LAW OF GEORGIA

ON ELECTRONIC DOCUMENTS AND ELECTRONIC TRUST SERVICES

Article 1 - Purpose and scope of the Law

1. This Law sets forth the legal grounds for using electronic documents, electronic signatures and electronic trust services.

2. This Law shall not restrict the right of natural persons and legal entities under private law to use tangible documents and/or handwritten signatures according to their choice, as well as electronic documents and/or electronic signatures, made according to convetions that are different from this Law.

3. This Law shall not restrict the right of the National Bank of Georgia and the representatives of the financial sector to use electronic documents and/or electronic signatures, made according to conventions that are different from this Law.

4. This Law shall not apply to information that is recognised as a state secret by the legislation of Georgia and is subject to state protection.

Article 2 - Definition of terms

The terms used in this Law shall have the following meanings:

a) electronic document - a set of textual, audible, visual or audio-visual information and/or data stored in an electronic form;

b) tangible document - a set of information and/or data on paper or in any other tangible form;

c) signatory - a natural person, who uses an electronic signature to sign an electronic document in accordance with the requirements of this Law;

d) creator of a seal - a legal entity, who puts an electronic seal on an electronic document; for the purposes of this Law, 'legal entity' shall also include administrative bodies, apartment owners' associations, non-registered unions and partnerships;

e) electronic signature - a set of electronic data that is attached to or logically linked with an electronic document and is used for signing the electronic document;

f) electronic seal - a set of electronic data that is attached to or logically linked with an electronic document and is used for verifying the integrity and origin of the electronic document;

g) electronic signature/electronic seal validation data - data that is used for verifying electronic signatures/electronic seals;

h) electronic signature/electronic seal creation data - unique data that were used by a signatory/creator of a seal to create an electronic signature/electronic seal;

i) electronic signature/electronic seal creation device - a set of software and/or hardware devices that are used for creating an electronic signature/electronic seal;

j) certificate for electronic signature/electronic seal - a unique electronic document that links electronic signature/electronic seal validation data with a signatory/creator of a seal and contains at least the name and/or the pseudonym of a signatory/the full name and the identification code (if any) of a creator of a seal;

k) advanced electronic signature - an electronic signature that meets the following requirements:

k.a) it is exclusively linked to the signatory;

k.b) it can be used to identify the signatory;

k.c) it is created by means of electronic signature creation data that may be used by the signatory with sole control and with a high level of confidence;

k.d) it is attached to the signed data in a manner which enables the detection of any subsequent amendments made to them;

l) qualified electronic signature - an advanced electronic signature that is created by using an electronic signature creation device, on the basis of a certificate for qualified electronic signature;

m) advanced electronic seal - an electronic seal that meets the following requirements:

m.a) it is exclusively linked to the creator of a seal;

m.b) it can be used to identify the creator of a seal;

m.c) it is created by means of electronic seal creation data that may be used by the creator of a seal with sole control and with a high level of confidence;

m.d) it is attached to the sealed data in a manner which enables the detection of any subsequent amendments made to them;

n) qualified electronic seal - an advanced electronic seal that is created by using an electronic seal creation device, on the basis of a certificate for qualified electronic seal;

o) qualified electronic signature/qualified electronic seal creation device – an electronic signature/electronic seal creation device that meets the following requirements:

o.a) electronic signature/electronic seal creation data used in the creation of an electronic signature/electronic seal are confidential. A signatory/creator of a seal is entitled to transfer the right to manage the electronic signature/electronic seal data to a qualified trust service provider, who is entitled to duplicate the data only for the creation of a reserve copy. The procedures for the management of the electronic signature/electronic seal creation data by a qualified trust service provider, as well as the creation of the reserve copy of the data, are determined by the mandatory technical regulations for the qualified trust service providers ('the technical regulations') approved by the Government of Georgia;

o.b) electronic signature/electronic seal creation data used in the creation of an electronic signature/electronic seal are unique;

o.c) it is impossible to draw out the electronic signature/electronic seal creation data used in the creation of an electronic signature/electronic seal within reasonable limits and the electronic signature/electronic seal is reliably protected from counterfeiting using available technologies;

o.d) qualified electronic signature/qualified electronic seal creation devices shall not change the data that are to be signed/sealed and shall not prevent the submission of the data to a signatory/creator of a seal before signing/sealing;

o.e) other conditions determined by the technical regulations are met;

p) certificate for qualified electronic signature/qualified electronic seal – a certificate for electronic signature/electronic seal that is issued by a qualified trust service provider and meets the requirements of Article 6 of this Law;

q) time stamp - a set of electronic data that links an electronic document to a particular time and is used for verifying the existence of the electronic document at the specified time;

r) qualified time stamp - a time stamp, issued by a qualified trust service provider, that meets the requirements of Article 7 of this Law;

s) trust service - an electronic service, the purpose of which is the creation, verification, and identification of the authenticity and/or storage of electronic signatures/electronic seals or time stamps;

t) qualified trust service – a trust service, the purpose of which is the creation, verification, and identification of the authenticity and/or storage of qualified electronic signatures/qualified electronic seals or qualified time stamps and the certificates for qualified electronic signatures/qualified electronic seals related to them;

u) qualified trust service provider - an entity that is authorised in accordance with this Law and provides one or more qualified trust services provided for by this Law;

v) internal regulations - a mandatory public statement for qualified trust service providers on the procedures for the provision of the service;

w) high level of confidence - a set of objective circumstances, facts and/or information, which provide sufficient grounds to ensure that advanced electronic signature creation data are used with the sole control of the signatory, and advanced electronic seal creation data with the control of a legal entity.

Article 3 - Legal effect of an electronic signature and an electronic seal

1. A qualified electronic signature shall have the same legal effect as a handwritten signature.

2. A qualified electronic seal shall make it possible to verify the integrity and origin of an electronic document. The integrity and origin of an electronic document shall be deemed genuine, unless proved to the contrary.

3. If a natural person or a legal entity under private law chooses an electronic form to communicate with administrative bodies and the submitted document requires a signature and/or a seal, it shall be mandatory to put a qualified electronic signature and/or a qualified electronic seal on the document. This procedure shall not apply to cases when the Government of Georgia does not require a signature and/or a seal on the document.

4. An administrative body shall be obligated to put a qualified electronic signature and/or a qualified electronic seal on an electronic document. Putting a qualified electronic stamp on a document by an administrative body shall suffice.

5. Use of qualified electronic signatures shall not be mandatory within the structural units/divisions of administrative bodies and territorial bodies and/or during relations within their scopes. In this case, any used electronic documents and electronic signatures shall accordingly have the same legal force as tangible documents and handwritten signatures.

6. It shall be impermissible to refuse electronic documents during administrative proceedings and court proceedings only because they are presented in an electronic form, however, this fact shall not exclude the refusal to accept an electronic document for the relevant proceedings, if it does not meet the rules established for the said proceedings.

7. It shall be impermissible to refuse to grant evidentiary effect to electronic signatures and/or electronic seals during administrative proceedings and court proceedings, only because they do not meet the the requirements established by this Law for qualified electronic signatures and/or qualified electronic seals.

8. Notwithstanding the provision of paragraph 1 of this article, if there is an agreement between natural persons and/or legal entities under private law, for these entities, electronic documents and electronic signatures shall accordingly have the same legal force as tangible documents and handwritten signatures.

9. Electronic documents and electronic signatures created under the procedures established by the National Bank of Georgia shall accordingly have the

same legal force as tangible documents and handwritten signatures in the implementation of the activities of the National Bank of Georgia and representatives of the financial sector according to conventions that are different from this Law.

10. The cases of exemption from the obligations provided for by paragraphs 3 and 4 of this article shall be determined by a legal act of the Government of Georgia.

Article 4 - Electronic document

1. All copies of an electronic document shall be considered as originals. An electronic document shall not have an electronic copy.

2. The use of an electronic document shall be permitted in all cases where a tangible document in a written form is required, unless otherwise determined by law.

3. A printed version of an electronic document shall be a copy of the electronic document and shall have the same legal force as the electronic document if it has been certified and/or verified by a person responsible for signing or an authorised person provided for by the legislation of Georgia.

4. An electronic copy of a tangible document shall have the same legal force as the original if it has been certified and/or verified by a person responsible for signing or an authorised person provided for by the legislation of Georgia and/or an electronic seal.

Article 5 - Rights and obligations of a qualified trust service provider

1. Qualified trust service providers shall be authorised to provide one or more qualified trust services or trust services provided for by this Law and to determine a relevant fee.

2. Qualified trust service providers shall be obligated to:

a) develop internal regulations and ensure public access for all services that are provided in accordance with this Law. The internal regulations shall include the following information:

a.a) a description of the safe systems, devices and procedures used by the qualified trust service provider;

a.b) the grounds and scope of the insurance of the liability of the qualified trust service provider, including compensation for damage caused by the termination of the activities of the qualified trust service provider, and compensation for damage inflicted on the holders of a certificate, the users of a time stamp service and/or third parties;

a.c) terms and procedures for storing all necessary information related to the qualified trust services by a qualified trust service provider;

a.d) procedures for the termination of the activities of a qualified trust service provider and transferring the activities to another entity (if any);

a.e) the amount of the fee established for the qualified trust service, the procedures for the payment of the fee and possible changes of the terms of payment;

a.f) any other conditions established by the technical regulations;

b) notify a supervisory body on the possible termination of the activities of the qualified trust service no later than 30 calendar days prior to the termination;

c) notify a supervisory body and a consumer of the service regarding any changes made to the internal regulations no later than 14 calendar days prior to the changes;

d) use only safe systems, devices and procedures that ensure the reliability of the services provided and the integrity of the protected data, the verification of the authenticity of the data, and protection against forgery and unsanctioned use. The creation and modification of the data shall be permissible only for persons authorised by a qualified trust service provider;

e) ensure sufficient financial and technical resources and duly qualified personnel in accordance with the technical regulations;

f) ensure personal data protection and management of information security incidents under the procedures established by the legislation of Georgia;

g) ensure sufficient financial resources and guarantees in the case of an administrative body, and civil liability insurance in the case of other entities, to perform the obligations determined by this Law and the technical regulations and to compensate any possible damage;

h) develop a continuous service plan and submit it to a supervisory body;

i) fulfil any other requirement established by the technical regulations;

3. If qualified trust service providers terminate the provision of the service, they shall notify the consumer of the service no later than 30 days prior to the termination of the service. Otherwise, they shall compensate any damage caused by the failure to notify.

4. A qualified trust service provider shall be obligated to compensate any damage caused by the failure to fulfil the obligations of this article, except where the damage is caused by force majeure.

5. Qualified trust service providers shall be obligated to ensure continuous service in accordance with the technical regulations.

6. Qualified trust service providers shall be obligated to notify a supervisory body, no later than 24 hours, of any violation of the security of their systems or the integrity of their data or other events that may pose a substantial threat to the provision of the service determined by this Law and the technical regulations.

7. Qualified trust service providers shall be entitled to develop additional security mechanisms related to the services provided by them.

Article 6 - Certificate for qualified electronic signature/qualified electronic seal

1. A certificate for qualified electronic signature/qualified electronic seal shall include at least:

a) a stamp suited for electronic processing related to the issuance of a certificate as a qualified electronic signature/qualified electronic seal;

b) a set of data that is sufficient for identifying a qualified trust service provider, including at least the name of the qualified trust service provider and the code of the country where it is registered;

c) a set of data that is sufficient for identifying a signatory/creator of a seal, including at least the name and/or the pseudonym/full name and the identification code;

d) qualified electronic signature/qualified electronic seal validation data that correspond to the qualified electronic signature/qualified electronic seal creation data;

e) commencement and expiration dates of the validity of the certificate;

f) the identification number of the certificate that is unique to a trust service provider;

g) the electronic address of the electronic service that may be used to request the status of the validity of the certificate;

h) a stamp suited for electronic processing regarding the placement of the electronic signature/electronic seal creation data in a qualified device of an electronic signature/electronic seal (in the case of the placement of the data in such a device).

2. A certificate for qualified electronic signature/qualified electronic seal shall have an advanced electronic signature/advanced electronic seal of a qualified trust service provider.

3. Upon the request of the holder of the certificate, within the scope of the internal regulations, the certificate for qualified electronic signature/qualified electronic seal may include additional data. A qualified trust service provider shall be authorised to provide additional data in other electronic documents (qualified attribute certificate) related to the certificate for qualified electronic signature/qualified electronic seal that shall meet the following requirements:

a) they shall contain data that allow the identification of the certificate of the qualified electronic signature/qualified electronic seal;

b) they shall have the advanced electronic signature/advanced electronic seal of a qualified trust service provider.

4. Procedures for the placement and management of information in the certificate for qualified electronic signature/qualified electronic seal shall apply to qualified attribute certificates.

5. Qualified trust service providers that provide a service related to a qualified electronic signature/qualified electronic seal, apart from meeting the requirements of Article 5 of this Law, shall be obligated to:

a) identify natural or legal persons, to which a certificate shall be issued, in accordance with with the technical regulations;

b) ensure the authenticity of the data recorded in the certificate, upon its issuance;

c) ensure the prompt revocation of certificates in the cases provided for by law;

d) ensure the suspension and renewal of certificates in the cases provided for by law, if this service is provided for by the internal regulations;

e) maintain a database of certificates for qualified electronic signatures issued by them and ensure its update;

f) immediately provide information, through the internet, on the status of the validity of a certificate or the revocation of a certificate to an interested person, on a continuing basis, in the case of his/her application;

g) ensure the keeping of records of certificates issued by them, as well as of those related data and facts which may be used during legal proceedings or for the purpose of continuous service, storing them for at least 6 years after the revocation of certificates (or more than 6 years in cases provided for by the internal regulations) and specifying the exact time;

h) issue the identification data of the holder of a certificate registered under a pseudonym in the cases provided for by the legislation of Georgia.

6. The internal regulations shall additionally include the following information:

a) a description of a qualified electronic signature/qualified electronic seal creation device;

b) procedures for the issuance of certificates;

c) in the scope of the service related to certificates, including the issues related to the use of pseudonyms and the issuance of certificates containing the data referred to in paragraph 3 of this article;

d) the scope of a certificate;

e) the procedure for recording and storing an issued certificate;

f) the procedure for creating and storing qualified electronic signature/qualified electronic seal creation data and qualified electronic signature/qualified electronic seal validation data;

g) the rules and technical procedures for the suspension, renewal and revocation of the validity of a certificate.

Article 7 - Qualified time stamp

1. Qualified time stamps provide the presumption of the accuracy of the time and date, as well as the integrity of the data related to the time and date.

2. Qualified time stamps shall meet the following requirements:

a) the time and date shall be connected to the data in a manner which enables the detection of any subsequent amendments made to the time, date and data;

b) a qualified time stamp shall be based on an accurate source of time connected to Universal Time Coordinated (UTC).

3. Qualified time stamps shall have an advanced electronic signature/advanced electronic seal of a qualified trust service provider.

4. Qualified trust service providers that provide a service related to qualified time stamps, apart from meeting the requirements of Article 5 of this Law, shall:

a) maintain a database on a continuing basis of the qualified time stamps issued by them and ensure its availability;

b) not issue a qualified time stamp if it is determined that the time specified by the qualified trust service providers exceeds the maximum permissible deviation from UTC as provided for in the internal regulations.

5. The internal regulations that determine the procedure for the provision of a qualified time stamp service shall additionally include the following information:

a) the sources of UTC used for the provision of the service;

b) the maximum permissible deviation from UTC when issuing qualified time stamps.

Article 8 - Qualified identification of the authenticity of a qualified electronic signature/qualified electronic seal

1. The qualified identification of the authenticity of a qualified electronic signature/qualified electronic seal shall be carried out as follows:

a) the signature/seal shall be based on a certificate for qualified electronic signature/qualified electronic seal at the time of putting a qualified electronic signature/qualified electronic seal;

b) a certificate for qualified electronic signature/qualified electronic seal shall be issued by a qualified trust service provider and shall be valid at the time of the use of the qualified electronic signature/qualified electronic seal;

c) the qualified electronic signature/qualified electronic seal validation data shall comply with the data submitted to a party receiving the service (the receiving party) for the qualified identification of the authenticity of a qualified electronic signature/qualified electronic seal;

d) a set of data that uniquely determines a signatory/creator of a seal and is provided in a certificate shall precisely comply with the data submitted to the receiving party;

e) if a qualified electronic signature is put under a pseudonym, the receiving party shall be notified;

f) a qualified electronic signature/qualified electronic seal shall be created using qualified electronic signature/qualified electronic seal creation data.

g) the integrity of the signed data shall be protected;

h) the requirements established by this Law for an advanced electronic signature/advanced electronic seal shall be protected when using a qualified electronic signature/qualified electronic seal;

2. The system used for the qualified identification of the authenticity of a qualified electronic signature/qualified electronic seal shall provide information to the receiving party on meeting the requirements determined by paragraph 1 of this article and enable the detection of any issues related to the security of the data.

3. The qualified identification of the authenticity of a qualified electronic signature/qualified electronic seal shall be carried out by a qualified trust service provider, which shall:

a) identify the authenticity of a qualified electronic signature/qualified electronic seal in accordance with the requirements of this article;

b) provide the receiving party with reliable information on identifying the authenticity of a qualified electronic signature/qualified electronic seal that

has a qualified electronic signature/qualified electronic seal of a qualified trust service provider.

Article 9 - Qualified storage of a qualified electronic signature/qualified electronic seal

Qualified trust service providers shall be entitled to provide the service of the qualified storage of a qualified electronic signature/qualified electronic seal, which implies the extension of the reliability of the qualified electronic signature/qualified electronic seal after the term of its technological validity expires.

Article 10 - Revocation, suspension and renewal of certificates for qualified electronic signature/qualified electronic seal

1. In the case of the revocation of a certificate for qualified electronic signature/qualified electronic seal, its renewal shall be inadmissible. A qualified electronic signature/qualified electronic seal that was created/put after the revocation of a certificate for qualified electronic signature/qualified electronic seal shall be considered invalid.

2. The relevant time and date, based on an accurate source of time connected to UTC, shall be specified when revoking, suspending and renewing certificates for qualified electronic signature/qualified electronic seal. It shall be inadmissible to carry out these actions by specifying a past time and date. A qualified trust service provider shall immediately register the revocation, suspension and renewal of certificates for qualified electronic signature/qualified electronic seal indicating the relevant time and date.

3. Qualified trust service providers shall be entitled to offer the consumer of their services the service of the suspension of certificates for qualified electronic signature/qualified electronic seal that involves the temporary suspension of a certificate. At the time of the suspension of a certificate for qualified electronic signature/qualified electronic seal, a qualified trust service provider shall be obligated to publish information on the suspension and ensure the availability of this information throughout the entire period of the suspension of the certificate.

4. A certificate for qualified electronic signature/qualified electronic seal shall be suspended:

a) upon the request of the holder of the certificate;

b) on the basis of the substantiated request of a supervisory body;

c) by qualified trust service providers in the cases provided for by the internal regulations;

d) in other cases provided for by the legislation of Georgia.

5. The renewal of a certificate for qualified electronic signature/qualified electronic seal that has been suspended may be requested by the initiator of the suspension of the certificate or an authorised person provided for by the legislation of Georgia.

6. A certificate for qualified electronic signature/qualified electronic seal shall be revoked:

a) upon the request of the holder of the certificate;

b) after 10 calendar days following the suspension of the certificate, if the certificate is not renewed during this period;

c) by qualified trust service providers in the cases provided for by the internal regulations;

d) upon the termination of the provision of services by a qualified trust service provider, if the powers to issue a certificate for qualified electronic signature/qualified electronic seal and provide services have not been transferred to a third party;

e) in other cases provided for by the legislation of Georgia.

7. A qualified trust service provider shall immediately notify a holder of a certificate for qualified electronic signature/qualified electronic seal on the revocation, suspension and renewal of the certificate for qualified electronic signature/qualified electronic seal.

Article 11 - Authorisation and supervision of a qualified trust service provider

1. An entity that intends to become a qualified trust service provider shall be obligated to pass through an authorisation process at the Legal Entity under Public Law called the Data Exchange Agency operating under the Ministry of Justice of Georgia ('Data Exchange Agency') to establish the compliance of its activities with this Law and the technical regulations.

2. For the purpose of the supervision of the activities of a qualified trust service provider, the Data Exchange Agency shall perform the following functions:

a) examine the compliance of the activities of a qualified trust service provider with this Law and the technical regulations, when necessary, but no less than once in 2 years;

b) respond to violations discovered in the activities of a qualified trust service provider, in the cases provided for by this Law and the technical regulations;

c) suspend or revoke the authorisation of a qualified trust service provider;

d) produce and publish a list of qualified trust service providers and the services offered by them.

3. An entity that intends to become a qualified trust service provider shall submit the following documents to the Data Exchange Agency:

a) an application;

b) an audit report regarding the compliance of its activities with this Law and the technical regulations;

c) relevant documentation that, in the case of an administrative body, confirms its sufficient financial resources and guarantees, and in the case of other entities, the existence of civil liability insurance;

d) internal regulations.

4. For the purpose of the assessment of system security and the continuous activities of an entity interested in authorisation, the Data Exchange Agency shall be entitled to request additional information/documents from the entity, if necessary. Additional documentation/information to be submitted shall be determined by an order of the Minister of Justice of Georgia provided for by paragraph 8 of this article.

5. The Data Exchange Agency shall be entitled to refuse to authorise an entity interested in authorisation, if:

a) the submitted documentation/information is incomplete and/or inaccurate;

b) its activities do not comply with this Law and the technical regulations.

6. If the submitted documentation/information is incomplete and/or inaccurate, the Data Exchange Agency shall determine the term for the entity interested in authorisation to remedy such defect. The Data Exchange Agency shall be entitled to refuse authorisation if the defects are not remedied within this term, although this shall not deprive the entity interested in authorisation of the right to reapply to the Data Exchange Agency with a request for authorisation.

7. The Data Exchange Agency shall be entitled to suspend or terminate the authorisation of a qualified trust service provider in the case of its failure to meet the requirements provided for by this Law and the technical regulations.

8. The procedure for the authorisation and supervision of a qualified trust service provider shall be determined by an order of the Minister of Justice of Georgia.

Article 12 - Recognition of qualified trust services of organisations operating abroad or international organisations

The qualified trust services of organisations operating abroad or international organisations shall, in accordance with this Law, have the same legal force as qualified trust services operating in Georgia, if Georgia has entered into a relevant international agreement on the recognition of the qualified trust services.

Article 13 - Transitional provisions

1. The Legal Entity under Public Law called the Public Service Development Agency operating under the Ministry of Justice of Georgia shall be considered a qualified trust service provider before 1 July 2018.

2. An electronic document, requested from an information system before 1 January 2018, shall have the same legal force as a tangible document, if the system ensures verification of the electronic document automatically. Article 4(3) of this Law shall not apply to the cases provided for by this paragraph during the same period.

3. Electronic documents and electronic signatures used by an administrative body before 1 July 2018 shall accordingly have the same legal force as tangible documents and handwritten signatures.

4. Before the entry into force of this Law, on the basis of a certificate for electronic signature issued by the Legal Entity under Public Law called the Public Service Development Agency operating under the Ministry of Justice of Georgia, an electronic signature made within the period of validity of the certificate shall have the same legal force as a qualified electronic signature.

5. The Government of Georgia shall:

a) approve an action plan for the enforcement of the provisions of this Law that includes at least measures aimed at ensuring the establishment and the use of qualified electronic signatures/qualified electronic seals in the State before 1 October 2017;

b) approve the mandatory technical regulations for qualified trust service providers before 1 March 2018.

6. The Minister of Justice of Georgia shall approve the procedures for the authorisation and the supervision of qualified trust service providers before 1 March 2018.

Article 14 - Final provisions

1. The Law of Georgia of 14 March 2008 on Electronic Signatures and Electronic Documents (Legislative Herald of Georgia, No 7, 26.3.2008, Art. 46) shall be declared invalid.

2. This Law, except for Article 3(3) and (4) and Article 11, shall enter into force upon its promulgation.

3. Article 3(3) and (4) and Article 11 of this Law shall enter into force from 1 July 2018

President of Georgia **Giorgi Margvelashvili**

Kutaisi,

21 April 2017

No 639-IIს