Law on electronic identification and electronic signature

The Law was published in the Official Gazette of Montenegro, No. 31/2017 and 72/2019.

I. BASIC PROVISION

Subject matter

Article 1

This Law shall regulate requirements for using electronic signature, electronic seal, electronic time stump and electronic registered delivery services in legal transactions, administrative, judicial and other proceedings and certification of website authentication, as well as the electronic identification scheme and requirements for recognition of other states' electronic identification means.

Electronic identification

Article 2

Electronic identification is the process of using identification data in electronic form uniquely representing a natural person, a legal person, or a state authority.

Electronic identification scheme is a system for issuing electronic identification means to natural persons, legal persons, state authorities or natural persons representing legal persons or state authorities.

Electronic identification means may be a data set, computer equipment (hardware) or computer program (software) containing data in electronic form or binding a natural person, a legal person or a state authority to these data, and which are used for authentication for a service in electronic form.

Electronic trust services

Article 3

In order to use electronic signature, electronic seal, electronic time stump and electronic registered delivery service in legal transactions, administrative, judicial and other proceedings and certificate of website authentication, a natural person, a legal person and a state authority rely on electronic trust service.

Electronic trust services are services that enable high level of confidence in exchange and processing of data in electronic form.

Electronic trust services are creation of certificate for electronic signature, electronic seal and website authentication; creation of electronic time stamp; electronic registered delivery service; electronic signature and electronic seal verification; preserving of electronic signatures and electronic seals or certificate that relate to these services.

Electronic trust services that meet special requirements stipulated by this law are qualified electronic trust services.

Electronic trust service providers

Article 4

Electronic trust services shall be provided by a natural or legal person that meets requirements for providing such services prescribed by this law (hereinafter: electronic trust service provider).

Qualified electronic trust services shall be provided by a natural or legal person that meets requirements prescribed by this law (hereinafter: qualified electronic trust service provider).

Electronic trust services and qualified electronic trust services for state administration authorities and for other public authorities when it is prescribed by law, shall be provided by the state administration authority responsible for electronic government and electronic business tasks (hereinafter: the Ministry).

Electronic trust services and qualified electronic trust services may be provided by other public authorities within tasks from their competence, in accordance with special law.

Availability of electronic trust services to persons with disability

Article 5

Electronic trust services, as well as computer equipment (hardware) or computer program (software) used during provision of these services shall be available to persons with disability whenever it is possible.

Personal data protection

Article 6

Regulations governing personal data protection shall apply to personal data processing. Using of pseudonyms in electronic transactions is not prohibited.

Use of gender sensitive language

Article 7

All terms used in this Law with reference to natural persons in masculine gender shall include the same terms in feminine gender.

Definitions

Article 8

Terms used in this Law shall have the following meanings:

1) **identification data** include a set of data in electronic form enabling the identity of a natural person or a legal person, or public authority to be established;;
2) **authentication** is an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed;
3) **relying party** is a natural, legal person or public authority that rely on electronic identification or electronic trust service;
4) **signatory** is a natural person signing on its behalf or on behalf of a natural or legal person by using data for electronic signature creation;
5) **electronic signature creation data** is unique data (codes or private cryptographic keys) which is used by the signatory to create an electronic signature;
6) **creator of a electronic seal** is a legal person or public authority who uses an electronic seal by using data for electronic signature creation seal;
7) **electronic seal creation data** is unique data, which is used by the creator of the electronic seal to create an electronic seal;
8) **certificate for electronic seal** is an electronic attestation that links electronic seal validation data to a legal person or a public authority and confirms the name of that legal person or public authority;
9) **qualified certificate** for electronic seal is a certificate for an electronic seal, that is issued by a qualified trust service provider;
10) **electronic seal creation device** is computer hardware or computer software used to create an electronic seal;
11) **qualified electronic seal creation device** is an electronic seal creation device that meets the special requirements laid down by this Law;
12) **electronic document** is a set of data that is electronically shaped, sent, received or stored on electronic, magnetic, optical or other media, which contains features used to identify creator, determine authenticity of content and prove inalterability of content in time, and includes all forms of written text, data, pictures, drawings, maps, sound, music, speech and the likes;
13) **validation data** is data that is used to validate an electronic signature or an electronic seal;
14) **validation** is the process of verifying and confirming that an electronic signature or an electronic seal is valid;
15) **public authority** is a state authority, state administration authority, local self-government authority or local government authority and a legal person that performs public function;
16) **domain** is a system where internet addresses are linked to certain location on the Internet.

II. ELECTRONIC SIGNATURE AND ELECTRONIC SEAL

Electronic signature

Article 9

Electronic signature is a set of data in electronic form which is attached to or logically associated with electronic document and which is used for signature and electronic identification of signatory.

Electronic signature is created by electronic signature creation device and it is based on certificate for electronic signature creation.

Advanced electronic signature

Article 10

Advanced electronic signature is electronic signature which reliably guarantees signature identity and electronic document integrity, and which meets requirements laid down by this Law.

Advanced electronic signature must:

1) be uniquely linked to the signatory;
2) unambiguously identify the signatory;
3) be created using electronic signature creation device that the signatory can manage autonomously and which is under his sole control;
4) contain direct association with the data it relates to, in such a way that unambiguously allows insight in any changed of original data.

Advanced electronic signature based on electronic certificate issued in the European Union Member State shall be recognised as advanced electronic signature in Montenegro, provided that requirements referred to in paragraph 2 of this Article are met.

Qualified electronic signature

Article 11

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 certificate for electronic signature.

Legal effect of electronic signature

Article 12

An electronic signature shall not be denied validity and admissibility solely on the grounds that:
1) it is in an electronic form;
2) it is not based on qualified certificate for electronic signature.

Legal effects of electronic signature and advanced electronic signature

Article 13

Public authority or legal person may not refuse to receive electronic document with electronic signature or advanced electronic signature solely on the grounds that it is in electronic form.

Legal effects of qualified electronic signature

Article 14

A qualified electronic signature shall have the equivalent legal effect of a handwritten signature, or a handwritten signature and a seal in relation to data in paper form, and it is admissible as evidence in proceedings before state authorities, state administration authorities, local self-government authorities and local government authorities, and legal persons that perform public functions.

Certificate for electronic signature

Article 15

Certificate for electronic signature is a document in electronic form signed by the electronic trust service provider, which binds data for verification of electronic signature to a person and confirms the identity of that person.

Qualified certificate for electronic signature

Article 16

A qualified certificate for electronic signature is a certificate issued by the qualified electronic trust service provider, or public authority referred to in paragraphs 3 and 4 of Article 4 of this Law and which shale include:
1) an indication that it is a qualified certificate for electronic signature, in a form suitable for automated data processing;
2) a set of identification data on legal person, natural person or public authority issuing a qualified certificate for electronic signature, including name of the state where that person or public authority is registered as a qualified provider of electronic trust services, and:
- for a legal person or public authority: name, identification number, or tax identification number;
- for a natural person: name and surname and tax identification number;
3) a set of identification data on signatory (the name and surname or a pseudonym) which, if is used, it shall be clearly indicated;
4) electronic signature validation data that corresponds to the electronic signature creation data and which is under control of signatory;
5) details of that certificate's period of validity;
6) the identity code of the qualified certificate for electronic signature, which must be unique for the qualified electronic trust service provider;
7) the advanced electronic signature of the issuing qualified electronic trust service provider;

8) the location where that certificate supporting the advanced electronic signature or advanced electronic seal of the qualified electronic trust service provider is available free of charge;

9) the location of the services that can be used to enquire about the validity of that certificate;

10) an appropriate indication in a form suitable for automated processing if the electronic signature creation data related to the electronic signature validation data is located in a qualified electronic signature creation device.

In addition to data referred to in paragraph 1 of this Article, a qualified certificate for electronic signature shall include the signatory's identification number determined by the state administration authority responsible for interior affairs.

In addition to data referred to in paragraph 1 of this Article, a qualified certificate for electronic signature may include other details on signatory if a signatory request it, and these details shall not affect the interoperability and recognition of qualified electronic signatures.

The Government of Montenegro shall regulate the manner of the identification number determination.

Losing validity of qualified certificate for electronic signature and temporary suspension

Article 17

A qualified electronic signature shall lose its validity if the qualified certificate for electronic signature on which it is based is revoked after activation, in accordance with Article 51, paragraph 1 of this Law, from the moment of revocation of the certificate.

In the case referred to in paragraph 1 of this Article, the electronic signature cannot be reactivated.

A qualified electronic signature shall lose its validity during the suspension of the qualified electronic signature certificate referred to in Article 51, paragraph 3 of this Law.

In the case referred to in paragraph 3 of this Article, the electronic signature may be reactivated, when it is determined that the requirements for revocation of the qualified certificate referred to in Article 51 paragraph 1 of this Law are not met.

Electronic signature creation device

Article 18

The electronic signature creation device is the appropriate computer equipment or computer program that is used when creating an electronic signature using electronic signature data creation.

Qualified electronic signature creation device

Article 19

A qualified electronic signature creation device is a device for creating qualified electronic signature, which meet special requirements laid down by this Law.

A qualified electronic signature creation device must ensure that:

1) the qualified electronic signature creation data can occur only once and that its security is realised;
2) the qualified electronic signature creation data may not be determined from that signature;
3) the qualified electronic signature is protected against forgery using currently available technology;
4) the qualified electronic signature creation data used for electronic signature creation can be reliably protected by the signatory against unauthorised use.

During qualified electronic signature creation, the qualified electronic signature creation device shall not alter the data to be signed or prevent such data from being presented to the signatory prior to the process of qualified electronic signature creation.

Provisions of paragraph 1 and 2 of this Article shall apply accordingly to the electronic signature creation device.

Generating electronic signature creation data

Article 20

Generating or managing electronic signature creation data on behalf of the signatory may only be done by a qualified electronic trust service provider.

A qualified electronic trust service provider may duplicate the electronic signature creation data only for back-up purposes provided the following requirements are met:

1) the security of the duplicated datasets for electronic signature creation must be at the same level as for the original datasets for electronic signature creation; and

2) the number of duplicated datasets for electronic signature creation shall not exceed the number needed to ensure continuity of the qualified electronic signature creation service.

Certification of qualified electronic signature creation device

Article 21

The compliance of qualified electronic signature creation devices with the requirements referred to in Article 19 of this Law shall be assessed by the Ministry.

The Ministry shall put qualified electronic signature creation devices that are determined to comply with the requirements referred to in Article 19 of this Law on the list of certified qualified electronic signature creation devices.

The Ministry may delete a qualified electronic signature creation device from the list referred to in paragraph 2 of this Article if it determines in accordance with paragraph 1 of this Article that it does not comply with the requirements of Article 19 of this Law.

The list referred to in paragraph 2 of this Article shall be published on the Ministry's website.

The manner of assessing compliance referred to in paragraph 1 of this Article, as well as the content of the list referred to in paragraph 2 of this Article, shall be prescribed by the Ministry.

Notification to European Commission

Article 22

The Ministry shall submit a notification to the European Commission on the competence to assess the compliance of qualified electronic signature creation devices referred to in Article 21 of this Law.

No later than 30 days from the assessment of the compliance of qualified electronic signature creation devices with the requirements referred to in Article 19 of this Law, the Ministry shall notify the European Commission thereof.

Requirements for validation of qualified electronic signature

Article 23

The validity of a qualified electronic signature shall be confirmed by verification of a qualified electronic signature, which includes the following determinations, that:

1) the certificate supporting the signature was, at the time of signing, a qualified certificate for electronic signature issued in accordance with this Law;

2) the qualified certificate for electronic signature was issued by a qualified electronic trust service provider and was valid at the time of signing;

3) the signature validation data corresponds to the data provided to the relying party;

4) the unique set of data representing the signatory in the qualified certificate for electronic signature is correctly provided to the relying party;

5) the use of any pseudonym is indicated to the relying party if a pseudonym was used at the time of signing;

6) the qualified electronic signature was created by a qualified electronic signature creation device;

7) the integrity of the signed data has not been compromised;

8) the requirements provided for in Article 10 of this Law were met at the time of signature creation.

Validation of the qualified electronic signature shall be conducted in a manner that provides to the relying party the correct result of the validation.

A qualified validation service for qualified electronic signatures may only be provided by a qualified electronic trust service provider who conducts validation in compliance with paragraph 1 of this Article and allows relying party to receive the result of the validation process in an automated manner, which is reliable.

Validation process results shall be signed by an advance electronic signature or advanced electronic seal of the validation service provider.

The Ministry shall prescribe the manner of conducting the qualified electronic signature validation.

Preservation service for qualified electronic signatures

Article 24

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

The Ministry shall prescribe the manner of providing preservation services for qualified electronic signatures.

Electronic, advanced electronic and qualified electronic seals

Article 25

An electronic seal is a set of data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity and is based on certificate for electronic seal.

An advanced electronic seal is an electronic seal, which meets the special requirements in accordance with

this Law.

A 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.

Electronic time stamp and qualified electronic time stamp

Article 26

An 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 time.

A qualified electronic time stamp is an electronic time stamp, which meets the special requirements as follows:

1) it binds the date and time to data in such a manner as to preclude any possibility of the data being changed;
2) it is based on an accurate time source linked to Coordinated Universal Time (UTC); and
3) it is signed using an advanced electronic signature or sealed with an advanced electronic seal of the qualified electronic trust service provider.

Application mutatis mutandis

Article 27

Provisions of Articles 10, 12, 13, 14 and Articles 16 through 24 of this Law shall apply mutatis mutandis to validity, admissibility and legal effects of electronic seal, electronic time stamp, qualified electronic seal and qualified electronic time stamp, requirements for qualified electronic seal, content and issuance of certificate for qualified electronic seal, loosing validity, revocation and temporary suspension of certificate for electronic seal and certificate for qualified electronic seal, requirements for qualified electronic seal creation devices, assessment of compliance of qualified electronic seal creation device, and validation and preservation of electronic seal.

III. ELECTRONIC REGISTERED DELIVERY SERVICE

Electronic registered delivery service

Article 28

Electronic registered delivery service is a service that makes it possible to transmit data by electronic means and provides evidence on the handling of the transmitted data, including proof of sending and receiving the data, which protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations.

Legal effects of electronic registered delivery service

Article 29

A natural person, a legal person or public authority may not refuse to receive data sent and received using an electronic registered delivery service solely on the grounds that it is in an electronic form or that it does not meet all the requirements of the qualified electronic registered delivery service.

Requirements for sending data using qualified electronic registered delivery service

Article 30

Data sent and received using a qualified electronic registered delivery service shall enjoy the presumption of:

1) integrity of the data;
2) sending of the data by the identified sender
3) receipt of the data by the identified addressee
4) the accuracy of the date and time of sending and receipt of the data indicated by the qualified electronic registered delivery service

Qualified electronic registered delivery service

Article 31

A qualified electronic registered delivery service is an electronic registered delivery service, which meets special requirements as follows:

1) they are provided by one or more qualified electronic trust service providers;
2) they ensure with a high level of confidence the identification of the sender;

3) they ensure the identification of the addressee before the delivery of the data;

4) the sending and receiving of data is secured by an advanced electronic signature or an advanced electronic seal of a qualified electronic trust service provider in such a manner as to preclude the possibility of the data being changed undetectably;

5) any change of the data needed for sending or receiving the data is clearly indicated to the sender and addressee of the data;

6) the date and time of sending, receiving and any change of data are verified by a qualified electronic time stamp.

In the event of the data being transferred between two or more qualified electronic trust service providers, the requirements referred to in paragraph 1 of this Article shall apply to all the qualified electronic trust service providers.

The Ministry shall prescribe more detailed requirements that must be met by qualified electronic trust service.

IV. WEBSITE AUTHENTICATION

Notion and certificates

Article 32

Website authentication is an electronic process that enables verification of the website data integrity and trustworthiness of using the website and it is based on a certificate for website authentication, or on qualified certificate for website authentication.

A certificate for website authentication is an attestation that makes it possible to authenticate a website and binds the website to the natural or legal person to whom the certificate is issued.

A qualified certificate for website authentication is a certificate for website authentication, which is issued by a qualified electronic trust service provider and meets the special requirements laid down by this Law.

Qualified certificate for website authentication

Article 33

A qualified certificate for website authentication must contain:

1) an indication mark that it is a qualified certificate for website authentication in electronic form suitable for automatic processing;

2) a set of identification data on a legal person, natural person or public authority issuing a qualified certificate for website authentication, stating the name of the country in which that person or public authority is registered as a qualified electronic trust service provider, and for:

- legal person, or public authority: name, identification number, i.e. tax identification number,
- natural person: name and surname and tax identification number;

3) a set of identification data on:

- legal person or public authority to which the certificate was issued: name, identification or tax identification number and registered office (at least name of the city and state),
- to the natural person to whom the certificate was issued: name and surname or pseudonym which, if used, must be clearly indicated and the address (at least name of the city and country);

4) the name of one or more domains managed by a natural person, legal person or public authority to which a certificate for website authentication has been issued;

5) data on the period of validity of the qualified certificate for website authentication;

6) the identity code of the issued qualified certificate for website authentication, which must be unique for the qualified electronic trust service provider;

7) the advanced electronic signature or advanced electronic seal of the qualified electronic trust service provider issuing the certificate;

8) the location where the certificate supporting the advanced electronic signature or advanced electronic seal of the qualified electronic trust service provider is available free of charge;

9) the location of the services that can be used to enquire as to the validity status of the qualified certificate for website authentication.

V. REQUIREMENTS FOR PROVISION OF QUALIFIED ELECTRONIC TRUST SERVICES

Requirements for qualified electronic trust service providers

Article 34

A qualified electronic trust service provider must meet the following conditions, namely that:

1) it has an up-to-date plan for termination of the provision of electronic trust service in order to ensure its continuity, which is adopted in accordance with the internal acts referred to in Article 37, paragraph 4 of this Law;

2) it ensures the personal data processing in accordance with the regulations on the personal data

protection;

3) it provides, in an appropriate manner and in accordance with this Law and internal acts referred to in Article 37, paragraph 4 of this Law, verification of the signatory's identity and, if necessary, other characteristics of natural and legal persons, to whom a qualified certificate for electronic signature or a qualified certificate for electronic seal;

4) it has employees with specialist knowledge, experience and professional qualifications necessary for the provision of electronic trust services, especially in relation to: skills at the management level, expertise in the application of electronic signature technologies and appropriate security procedures, personal data protection and administrative procedure application;

5) it uses trustworthy systems and products that are protected against unauthorised modification and ensure the technical and cryptographic security of the processes;

6) it takes measures against forgery of certificates, and in cases where it creates data for the electronic signature creation, guarantees the secrecy of the process of creating such data and delivers certificates to signatories in a secure manner;

7) it possesses financial resources for insurance against risk and liability for possible damage caused by the issuance of qualified certificates, in the amount that can cover the risk of damage and liability caused by the use of qualified certificates issued, if the signatory is not liable for the damage or concluded an insurance contract against risks and liability for this type of damage;

8) it has a system for storing all relevant data relating to qualified certificates for a certain period of time, especially for the purpose of providing these data from the records of qualified certificates for judicial and other legal proceedings, where this data can be stored electronically, in the manner allowing the verification of electronic signatures;

9) it uses trustworthy systems to store qualified certificates in a verifiable form so that:

- only authorised persons can make entries and changes to the data when providing electronic trust service,
- the data from the qualified certificate can be checked for authenticity,
- the data are publicly available in a fast and secure manner only in cases where the registered signatory consented,
- any technical change, which could violate the security requirements, is visible to a qualified electronic trust service provider.

The Ministry shall prescribe more detailed requirements referred to in paragraph 1 of this Article.

Provision of qualified electronic trust services for public authorities

Article 35

When the Ministry and the public authority referred to in Article 4, paragraph 4 of this Law perform qualified electronic trust services, they must meet the requirements referred to in Article 34, paragraph 1, items 1 to 6 and items 8 and 9 of this Law.

The fulfilment of the requirements referred to in paragraph 1 of this Article shall be determined by the Ministry.

The Ministry shall prescribe the manner of providing electronic trust services and qualified electronic trust services for state administration authorities.

Legal effects of qualified certificates issued in another state

Article 36

Qualified electronic trust services in Montenegro may also be provided by electronic trust service providers based in another country.

Qualified certificates issued by electronic trust service providers based in a country other than a Member State of the European Union have the same legal effect as qualified certificates issued in Montenegro, provided that:

1) the electronic trust service provider meets the requirements prescribed by this Law for the issuance of qualified certificates and is registered in the register of qualified electronic trust service providers in Montenegro or is registered in a Member State of the European Union;

2) a qualified electronic trust service provider registered in the register of qualified electronic trust service providers in Montenegro or registered in a Member State of the European Union guarantees such a qualified certificate;

3) they are in accordance with an international agreement concluded between Montenegro and another state or international organisation;

4) they are in accordance with an international agreement concluded between the European Union and a country that is not a Member State of the European Union or an international organisation;

5) the electronic trust service provider meets the requirements set by the regulations of the European Union for the issuance of qualified certificates and if it is registered in a Member State of the European Union;

Certificates of electronic trust service providers based in a Member State of the European Union, which do not meet the requirements for issuing a qualified certificate in accordance with this Law, have the same legal effect as certificates issued in Montenegro in accordance with this Law.

VI. RECORDS AND REGISTERS

Notification on starting electronic trust service provision

Article 37

Electronic trust services may be provided by an electronic trust service provider entered in the records of electronic trust service providers (hereinafter: records), kept by the Ministry.

Entry in the records shall be made on the basis of the notification on starting the electronic trust service provision, submitted by the electronic trust service provider to the Ministry, at least eight days before the day indicated in the notification as the day of starting the electronic trust service provision.

The electronic trust service provider shall submit a notification to the Ministry on changes in the provision of electronic trust services.

Along with the notifications referred to in paragraphs 1 and 3 of this Article, internal acts on the manner and procedures of providing electronic trust services, security system and technical infrastructure shall be attached.

Entry in records

Article 38

Entry in the records shall be realised immediately after submitting the notification on starting of the electronic trust service provision.

The records shall contain data on the electronic trust services provider who submitted the notification, namely: name and surname of a natural person, or name of a legal person, address and e-mail address, activity code and tax identification number, or unique identification number for the natural person, registration number from Central Register of Business Entities.

The records shall be kept in electronic form suitable for automatic processing and shall be available to the public on the Ministry's website.

The Ministry shall prescribe more detailed content and manner of keeping records.

Decision on meeting requirements for qualified electronic trust service provision

Article 39

An electronic trust service provider that is entered into records may submit a request for entry in the register of qualified electronic trust service providers (hereinafter: the register), kept by the Ministry.

Along the request referred to in paragraph 1 of this Article, the electronic trust service provider shall submit documentation proving that it meets the requirements referred to in Article 34 of this Law.

The Ministry shall issue a decision on meeting requirements for provision of qualified electronic trust services prescribed by this Law, based on the review of the attached documentation referred to in paragraph 1 of this Article and, if necessary, based on direct insight.

The decision referred to in paragraph 3 of this Article shall be issued within 15 days from the day submitting the correct request.

Entry in register

Article 40

The Ministry shall enter the applicant in the register, based on the decision establishing that the applicant for entry in the register meets the requirements of Article 34 of this Law, immediately after its adoption.

Electronic trust service providers established in another state shall be also entered in the register, at their request, if they meet the conditions referred to in Article 34 of this Law.

The register shall contain data on the qualified electronic trust service provider entered in the register, namely: name and surname of the natural person, or name of the legal person, address and e-mail address, activity code and tax identification number, or unique identification number for the natural person, registration number from the Central Register of Business Entities.

The register shall be kept in electronic form suitable for automatic data processing and be available to the public on the Ministry's website.

The Ministry shall sign the register with an advanced electronic signature.

The Ministry shall submit to the European Commission information on its competence to keep and publish the register, as well as on where the data on the register is published, certificates used for signing or sealing the register, as well as all its alterations.

The Ministry shall prescribe more detailed content and manner of keeping the register.

Deletion from register

Article 41

The qualified electronic trust service provider shall notify the Ministry about all changes related to the provision of qualified electronic trust services, as well as about the intention to stop providing those services.

After the notification referred to in paragraph 1 of this Article, where the Ministry should determine that the qualified electronic trust service provider does not meet the requirements of Article 34 of this Law, or ceases to provide electronic trust services, it shall delete that service provider from the register.

Deletion from the register may also be performed in other cases when it is determined that a qualified electronic trust service provider does not meet the requirements referred to in Article 34 of this Law.

Indication of entry in register in certificates

Article 42

A qualified electronic trust service provider that is entered into register may indicate this fact in the certificates it issues.

Use of the certification mark for EU electronic transactions

Article 43

Once entered in the register, a qualified electronic trust provider may use the EU certification mark to indicate qualified electronic trust services in a simple, recognisable and clear way.

VII. RIGHTS, OBLIGATIONS AND RESPONSIBILITIES OF SIGNATORIES, CREATORS OF ELECTRONIC SEAL AND ELECTRONIC TRUST SERVICE PROVIDERS

Issuance of certificates

Article 44

A qualified certificate may be issued to a legal person, natural person or public authority, at its request, based on established identity and other data on the legal person, natural person or public authority for which the qualified certificate is issued.

The right to choose electronic trust service provider

Article 45

A legal or natural person shall independently choose the electronic trust service provider.

A legal or natural person may use the electronic trust services of one or more electronic trust service providers.

A legal or natural person shall use an electronic signature, an electronic stamp and an electronic time stamp, i.e. electronic trust services based on a contract with a selected electronic trust service provider.

A legal or natural person may use the electronic trust services of an electronic trust service provider established in another state.

Obligation to preserve devices and data for creating electronic signature or electronic seal

Article 46

The signatory, i.e. the creator of the electronic seal shall carefully keep the devices for creation of electronic signature, i.e. electronic seal or electronic time stamp, as well as the data for creation of electronic signature, i.e. electronic seal or electronic time stamp from unauthorised access and use and to use them in accordance with this law.

No one without authorisation may access and use the devices for creating electronic signature, electronic seal or electronic time stamp, as well as data for creating an electronic signature, i.e. electronic seal or electronic time stamp.

Obligations of signatory and creator of electronic seal

Article 47

The signatory, i.e. the creator of the electronic seal hall submit to the electronic trust service provider all necessary data and information on changes that affect or may affect the accuracy of establishing his identity, immediately, and no later than within 48 hours of the change occurring.

The signatory, i.e. the creator of the electronic seal shall immediately request the revocation or suspension of the certificate issued to him in case of:

1) loss of or damage to the device for creating an electronic signature, i.e. electronic seal or electronic time stamp or loss of data for creating an electronic signature, i.e. electronic seal or electronic time stamp;

2) doubt of the confidentiality of data for the creation of an electronic signature, i.e. an electronic seal or electronic times stamp.

When the electronic signature certificate states that the signatory signs on behalf of another natural or legal person, the obligation to request the revocation or suspension of the certificate in the cases referred to in paragraph 2 of this Article shall also apply to that person.

Responsibility of signatory and creator of electronic seal

Article 48

The signatory, i.e. the creator of the electronic seal shall be liable for irregularities that have occurred due to non-fulfilment of obligations referred to in Articles 46 and 47 of this Law.

The signatory, i.e. the creator of the electronic seal shall not be liable for the irregularities referred to in paragraph 1 of this Article, if he proves that the injured party did not take or wrongly took actions related to validation of electronic signature, electronic seal or electronic time stamp.

Obligations of the electronic trust service provider

Article 49

The electronic trust service provider shall:

1) ensure that each qualified certificate contains the information referred to in Article 16 of this Law;
2) conduct a complete verification of the identity of a natural person, legal person, or public authority to which a qualified certificate is issued;
3) keep records of qualified certificates issued and ensure the accuracy and completeness of the data entered in those records;
4) enter basic data on his identity in each certificate and allow each interested person with insight into those data;
5) keep up-to-date, accurate and security-protected records on the validity of the certificate;
6) provide visible information on the exact date and time (hour and minute) of issuance, suspension, expiration of the term and revocation of the certificate, at least until the day of expiration of the validity period specified in the certificate;
7) preserve all data and documentation on issued, suspended, expired and revoked certificates for the purposes of proving and verification in judicial, administrative and other proceedings, for at least ten years from the termination of their validity, whereby data and accompanying documentation may be in electronic form;
8) apply the provisions of laws and other regulations governing the personal data protection.

A qualified electronic trust service provider shall perform the identity verification referred to in paragraph 1, item 2 of this Article by obtaining data on the basis of which verification is performed directly from a natural person or authorised representative of a legal person or authority or from another person.

The identity verification referred to in paragraph 1 item 2 of this Article shall be performed in one of the following ways:

1) in the physical presence of a natural person or an authorised representative of a legal person or public authority;
2) remotely, using electronic identification means, 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 or public authority was ensured and if the electronic identification scheme out of which these means were issued meets the requirements set out in Article 60 of this Law with regard to the security levels 'substantial' or 'high';
3) by means of a certificate of a qualified electronic signature or of a qualified electronic seal issued with verification in the manner referred to in items 1 and 2 of this paragraph; or
4) by using other identification methods, which with regard to trustworthiness provide security of identity verification equal to identity verification, based on physical presence.

Prior to the application of the method referred to in paragraph 3, item 4 of this Article, the qualified electronic trust service provider shall obtain the consent of the Ministry for the application of that method.

The electronic trust service provider determines the prices of electronic trust services, with the prior consent of the Ministry.

Providing information to applicants

Article 50

The electronic trust service provider, before concluding the contract referred to in Article 45, paragraph 3 of

this Law, must notify the legal or natural person who submitted the request for the issuance of the certificate of all important circumstances for its use.

The notification referred to in paragraph 1 of this Article must contain:

1) excerpt from valid regulations and internal acts referred to in Article 37, paragraph 4 of this Law;
2) information on possible restrictions related to the use of the certificate;
3) information on appropriate legal protection or out-of-court settlement, if the service provider agrees to it in the event of a dispute;
4) data on the measures to be implemented by the signatories, i.e. the creators of the electronic seal and on the technology required for the secure production and verification of the electronic signature.

Certificate revocation and suspension

Article 51

The electronic trust service provider shall revoke the certificate in the event that:

1) revocation of the certificate is requested by the signatory, i.e. the creator of the electronic seal or his authorised representative;
2) it determines that the data in the certificate is incorrect or the certificate was issued on the basis of incorrect data;
3) it receives notification that the signatory or the legal or natural person on whose behalf he is signing has lost their legal capacity, died or ceased to exist, or the validity of the authorisation for signing has expired or the facts affecting the validity of the certificate have changed;
4) it determines that the electronic signature creation data or the information system of the signatory are compromised in a way that affects the trustworthiness and security of the electronic signature creation or when a third party uses that data in an inappropriate manner;
5) it determines that the electronic signature verification data or the information system of the electronic trust service provider are compromised in a way that affects the security and trustworthiness of the certificate;
6) it ceases to operate or is prohibited from operating, and the validity of the certificates issued has not expired, unless the electronic trust services are transferred to another provider of those services;
7) the validity period of the certificate expires;
8) it receives a court decision or administrative act relating to the validity of the certificate or
9) there are other legal reasons laid down by internal acts referred to in Article 37, paragraph 4 of this Law.

The electronic trust service provider shall publish a list of revoked certificates on its website, and the revocation of certificates takes effect from the moment of publication of this list.

If the facts referred to in paragraph 1 of this Article cannot be immediately established in an unequivocal manner, the electronic trust service provider shall suspend the certificate without delay until those facts are established.

The date and time of suspension and revocation of the certificate shall be entered in the records referred to in Article 49, paragraph 1, item 5 of this Law.

The electronic trust service provider shall inform the signatory, i.e. the creator of the electronic seal about the suspension or revocation of the certificate, within 24 hours from the received request or notification, i.e. the occurrence of the circumstances referred to in paragraph 1 of this Article.

Certificate protection measures

Article 52

The electronic trust service provider shall:

1) apply organisational and technical measures for the protection of certificates and data related to signatories and creators of electronic seals;
2) establish and apply a system of protection of access to records of certificates and revoked and suspended certificates which will enable access only to authorised persons and which provides verification of the accuracy of data transfer and timely insight into possible errors of technical means.

The Ministry shall prescribe measures and activities referred to in paragraph 1 of this Article.

Obligations of electronic trust service provider in case of contract termination

Article 53

In the event that the electronic trust service provider, due to possible bankruptcy or the need or intention to terminate the business, terminates the contract referred to in Article 45 paragraph 3 of this Law, it shall notify the signatory or creator of the electronic seal and the Ministry at least three months before the date scheduled to terminate the contract.

The electronic trust service provider shall ensure the continuation of electronic trust services for signatories, i.e. creators of electronic seals to whom it has issued certificates with another service provider to whom it shall submit complete documentation related to the provision of electronic trust services, and shall notify signatories i.e. creators of electronic seals on electronic trust services with another electronic trust service provider.

If the electronic trust service provider should not ensure the continuation of these services with another

electronic trust service provider, it shall revoke all issued certificates and immediately, but no later than within 48 hours, notify the Ministry and submit complete documentation regarding the electronic trust services provided.

The Ministry shall immediately revoke all certificates issued by the electronic trust service provider, which for any reason did not revoke the issued certificates, at the expense of the electronic trust service provider.

Obligation to link records

Article 54

The electronic trust service provider shall enable the connectivity of its records of issued and records of revoked and suspended certificates with other electronic trust services providers applying available information technology and using of technical and software means whose operation is in accordance with applicable international standards.

Liability risk insurance

Article 55

A qualified electronic trust service provider shall insure the risk of liability for damages resulting from the provision of electronic trust services.

The minimum amount of insurance referred to in paragraph 1 of this Article shall be determined by the Ministry.

Liability for damage

Article 56

An electronic trust provider that issues qualified certificates or guarantees qualified certificates of another electronic trust service provider shall be liable for damage caused to a person who has trusted that certificate, if:

1) the information contained in the qualified certificate is not correct at the time of its issuance;

2) the certificate does not contain all the elements prescribed for a qualified certificate;

3) it has not ensured that the signatory, i.e. the creator of the electronic seal at the time of issuing the certificate possesses data for creating an electronic signature, i.e. an electronic seal corresponding to the data for verifying an electronic signature or electronic seal given or identified in the certificate;

4) it does not ensure that the data for the creation and data for the verification of the electronic signature, i.e. the electronic seal can be used complementary, in the case when these data are created by the electronic trust service provider;

5) it fails to revoke the certificate in accordance with Article 51 of this Law;

6) the certificate does not contain information on restrictions related to use.

The electronic trust service provider shall not be liable for the damage referred to in paragraph 1 of this Article, if he proves before a court or other competent authority that he acted with the care of a good businessperson.

The electronic trust service providers shall not be liable for damage caused by the use of the certificate beyond the restrictions, if these restrictions are clearly indicated in the certificate.

The electronic trust service provider shall be liable for the damage caused to the signatory, i.e. the creator of the electronic seal or a conscientious third party due to deficiencies or delays in providing insight into the data on the validity, expiration or suspension of the certificate.

Collection and processing of personal data

Article 57

The electronic trust service provider may collect personal data necessary for the issuance and maintenance of the certificate, directly from the signatory or indirectly with his explicit consent.

Data collected in accordance with paragraph 1 of this Article may not be processed or used for other purposes without the expressed consent of the signatory.

At the request of the signatory, the electronic trust service provider may enter in the certificate his pseudonym instead of the full name of the signatory, after verifying his identity.

The electronic trust service provider shall provide data on the identity of the signatory to the state body authorised by law to collect and process them, at its request.

The electronic trust service provider may collect the data referred to in paragraph 1 of this Article directly or by subcontracting other natural or legal persons.

Risk management

Article 58

Electronic trust service providers shall manage risks and take measures to increase security level.

The electronic trust service provider shall notify the Ministry of security breaches or loss of integrity that affect the electronic trust service, no later than within 24 hours of learning of such breach or loss of

integrity.

In the event that a breach of security and loss of integrity adversely affects a natural or legal person to whom electronic trust services have been provided, the electronic trust service provider shall notify that natural or legal person.

In the event that the breach of security or loss of integrity referred to in paragraph 2 of this Article concerns two or more Member States of the European Union, the Ministry shall notify the supervisory authorities in other Member States concerned and the European Network and Information Security Agency (ENISA).

The Ministry shall inform the public or require electronic trust service providers to do so if it determines that the detection of a breach of security or loss of integrity referred to in paragraph 2 of this Article is in the public interest.

The Ministry shall submit once a year a report on the security breaches and loss of integrity referred to in paragraph 2 of this Article received from the electronic trust service providers to the European Network and Information Security Agency (ENISA).

VIII. ELECTRONIC IDENTIFICATION

Electronic identification scheme management

Article 59

Electronic identification schemes are managed by natural and legal persons, as well as the public authority referred to in Article 4 paragraphs 3 and 4 of this Law, within which means of electronic identification are issued.

Assurance level of electronic identification scheme

Article 60

An electronic identification scheme may have a low, significant or high assurance level that also applies to electronic identification means.

The assurance levels referred to in paragraph 1 of this Article are the following:

1) an assurance level "low" that guarantees a limited degree of trustworthiness of the electronic identification means in relation to the requested or established identity of a person;

2) an assurance level "substantial" that guarantees a significant degree of trustworthiness of the electronic identification means in relation to the requested or established identity of a person;

3) an assurance level "high" that guarantees a high degree of trustworthiness of the electronic identification means in relation to the requested or established identity of a person.

The assurance levels referred to in paragraph 2 of this Article include references to technical specifications, standards and accompanying procedures, as well as technical controls aimed at reducing the risk of misuse or change of identity.

The Ministry shall determine assurance levels referred to in paragraph 2 of this Article in relation to the minimum technical standards and accompanying procedures.

The Ministry shall prescribe the minimum technical standards and accompanying procedures.

Requirements relating to electronic identification scheme

Article 60a

The electronic identification scheme must meet the following conditions:

1) the electronic identification scheme and electronic identification means issued within that scheme meet the requirements of at least one of the assurance levels referred to in Article 60, paragraph 2 of this Law;

2) a natural person, legal person, i.e. public authority issuing electronic identification means ensures that the identification data on the basis of which electronic identification means are issued unambiguously represent a natural person, legal person, i.e. public authority to which the means is issued, at the time of issuance, in accordance with the technical standards and procedures referred to in Article 60 paragraph 3 of this Law for the appropriate assurance level;

3) the natural person, legal person or public authority issuing the electronic identification means shall ensure that these means are issued to the natural person, legal person or public authority on the basis of whose identification data the means was issued, in accordance with technical standards and procedures referred to in Article 60. paragraph 3 of this law for the appropriate assurance level and

4) the electronic identification scheme meets the technical and operational requirements referred to in Article 61, paragraph 1 of this Law.

The compliance with the requirements referred to in paragraph 1 of this Article shall be determined by the Ministry.

Register of electronic identification schemes

Article 60b

An electronic identification scheme that meets the requirements referred to in Article 60a of this Law shall be entered in the register of electronic identification schemes.

The register of electronic identification schemes shall contain:

1) description of a electronic identification scheme,
2) the assurance level of the electronic identification scheme and electronic identification means issued within that scheme,
3) data on the natural person, legal person, i.e. public authority that manages the electronic identification scheme as follows:

- for legal person, i.e. public authority: name, identification number, i.e. tax identification number;
- for natural person: name and surname and tax identification number;

4) date of entry of the electronic identification scheme, as well as changes and deletions from the register.

The Ministry shall keep the register of electronic identification schemes.

The register shall be kept in an electronic form suitable for automatic processing and is available to the public on the Ministry's website.

The register is signed by the Ministry with an advanced electronic signature.

Interoperability

Article 61

Electronic identification schemes entered in the register of electronic identification schemes must meet the minimum technical standards and procedures referred to in Article 60 paragraph 3 of this Law and the technical and operational requirements relating to the node, node operator and relying party identity data, and the process of establishing interoperability framework.

The node is the place of connection of the electronic identification scheme, which is part of the interoperability structure of the electronic identification schemes and has the ability to recognise and process, i.e. to forward data transmission to other nodes and to connect to electronic identification schemes of other states.

The node shall be established and managed by the Ministry.

The technical and operational requirements relating to the node, node operator and relying party identity data, and the process of establishing the interoperability framework shall be prescribed by the Ministry.

Cooperation

Article 62

The Ministry shall cooperate with the Member States of the European Union with regard to the following:

1) interoperability of electronic identification schemes entered in the register of electronic identification schemes;
2) security of the electronic identification schemes.

The cooperation referred to in paragraph 1 of this Article shall include:

1) the exchange of information, experience and good practice as regards electronic identification schemes and in particular technical requirements related to interoperability and security levels related to electronic identification schemes;
2) the exchange of information, experience and good practice as regards working with security levels of electronic identification schemes;
3) the exchange of information on conformity assessment of electronic identification schemes.

Recognition of electronic identification certificates and means

Article 63

Qualified certificates issued by electronic trust service providers based in one of the Member States of the European Union have the same legal effect as qualified certificates issued in Montenegro.

Where a public authority requires electronic identification for a service it provides online by means of electronic identification and authentication in order to access that service, in accordance with regulations, electronic identification means issued in a Member State of the European Union shall be recognised for cross-border authentication purpose if:

1) the electronic identification means is issued within the electronic identification scheme which is placed on the list of notified electronic identification schemes published by the European Commission;
2) the assurance level of electronic identification means corresponds to the assurance level equal to or higher than the assurance level required by the public authority for access to that service on the Internet;
3) the public authority applies a significant or high assurance level in relation to access to that service on the

Internet.

Notification to European Commission

Article 64

The Ministry shall provide the European Commission with the following information and, without delay, any subsequent changes to that information relating to:

1) description of the electronic identification scheme and its level of security, data on the natural and legal person, i.e. the public authority referred to in Article 4, paragraph 3 and 4 of this Law, which issues electronic identification means;

2) the valid system of supervision and information on the rules and responsibilities of the natural and legal person, i.e. the public authority referred to in Article 4, paragraphs 3 and 4 of this Law, which issues electronic identification means, i.e. conducts the authentication procedure;

3) natural and legal person, i.e. public authority referred to in Article 4 paragraphs 3 and 4 of this Law which manages the registration of unique personal identification data;

4) the description of the manner of meeting the technical and operational requirements related to the interoperability framework referred to in Article 61, paragraph 4 of this Law;

5) the description of authentication referred to in Article 65, paragraph 1, item 6 of this Law;

6) the certificate suspension or revocation.

The Ministry may submit a request to the European Commission for deletion of the electronic identification scheme entered in the register of electronic identification schemes from the list of notified schemes published by the European Commission.

Elegibility of electronic identification scheme

Article 65

The electronic identification scheme is eligible for notification referred to in Article 64 of this Law if:

1) the electronic identification means are recognised by a Member State of the European Union;

2) electronic identification means may be used to access any service provided by a public authority which requires electronic identification in a Member State of the European Union;

3) the electronic identification scheme and electronic identification means issued within that scheme meet the requirements of any level of security referred to in Article 60 of this Law;

4) the Ministry ensures that personal identification data, in accordance with technical specifications, standards and procedures for the appropriate level of security referred to in Article 60 of this Law, are attributed to a natural or legal person using personal identification data in electronic form at the time electronic identification means are issued within that scheme;

5) the electronic identification service provider issuing electronic identification means within that scheme ensures that electronic identification means are attributed to a natural or legal person who uses personal identification data in electronic form in accordance with the appropriate level of security referred to in Article 60 of this Law;

6) the Ministry ensures the availability of online authentication, so that the interested party can confirm the personal identification data received in electronic form.

Security breach

Article 66

Where either the electronic identification scheme of a electronic identification service provider that is entered in the register of electronic identification schemes, or authentication referred to in Article 65 paragraph 1 item 6 of this Law is breached or partly compromised in a manner that affects the reliability of the cross-border authentication of that scheme, the Ministry shall, without delay, suspend or revoke that cross-border authentication or the compromised parts concerned, and shall inform Member States of the European Union and the European Commission.

When the breach or compromise referred to in paragraph 1 of this Article is remedied, the Ministry shall re-establish the cross-border authentication and shall inform Member States of the European Union and the European Commission.

If the breach or compromise referred to in paragraph 1 of this Article is not remedied within three months of the suspension or revocation, the Ministry shall notify Member States of the European Union and the European Commission of the withdrawal of the electronic identification scheme.

Liability

Article 67

The Ministry shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligations in a cross-border transaction under Article 65 paragraph 1 items 4 and 6 of this Law.

An electronic identification service provider issuing electronic identification means shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligations in a cross-border transaction under Article 65 paragraph 1 item 5 of this Law

An electronic identification service provider operating the authentication procedure shall be liable for damage

caused intentionally or negligently to any natural or legal person due to a failure to ensure the correct operation of the authentication referred to in Article 7 paragraph 1 item 6 in a cross-border transaction.

IX. SUPERVISION

Administrative and inspection supervision

Article 68

Administrative supervision over the implementation of this law shall be performed by the Ministry.

Inspection supervision over the work of electronic trust service providers and qualified electronic trust service providers and compliance of the electronic identification schemes shall be performed by the Information Society Inspectorate, in accordance with the law governing inspection supervision and this Law.

Obligations of information society inspectorate

Article 69

The Information Society Inspectorate shall submit to the Ministry a report on activities within its competence by March 1 of the current year for the previous calendar year.

X. PENAL PROVISIONS

Article 70

A legal person shall be fined with €1,000 to €10,000 for misdemeanour if it:

1) does not have an up-to-date plan for termination of the provision of electronic trust service in order to ensure its continuity, which is adopted in accordance with the internal acts referred to in Article 37, paragraph 4 of this Law (Article 34 paragraph 1 item 1);

2) fails to ensure the processing of personal data in accordance with the regulations on personal data protection (Article 34 paragraph 1 item 2);

3) fails to provide, in an appropriate manner and in accordance with this Law and internal acts referred to in Article 37, paragraph 4 of this Law, verification of the signatory's identity and, if necessary, other characteristics of natural and legal persons, to whom a qualified electronic signature certificate, i.e. qualified electronic seal certificate is issued (Article 34 paragraph 1 item 3);

4) has no employees with specialist knowledge, experience and professional qualifications necessary for the provision of electronic trust services, especially in relation to: skills at the management level, expertise in the application of electronic signature technologies and appropriate security procedures, personal data protection and administrative procedure application (Article 34 paragraph 1 item 4);

5) does not use trustworthy systems and products that are protected against unauthorised modification and ensure the technical and cryptographic security of the processes (Article 34 paragraph 1 item 5);

6) does not take measures against forgery of certificates, and in cases where it creates data for the electronic signature creation, guarantees the secrecy of the process of creating such data and delivers certificates to signatories in a secure manner (Article 34 paragraph 1 item 6);

7) does not possess financial resources for insurance against risk and liability for possible damage caused by the issuance of qualified certificates, in the amount that can cover the risk of damage and liability caused by the use of qualified certificates issued, if the signatory is not liable for the damage or concluded an insurance contract against risks and liability for this type of damage (Article 34, paragraph 1 item 7);

8) does not have a system for storing all relevant data relating to qualified certificates for a certain period of time, especially for the purpose of providing these data from the records of qualified certificates for judicial and other legal proceedings, where this data can be stored electronically, in the manner allowing the verification of electronic signatures (Article 34, paragraph 1 item 8);

9) use trustworthy systems to store qualified certificates in a verifiable form so that only authorised persons can make entries and changes to the data when providing electronic trust service, the data from the qualified certificate can be checked for authenticity, the data are publicly available in a fast and secure manner only in cases where the registered signatory consented, and that any technical change, which could violate the security requirements, is visible to a qualified electronic trust service provider (Article 34, paragraph 1 item 9);

10) fails to submit to the Ministry a notification on changes in the provision of electronic trust services (Article 37, paragraph 3);

11) fails to conduct a complete verification of the identity of a natural person, legal person, or public authority to which a qualified certificate is issued (Article 49 paragraph 1 item 2);

12) fails to keep records of qualified certificates issued and fails to ensure the accuracy and completeness of the data entered in those records (Article 49 paragraph 1 item 3);

13) fails to keep up-to-date, accurate and security-protected records on the validity of the certificate (Article 49 paragraph 1 item 5);

14) fails to notify the legal or natural person who submitted the request for the issuance of the certificate of all important circumstances for its use, before concluding the contract referred to in Article 45, paragraph 3 of this Law (Article 50);

15) fails to revoke the certificate as requested by the signatory, i.e. the creator of the electronic seal or his

authorised representative (Article 51 paragraph 1 item 1);

16) fails to revoke the certificate when it determines that the data in the certificate is incorrect or the certificate was issued on the basis of incorrect data (Article 51 paragraph 1 item 2);

17) fails to revoke the certificate when it receives notification that the signatory or the legal or natural person on whose behalf he is signing has lost his legal capacity, died or ceased to exist, or the validity of the authorisation for signing has expired or the facts affecting the validity of the certificate have changed (Article 51 paragraph 1 item 3);

18) fails to revoke the certificate when it determines that the electronic signature creation data or the information system of the signatory is compromised in a way that affects the trustworthiness and security of the electronic signature creation or when a third party uses that data in an inappropriate manner (Article 51 paragraph 1 item 4);

19) fails to revoke the certificate when it determines that the electronic signature verification data or the information system of the electronic trust service provider are compromised in a way that affects the security and trustworthiness of the certificate (Article 51 paragraph 1 item 5);

20) fails to revoke the certificate when it ceases to operate or is prohibited from operating, and the validity of the certificates issued has not expired, unless the electronic trust services are transferred to another provider of those services (Article 51 paragraph 1 item 6);

21) fails to revoke the certificate when the validity period of the certificate expires (Article 51 paragraph 1 item 7);

22) fails to revoke the certificate when it receives a court decision or administrative act relating to the validity of the certificate (Article 51 paragraph 1 item 8);

23) fails to revoke the certificate when there are other legal reasons set forth by internal acts referred to in Article 37, paragraph 4 of this Law (Article 51 paragraph 1 item 9);

24) fails to publish a list of revoked certificates on its website (Article 51 paragraph 2);

25) fails to suspend the certificate without delay if the facts referred to in Article 51 paragraph 1 cannot be immediately established in an unequivocal manner (Article 51 paragraph 3);

26) fails to inform the signatory, i.e. the creator of the electronic seal about the suspension or revocation of the certificate, within 24 hours from the received request or notification, i.e. the occurrence of the circumstances due to which the certificate is being revoked or suspended (Article 51 paragraph 5);

27) fails to apply organisational and technical measures for the protection of certificates and data related to signatories and creators of electronic seals (Article 52 paragraph 1 item 1);

28) fails to establish and apply a system of protection of access to records of certificates and revoked and suspended certificates which will enable access only to authorised persons and which provides verification of the accuracy of data transfer and timely insight into possible errors of technical means (Article 52 paragraph 1 item 2);

29) fails to notify the signatory or creator of the electronic seal and the Ministry, at least three months before the date scheduled to terminate the contract, that it terminates the contract referred to in Article 45 paragraph 3 of this Law due to possible bankruptcy or the need or intention to terminate the business (Article 53 paragraph 1);

30) fails to ensure the continuation of electronic trust services for signatories, i.e. creators of electronic seals to whom it has issued certificates with another service provider to whom it shall submit complete documentation related to the provision of electronic trust services, and fails to notify signatories i.e. creators of electronic seals on electronic trust services with another electronic trust service provider (Article 53 paragraph 2);

31) fails to revoke all issued certificates and to notify the Ministry immediately, but no later than within 48 hours, and to submit complete documentation regarding the electronic trust services provided if it fails to ensure the continuation of these services with another electronic trust service provider, (Article 53 paragraph 3);

32) fails to enable the connectivity of its records of issued certificates and records of revoked and suspended certificates with other electronic trust services providers applying available information technology and using of technical and software means whose operation is in accordance with applicable international standards (Article 54);

33) fails to insure the risk of liability for damages resulting from the provision of electronic trust services (Article 55 paragraph 1);

34) fails to provide data on the identity of the signatory to the state body authorised by law to collect and process them, at its request (Article 57 paragraph 4).

For the misdemeanour referred to in paragraph 1 of this Article, the responsible person in the legal person shall also be fined in the amount of €150 to €2,000.

For the misdemeanour referred to in paragraph 1 of this Article, the responsible person in the public authority shall be fined in the amount of €150 to €2,000.

For the misdemeanour referred to in paragraph 1 of this Article, a natural person shall be fined in the amount of €150 to €1000.

Article 71

A legal person shall be fined with €500 to €5,000 for misdemeanour if:

1) it refuses to receive electronic document with electronic signature or advanced electronic signature solely on the grounds that it is in electronic form (Article 13);

2) it refuses to receive data sent and received using an electronic registered delivery service solely on the grounds that it is in an electronic form or that it does not meet all the requirements of the qualified electronic (Article 29).

For the misdemeanour referred to in paragraph 1 of this Article, the responsible person in the legal person shall also be fined in the amount of €30 to €2,000.

For the misdemeanour referred to in paragraph 1 of this Article, the responsible person in the public authority shall also be fined in the amount of €30 to €2,000.

Article 72

A legal person shall be fined with €500 to €5,000 for misdemeanour if:

1) it fails to carefully keep the devices for creation of electronic signature, i.e. electronic seal or electronic time stamp, as well as the data for creation of electronic signature, i.e. electronic seal or electronic time stamp from unauthorised access and use and to use them in accordance with this Law (Article 46 paragraph 1);

2) it without authorisation accesses and uses devices for creating electronic signature, electronic seal or electronic time stamp, as well as data for creating an electronic signature, i.e. electronic seal or electronic time stamp (Article 46 paragraph 2);

3) it fails to submit to the electronic trust service provider all necessary data and information on changes that affect or may affect the accuracy of establishing his identity, immediately, and no later than within 48 hours of the change occurring (Article 47 paragraph 1);

4) it fails to immediately request the revocation or suspension of the certificate issued to him in case of loss of or damage to the device for creating an electronic signature, i.e. electronic seal or electronic time stamp or loss of data for creating an electronic signature, i.e. electronic seal or electronic time stamp (Article 47 paragraph 2 item 1);

5) it fails to request immediately the revocation or suspension of the certificate issued to him in case when in doubt of the confidentiality of data for the creation of an electronic signature, i.e. an electronic seal or an electronic time stamp (Article 47 paragraph 2 item 2).

For the misdemeanour referred to in paragraph 1 of this Article, the responsible person in the legal person shall also be fined in the amount of €30 to €2,000.

For the misdemeanour referred to in paragraph 1 of this Article, a natural person shall be fined in the amount of €30 to €2,000.

XI. TRANSITIONAL AND FINAL PROVISIONS

Article 73

Secondary legislation for implementation of this Law shall be adopted within 12 months from the date of entry into force of this Law.

Article 73a

Secondary legislation adopted on the basis of the Law on Electronic Identification and Electronic Signature (Official Gazette of Montenegro, No. 31/17) shall be harmonised with this Law within 12 months from the day this Law enters into force.

Article 74

Provisions of Article 10 paragraph 3, Articles 22, 36, Article 40 paragraph 2 and 6, Article 43, Article 45 paragraph 4, Article 58 paragraph 4 and 6, and Articles 62 to 67 of this Law shall apply from the day of Montenegro's accession to the European Union.

Article 75

On the day this Law enters into force, the Law on Electronic Signature (Official Gazette of Republic of Montenegro No. 55/03 and Official Gazette of Montenegro, No. 41/10 and 40/11) shall be repealed.

Article 75a

Qualified electronic signature certificates and devices for creating an electronic signature, which are based on a qualified electronic signature certificate, issued before the date of entry into force of this Law shall be considered qualified electronic signature certificates, i.e. qualified devices for creating an electronic signature in accordance with this Law, until the expiry date of those certificates.

Article 76

This Law shall enter into force on the eighth day from the day of its publication in the Official Gazette of Montenegro.