A qualified electronic time stamp shall enjoy the presumption of the accuracy of the date and the time it indicates and the integrity of the data to which the date and time are bound.

3) The qualified certificate for electronic time stamp issued by the qualified trust service provider shall have the same legal effect and probative force as a public document.

7. Electronic registered delivery

Requirements for qualified electronic registered delivery services

Article 53

(1) Qualified electronic registered delivery services shall meet the following requirements:

- 1) to be provided by one or more qualified trust service providers;
- 2) to ensure a high level of security for identification of the sender;
- 3) to ensure the identification of the addressee before the delivery of the data;
- 4) sending and receiving of data is secured with the use of an advanced electronic signature or an advanced electronic seal of a qualified trust service provider in such a manner as to preclude the possibility of the data being changed undetectably;
- 5) to ensure secure data exchange that is in line with the objectives of sending and receiving data, through which the sender and the addressee of the data can be clearly identified;

- 6) to ensure that the date and time of sending, receiving and any potential change of data are clearly indicated by an electronic time stamp;
 - 7) in the event of the data being transferred between two or more qualified electronic registered delivery service providers, to ensure that the requirements shall apply to all of the qualified electronic registered delivery service providers.
- (2) The standards containing the certificates for qualified electronic recommended delivery shall be prescribed by the Minister of Information Society and Administration.

Legal effect of electronic registered delivery service

Article 54

- 1) Data sent and received using an electronic registered delivery service shall not be denied probative force solely on the grounds that it has an electronic form or that it meets the requirements of the qualified electronic registered delivery service.
- 2) Data sent and received using a qualified electronic registered delivery service shall enjoy the presumption of the integrity of the data, the sending of that data by the identified sender, its receipt by the identified addressee and the accuracy of the date and time of sending and receipt indicated by the qualified electronic registered delivery service provider.
- 3) The certificate of a qualified electronic registered delivery issued by a qualified trust service provider shall have the same legal effect and probative force as a public document.

8. Website authentication checks

Qualified certificates for website authentication

Article 55

A qualified certificate for website authentication should fulfil the standards prescribed by the Minister of Information Society and Administration.

Legal effect and probative force of a qualified certificate for website authentication

Article 56

- (1) A qualified certificate for website authentication issued by a qualified trust service provider shall have the same legal effect and probative force as a public document.
- (2) A qualified certificate of authenticity of websites issued by a qualified trust service provider registered in the European Union or in a member state of the Union shall be recognized as having been issued by a domestic legal entity.

9. Electronic preservation of documents

Preparation of documents for electronic preservation

Article 57

(1) Preparation of documents for electronic preservation refers to:

- 1) documents originally created in an electronic form suitable for electronic preservation;
 - 2) conversion of an electronic document in a different form suitable for electronic preservation;
 - 3) digitization of documents originally created in a form that is not electronic into a form suitable for electronic preservation.
- (2) A document prepared for electronic preservation may also include metadata, at the choice of the person who prepares documents for electronic preservation or for the needs of the process itself.

Preparation of documents for trustworthy electronic preservation and qualified electronic preservation

Article 58

(1) Preparation of documents for trustworthy electronic preservation must meet the following requirements:

- 1) ensure that all essential elements of the content of the original document are faithfully transferred to a document prepared for electronic preservation, taking into account the nature and purpose of the document, i.e. the integrity of the content of the document is preserved;
 - 2) ensure that the usability of the original document is preserved;
 - 3) ensure that all elements of the content of the original document, of relevance to its authenticity, are included;
 - 4) ensure security of the integrity of the original document, as well as its additional documents, using electronic signature or seal and electronic time stamp;
 - 5) carry out control of the accuracy and quality of the conversion, in order to eliminate any errors that might arise in the conversion process;
 - 6) ensure that records are kept about undertaken actions in the preparation process for electronic preservation.
- (2) If the prescribed deadline for document preservation is longer than five years, the document prepared for trustworthy electronic preservation should be in a format that is suitable for long-term preservation.
- (3) Preparation of documents for trustworthy qualified electronic preservation must:

- 1) ensure that all essential elements of the content of the original document are faithfully transferred to a document prepared for electronic preservation, taking into account the nature and purpose of the document, i.e., the integrity of the content of the document is preserved;

- 2) ensure that the usability of the original document is preserved;
 - 3) ensure that all elements of the content of the original document, of relevance to its authenticity, are included;
 - 4) ensure security of the integrity of the original document as well as its additional documents, using electronic signature or electronic qualified seal and qualified electronic time stamp;
 - 5) carry out control of the accuracy and quality of the conversion, in order to eliminate any errors that might arise in the conversion process;
 - 6) ensure that records are kept about undertaken actions in the preparation process for electronic preservation.
- (4) If the prescribed deadline for document preservation is of enduring value, the document prepared for trustworthy qualified electronic preservation should be in a format that is suitable for long-term preservation.
- (5) On the proposal of the Ministry of Information Society and Administration, the Government shall prescribe detailed requirements that must be met for trustworthy preparation of a document for electronic preservation and qualified electronic preservation, and the document formats that are suitable for preservation.

Trustworthy electronic preservation and qualified electronic preservation of documents

Article 59

- 1) Trustworthy electronic preservation of documents, which originally contain an electronic signature or seal as a confirmation of the integrity and origin of such documents, shall be performed in such a manner that suitable procedures and technological solutions are used during the preservation.
- 2) Trustworthy electronic preservation of documents prepared in accordance with Article 58 of this Law, which bear electronic signature or seal and electronic time stamp in the manner defined in Article 58, paragraph (1), item 4) of this Law in order to verify the integrity and accuracy of the original document, and of its additional documents, shall be performed in such a manner that suitable technological solutions are used during the preservation period.
- 3) Trustworthy qualified electronic preservation of documents, which originally contain a qualified electronic signature or qualified electronic seal as a confirmation of the integrity and origin of such documents, shall be performed in such a manner that suitable procedures and technological solutions are used during the preservation.
- 4) Trustworthy electronic preservation of documents prepared in accordance with Article 58 of this Law, which bear a qualified electronic signature or qualified electronic seal and electronic time stamp in a manner defined in Article 58, paragraph (2), item 4) of this Law in order to verify the integrity and accuracy of the original document, and of its additional documents.

- 5) The Minister of Information Society and Administration shall prescribe the methodology for implementation of the procedures and technological solutions.

Electronic document preservation and qualified electronic document preservation services

Article 60

- 1) Electronic document preservation services shall be provided by a trust service provider that has taken appropriate technical and organizational measures by which it ensures the security of electronic document preservation, in accordance with the provisions of this Law.
- 2) An electronic document preservation service provider may opt to limit the document preservation only to documents that contain an electronic signature or seal in their original form.
- 3) A document preserved within electronic document preservation services shall enjoy the presumption of authenticity of the original document, a certificate of which shall be issued by the provider of the electronic document preservation service, according to the provisions of this Law.
- 4) If the document is preserved within the electronic document preservation service so that the preservation period is longer than the specified period of preservation of the original document, in accordance with the regulations regarding archive work, the original document may be destroyed, unless otherwise specified by law.
- 5) Qualified electronic document preservation services shall be provided by a trust service provider that has taken appropriate technical and organizational measures by which it ensures the security of the qualified electronic document preservation, in accordance with the provisions of this Law.
- 6) A qualified electronic document preservation service provider may opt to limit the document preservation only to documents that contain a qualified electronic signature or qualified electronic seal in their original form.
- 7) A document preserved within qualified electronic document preservation services shall enjoy the presumption of authenticity of the original document in legal transactions, a certificate of which shall be issued by the provider of the qualified electronic document preservation service.
- 8) If the document is preserved within the qualified electronic document preservation service so that the preservation period is longer than the specified period of preservation of the original document, the original document may be destroyed, unless otherwise specified by law.
- 9) The Minister of Information Society and Administration shall prescribe the standards to be fulfilled by electronic document preservation services and qualified electronic document preservation services.

VI. ELECTRONIC AUTHORIZATION

Register of authorizations

Article 61

- 1) For the exercise of rights by electronic means before any third party by a representative, the principal may authorize a proxy based on an electronic Register of authorizations.
- 2) The authorization shall be issued using the electronic identification of the principal and by signing the authorization with a qualified electronic signature.
- 3) The principal shall determine the actions for which the authorization is granted, the scope and the time limit of its validity.
- 4) The Register of authorizations shall be kept by qualified trust service providers for issuing qualified certificates for electronic signature, that issued the qualified certificate for electronic signature to the principal.
- 5) The persons referred to in paragraph (4) of this Article shall confirm each entry in the Register with a qualified electronic seal and a qualified electronic time stamp.
- 6) The Minister of Information Society and Administration shall prescribe the content and the manner of keeping the Register and the checks of the validity of powers.

Written form

Article 62

Authorizations registered in the Register of authorizations pursuant to Article 61 of this Law shall have the same legal effect and probative force as the written form of notarised authorizations.

Revocation of authorization

Article 63

Authorization shall be revoked by a statement of revocation of authorization, given in the same manner and under the same conditions as the registered authorization.

Maintenance, keeping and accessing the Register of authorizations

Article 64

- 1) The Register of authorizations does not constitute a public book.
- 2) The principals, authorised persons and relying parties only have access to the data contained in the Register of authorizations from Article 61 of this Law, which refer to the relevant authorizations related to them.

VII. SUPERVISION

Supervision of trust service providers and qualified trust service

Article 65

- 1) Supervision over the application of this law shall be performed by administrative servants in the Ministry of Information Society and Administration, upon prior authorization by the Minister of Information Society and Administration.
- 2) The authorised persons referred to in paragraph (2) of this Article shall supervise the fulfilment of the conditions determined by this Law and the regulations adopted for the implementation of this Law.
- 3) The Minister of Information Society and Administration shall prescribe the form and content of the minutes and the misdemeanour order.

Scope of authorization for performing supervision

Article 66

The persons referred to in Article 65 of this Law may:

- 1) order the removal of established irregularities and give a deadline within which the irregularities shall be removed;
- 2) order to prohibit the use of inadequate procedures and infrastructure, and give a deadline to the service provider in which it is obliged to provide adequate procedures and infrastructure;
- 3) temporarily prohibit the performance of services until the adequate procedures and infrastructure are provided by the qualified trust service providers;
- 4) order a temporary revocation of some or all of the certificates issued by the trust service provider, if there is a reasonable suspicion of inadequate procedure or forgery.

VIII. PENAL PROVISIONS

Article 67

(1) A penalty of 5,000 to 10,000 euro in denar equivalent shall be imposed to the provider of qualified trust service - legal person, if:

- 1) they fail to undertake the necessary technical and organizational measures to manage the risks that jeopardize the reliable and secure provision of trust services;
- 2) they fail to inform, without delay, and no later than 24 hours of becoming aware, the Ministry of Information Society and Administration of any security breaches or loss of

integrity of the services that have a significant impact on the provision of trust services or the protection of personal data processed within the provision of the service;

3) in the event of a security breach or loss of integrity of the services, they fail to inform, without delay, the user of the trust services, if there is a threat to the security or loss of integrity of the trust services or if it could adversely affect the trust services users;

4) they fail to inform, before concluding the agreement referred to in Article 28 paragraph (1), the person who submitted the request for qualified trust service provision about all important circumstances that affect the use of the service referred to in Article 28 paragraph (2);

5) they fail to fulfil the requirements in Article 29 of this Law;

6) when issuing a qualified certificate for a trust service, they fail to verify the identity information of the natural or legal person, contained in the qualified certificate, in accordance with Article 31 paragraph (2) of this Law;

7) they fail to assess the fulfilment of requirements before the beginning of the provision of qualified trust services, i.e., at least once in 24 months;

8) they are not registered in the Register of qualified trust service providers and electronic identification schemes before commencing the provision of qualified trust services;

9) a trust service provider, who intends to cease its activities, is obliged to notify each qualified trust service user and the Ministry of Information Society and Administration about the intention, at least three months before the intended cease of performance of the activities;

10) in case of the cease of performance of the activities, a qualified trust service provider fails to submit all necessary technical devices regarding the performance of services to another provider of qualified trust services to whom it transfers the obligation of performing one or more trust services;

11) in case of termination of the activity of a qualified trust service provider did not submit the complete documentation and equipment regarding the provision of services to another qualified trust service provider to whom it transfers the obligation to perform one or more trust services or to the Ministry of Information Society and Administration;

12) a qualified electronic signature or seal certificate do not contain all the data referred to in Article 47 paragraph (1) of this Law;

13) a provider of qualified trust services for issuing qualified electronic signature or seal certificates fails to revoke the issued certificates, in the cases referred to in Article 42 paragraph (1) of this Law;

14) a provider of qualified trust services for issuing of qualified electronic signature or seal certificates fails to inform the qualified trust service users about the revocation of the

certificate within 24 hours of the received notification, or of the occurrence of the circumstances for which the certificate is revoked;

15) a provider of qualified trust services for issuing of qualified electronic signature or seal certificates fails to preserve complete documentation on issued and revoked qualified electronic signature or seal certificates, as well as devices of electronic identification and verification in administrative, legal and other proceedings, at least ten years after the expiration of the certificate validity;

16) trustworthy electronic preservation and qualified electronic preservation of documents is not performed in accordance with Article 58 of this Law;

(2) For the misdemeanor referred to in paragraph (1) of this Article, the responsible person of a legal person – a qualified trust service provider shall be punished with a fine ranging from 1,000 to 5,000 euros in denar equivalent.

(3) With a fine ranging from 5,000 to 10,000 euros in denar equivalent shall be punished the provider of non-qualified trust services if it fails to notify the Ministry of Information Society and Administration on the performance of activity, in accordance with Article 24 of this Law.

(4) For the infringement referred to in paragraph (3) of this Article, the responsible person of a legal person – a non-qualified trust service provider shall be punished with a fine ranging from 1,000 to 5,000 euros in denar equivalent.

Article 68

1) A fine ranging from 1,000 to 5,000 euros in denar equivalent shall be imposed to the legal person - qualified trust service user, if in case of change of the data referred to in Article 31 paragraph (3) of this Law, it fails to notify, without delay, the qualified trust service provider.

2) A fine ranging from 500 to 1,000 euros in denar equivalent shall be imposed to the responsible person of a legal person - qualified trust service user for the misdemeanor referred to in paragraph (1) of this Article.

3) A fine ranging from 100 to 300 euros in denar equivalent shall be imposed to the natural person - qualified trust service user for the misdemeanor referred to in paragraph (1) of this Article.

Article 69

(1) A fine ranging from 1,000 to 5,000 euros in denar equivalent shall be imposed to the legal person who has registered an electronic identification scheme if:

1) the electronic identification scheme does not meet the requirements of Article 11 of this Law and

2) they fail to undertake the necessary technical and organizational measures to manage the risks that could jeopardize the reliable and secure provision of the services in accordance with Article 18 of this Law.

(2) For the misdemeanor referred to in paragraph (1) of this Article, the responsible person of a legal person shall be punished with a fine ranging from 500 to 1,000 euros in denar equivalent.

Article 70

- 1) A fine ranging from 7,000 to 15,000 euros in denar equivalent shall be imposed to the legal person – qualified trust services provider if they fail to act on the order of the authorised person for supervision within the deadline specified in Article 65 of this Law.
- 2) For the misdemeanor referred to in paragraph 1 of this Article, the responsible person of a legal person – qualified trust service provider shall be punished with a fine ranging from 1,000 to 5,000 euros in denar equivalent.

Article 71

- 1) A fine ranging from 7,000 to 15,000 euros in denar equivalent shall be imposed to the state authority if it fails to recognize the validity, or denies the probative force of an electronic document created in accordance with this Law, or a digitized document created in accordance with Article 10 of this Law, only because it was in electronic format.
- 2) A fine ranging from 1,000 to 5,000 euros in denar equivalent shall be imposed to the official who manages the state authority, or the responsible person of a legal person who performs public authorizations, if they deny the probative force of electronic documents or documents issued in accordance with this Law, only because they were issued or used in electronic format.

Article 72

- (1) For the misdemeanours determined by this Law, a competent court leads and conducts a misdemeanour procedure and sanction.

IX. TRANSITIONAL AND FINAL PROVISIONS

Article 73

The bylaws whose adoption is determined by this law shall be adopted within three months from the day this law enters into force.

Article 74

- (1) Electronic signatures, electronic seals and electronic time stamps issued until the day of commencement of the application of this law in accordance with the Law on Electronic Data Form and Electronic Signature, continue to be valid until the expiration of their validity.
- (2) The legal entities that perform activity until the day of starting the application of this law in accordance with the Law on Electronic Data Form and Electronic Signature, with the entry into force of this law shall continue to issue electronic signatures and shall provide services in accordance with the Law on Data in Electronic Form and Electronic Signature.

Article 75

(1)The providers of trust service, i.e., the issuers of certificates that perform activity on the basis of the Law on Electronic Data Form and Electronic Signature are obliged to harmonize their work with the provisions of this law no later than 1 September 2020.

(2)In the period until harmonization with the provisions of this law, the providers of trust service referred to in paragraph (1) of this Article, i.e., the issuers of certificates shall provide the services for issuance of certificates for electronic signatures, electronic seals and time stamps in accordance with the Law on Electronic Data Form and Electronic Signature.

(3) Trust service providers that perform activity on the basis of the Law on Data in Electronic Form and Electronic Signature, which will not harmonize their own work within one year from the day of enactment of the bylaws provided by this law, shall not be entered in the Register of Electronic Schemes identification and Trust Services.

Article 76

This Law ceases to be valid upon the accession of the Republic of North Macedonia in the European Union.

Article 77

With the day of the beginning of the application of this law, the Law on Data in Electronic Form and Electronic Signature ("Official Gazette of the Republic Macedonia“ No. 34/2001, 6/2002, 98/2008 and 33/15) ceases to be valid.

Article 78

This law shall enter into force on the day of its publication in the "Official Gazette of the Republic of North Macedonia", and it shall start to be applied from 1 September 2020, except for Chapter II. Electronic document, which shall start to be applied from 20 December 2019.