Brief of The Electronic Transactions Law

Issued by Royal Decree No. M/18 dated 08/03/1428 AH

Definitions

Electronic Transaction

Any exchange, correspondence, contract, or other procedure concluded or executed - in whole or in part - by electronic means.

Electronic Data

Data with electronic characteristics in the form of text, symbols, images, drawings, sounds or other electronic formats, combined or separate.

Electronic Data System

One or more electronic devices or software used to generate, extract, send, broadcast, receive, store, display, or process electronic data.

Electronic Record

Data produced, received, transmitted, or stored electronically, capable of being retrieved or obtained in an understandable manner.

Electronic Signature

Electronic data included in, added to or logically associated with an electronic transaction used to verify the identity and consent of the person signing it and to detect any modification of such transaction after signing it.

Digital Certificate

Electronic document issued by a certification services provider, used to confirm the identity of the person in possession of the electronic signature system, which contains the verification data of his/her signature.

Certification Service Provider

A person authorized to issue digital certificates or perform any service or function relating thereto and electronic signatures in accordance with the Electronic Transaction Law ("**the law**").

Objectives of the Law

- Controling and regulating electronic transactions and signatures in the public and private sectors.
- Enhancing confidence in the validity and integrity of electronic transactions, signatures, and records.
- Ease of use of electronic transactions and signatures domestically and internationally.
- Prevention of misuse and fraud in electronic transactions.

Exceptions to electronic transactions and signatures

1. Personal status related transactions.
2. Issuance of instruments relating to property disposition

Unless otherwise permitted by the competent authority.

Approval of electronic transaction

1. Consent can be express or implied, except for a government entity, it must be express.
2. Additional special conditions may be established for accepting electronic transaction as long as they do not contradict with the Law.

Contact us | Faisaliah Tower, Level 11
Riyadh, King Fahd Road, Saudi Arabia | +966 11 484 7171 | info@erlf.com | www.erlf.com

Binding Force and acceptability of electronic transactions

- Electronic transactions, records and signatures shall have binding force, and their validity or enforceability shall neither be denied nor prevented by reason of being made in whole or in part in electronic form, as long as it is consistent with the Law.
- The binding force and enforceability of electronic transactions are linked to its details' availability for review.
- The offer and acceptance of an electronic transaction may be expressed through an electronic transaction.
- An electronic record is considered an original when the integrity of its information is being validated.
- An electronic transaction or signature is acceptable as a proof of evidence, it may as well be acceptable as a presumption of evidence.

"If a hand-written signature is required for any document or contract or similar, such requirement shall be deemed satisfied by an electronic signature generated in accordance with this Law. The electronic signature shall be equal to hand-written signature, and it shall have the same legal effects. "

- In the event that an electronic signature is provided in a Shariah or legal procedure, the basic rule, unless the opposite is proved or agreed upon, shall be:
- The signature belongs to the person specified in the digital certificate and is affixed according to the purpose specified therein.
- The electronic transaction has not been changed after the electronic signature was affixed thereon.

Conditions for conducting an electronic signature and its specifications

- It shall be associated with a certified and valid digital certificate.
- The integrity of the signatory's identification information, and its compatibility with the digital certificate.
- The absence of technical deficiencies and availability of the minimal technical and administrative structure related to signature procedures.
- The signatory's compliance with all the requirements of the digital certification procedures.
- The availability of the following substantive elements as minimum:
  - Digital certificate issuer.
  - Signature type, its scope, and its serial number.
  - Date and duration of signature.
  - The type of encryption algorithm used and the public encryption key.
  - The scope of use of the signature and the limits of its statutory liability, as well as the requirements for the protection of the confidentiality of information.
  - The signatory's identification information, including his name and full address.

Certification Service Provider's duties and obligations

1 Obtaining the necessary license from the Communications and Information Technology Commission (the "**Commission**") before commencing its activity.

2 Issuing digital certificates in accordance with the conditions of issuance, delivering and preserving, establishing a database, and making them available for review.

3 Using reliable means for issuing certificates and taking the necessary means to protect them.

4 Maintaining the confidentiality of the information obtained and handing over information and documents to the Commission in the event its activity is suspended.

5 Obtaining personal information from the applicant directly, or from who is authorized.

Contact us | Faisaliah Tower, Level 11
Riyadh, King Fahd Road, Saudi Arabia | +966 11 484 7171 | info@erlf.com | www.erlf.com

Responsibilities of the certificate holder

1. The integrity and confidentiality of its signature system, his liability for its use, his compliance with the certificate and the terms of the signature.
2. Providing correct information to the Certification Service Provider and the relevant parties and informing them of any change thereto.
3. Informing the Certification Service Provider of any change in the information contained in the digital certificate.
4. Refraining from reusing the elements of the electronic signature of a suspended or cancelled certificate.

Violations

The following acts are illegal:

- Practicing Certification Service Provider's activity without a license.
- Misuse or disclosure by the Certification Services Provider of information collected.
- Disclosure by the Certification Service Provider of information made known to it by reason of its work.
- Provision by the Certification Services Provider of false statements or misleading information to the Commission or mishandling its services.
- Use of electronic transaction for a fraudulent or unlawful purpose
- Forging or using an electronic transaction knowing its forgery.
- Intentionally providing false information to the Certification Service Provider or related parties.
- Access and disposal of an electronic signature system of another person without proper authorization.
- Impersonating another person or alleging authorization for the digital certification procedures for another person's signature.
- Publication, presentation to others, of a forged, incorrect, cancelled or suspended digital certificate.

Penalties and compensation for damage

A fine of not exceeding five million (5,000,000) Saudi Arabian Riyals or imprisonment for a term not exceeding five (5) years or both, and seizure of the devices, systems and programs used to commit the offence may be imposed. The summary of the final judgement may be published at the expense of the sentenced person based on the type, gravity and impact of the offence committed.

A person who has suffered damage shall be entitled to file a claim to the competent judicial authority to seek compensation for damages suffered.

Controls and duration of preserving electronic record and data

- Records must be kept in their nature and entire original data and may be archived in any form without prejudice to its content and quality.
- The duration of preserving an electronic record is determined by the application of regulations and resolutions relevant to electronic transaction.
- The parties to an electronic transaction shall be bound by the bilateral agreements concluded between them with respect to the duration of the preservation of electronic data.
- The electronic record must contain the following data as minimum:
  - Information of the originator, transmitter, and addressee of the electronic record.
  - The operation number and nature embodied in the electronic record.
  - Date and time of establishment of the electronic record, date and time of transmission, date and time of receipt.
  - Repatriation, modification, or cancellation information, as well as receipt confirmation letters as and when required.

Contact us | Faisaliah Tower, Level 11
Riyadh, King Fahd Road, Saudi Arabia | +966 11 484 7171 | info@erlf.com | www.erlf.com

The responsible party for preserving electronic records

- The person responsible for preserving the electronic record shall be determined by the application of regulations, bylaws, and resolutions relevant to the electronic record.
- The services of another entity may be used to meet the requirements for preserving the electronic record.
- The party responsible for preserving shall as well archive and do periodic backup of the records.
- The parties to an electronic transaction shall comply with their bilateral agreements concerning the preservation of electronic data and the rules and procedures governing the operation of the National Digital Certification Centre (the "**Centre**").

Electronic record preserving requirement

- Following clear and documented rules and procedures for preservation.
- Preserving in a form compatible with the system of the reserving party.
- Ensuring that records are safe from unauthorized conduct and that they are retrievable in events of disasters.
- In determining the date and time, the following must be observed:
  - Adopting the Gregorian date -at least- and adding the Hijri date when required.
  - Specifying the time in hours, minutes, and seconds -at least-.
  - Compliance with the official time adopted by the Centre, or another time agreed-upon by the parties.
- Embodying in the record, a time stamp approved by the Centre, or another stamp agreed upon by the parties.
- Ensuring that the preservation or preserved content is made according to the form issued, transmitted, or received.

Conditions for presenting and accessing to electronic records and data

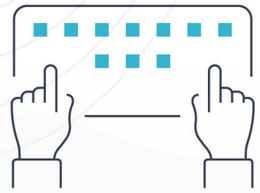
1. The availability of information in a standard electronic format that is readable, understandable, and complete.
2. Identification by entities, of review authorities pursuant to the work needs.
3. Application of suitable technical solutions to record events of review.
4. Observing the privacy and confidentiality of records and refraining from allowing third parties to access them without its parties' consent.

Creation of electronic records

1. An electronic record is considered issued by its originator or by who is authorized.
2. The originator of a record may use a technical medium to create or transmit the record, in which case the intermediary shall not be considered the originator.
3. The mediator is committed to ensuring that transmission of the information in its exact content without change.

Transmitting electronic records

- The originator of a record, or who is authorized, is responsible for its transmission.
- The time of dispatch of the record is the time when it moves to another electronic system beyond the authorities of the originator.
- Unless otherwise agreed, the record shall be deemed to have been sent to and from a party's statutory address and, **in the event of multiple addresses, the following shall apply:**
  - the address most closely related to the electronic transaction.
  - or the address specified in the articles of association of a legal person.
  - or the residence of the addressee.



Requirements for the creation and transmission of an electronic record

- The record shall keep its entire data that was embodied therein at the time of creation.
- Availability of information of the originator, the recipient, the time and place of transmission, the time and place of reception.
- The mediator is obliged to ensure that the information from the originator's system reaches the recipient' system with the exact content without change.

Acknowledgement of receipt of an electronic record

- When an acknowledgement of receipt is required without a particular form required:
  - It may be done by any means from the addressee, automatically or otherwise.
  - It may be done by any conduct of the addressee indicating its receipt.
- When an acknowledgement of receipt is required, the transmission of the record shall be considered as if it does not exist until an acknowledgement of receipt is received, unless otherwise agreed.
- Receipt of an electronic record shall be proofed by any agreed form of evidence.
- Receiving an acknowledgement of receipt does not mean that the content of the transmitted record is identical to the content of the received record unless it contains a content preservation mechanism.
- Acknowledgement of arrival of the record must include the date, time and special number of the message or its topic.
- The technical requirements of the acknowledgement letter shall be deemed met unless proven otherwise.

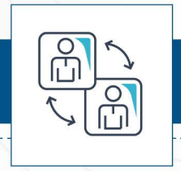
Continuation of service in case of suspension of the Certification Services Provider, or cancellation, or non-renewal of its license

- The Centre shall consider the continued provision of services to users of the Certification Service Provider whose license is suspended, cancelled, or expired.
- The Centre shall take such necessary measures at the expense of the Certification Service Provider whose license is suspended, cancelled, or expired, and who failed at taking the necessary measures, to ensure the rights of the users of its services.

Contact us | Faisaliah Tower, Level 11
Riyadh, King Fahd Road, Saudi Arabia | +966 11 484 7171 | info@erlf.com | www.erlf.com

Provisions and criteria for disposal of Certification Services Provider's information and documentation in case of discontinuance of its activities

- The Certification Service Provider whose activity is suspended is obliged to:
- Keep all information on digital certificates and other data without modifying their content.
- Provide the Commission with all technical details, transfer and transmit the data as determined by the Centre.
- The Commission may take the necessary measures to protect users' rights.
- A person whose dealing with a Certification Service Provider, who has suffered damages shall be entitled to file a claim for compensation.
- After the Certification Services Provider has completed its duties, it shall be prohibited from keeping any copies of electronic records and data.



Elements of a digital certificate

- Availability in a digital certificate of the following technical elements as minimum:
- Issuer of the digital certificate, including all information indicating the Certification Services Provider.
- The identity information of the certificate holder, which includes his full name and address.
- The issuance date and duration of the certificate.
- Scope of use of the certificate, limits of its statutory liability, and conditions for the protection of confidentiality of information.
- The Certification Service Provider shall prepare certified forms approved by the Commission to users and shall be liable for damage caused by reliance on them.

Procedure for approval of suspending activity, assigning license or merging

The Certification Services Provider shall continue to provide its services and shall never cease or assign them without the prior approval of the Commission.

The Certification Services Provider shall not merge or partner with any other party without the approval of the Commission based on a submitted comprehensive study.

Accreditation of foreign digital certificates

1 Foreign digital certificates are certified in accordance with the Centre's reciprocal certification policy.

2 The procedures for recognition of a foreign issuer of certificate shall be consistent with those for obtaining a license to provide certification services.

3 The certification of foreign digital certificates shall not affect the rights of the certificate holder or those who deal with him.

4 The Centre continuously publishes and updates a list of recognized foreign entities.

5 The Centre may reject foreign digital certificates issued from a recognized foreign entity, whenever the public interest requires.

Contact us | Faisaliah Tower, Level 11 Riyadh, King Fahd Road, Saudi Arabia | +966 11 484 7171 | info@erlf.com | www.erlf.com

Identification of means to protect certificates from forgery, fraud, and damage

1. The Certification Service Provider shall adopt appropriate means of protection at a high level of security as approved by the Centre.
2. The Certification Service Provider shall notify the Commission and beneficiaries in the event of a potential threat to the security and safety of its electronic and administrative resources.

Events of cancellation or suspension of a certificate

- A digital certificate may be cancelled or suspended pursuant to a request of its holder, without prejudice to the rights of those who had previously relied on it.
- A digital certificate shall be cancelled or suspended pursuant to an order from the Commission, **and the Certification Services Provider shall be responsible for:**
  - Executing the cancellation or suspension order.
  - Notifying certificate holder of the procedures.
  - Alerting those who rely on the certificate in the future that it is not valid.

Competent Authorities

- **Ministry of Communications and Information Technology**
  - Drawing public policies and setting plans and developing programs for electronic transactions and signatures.
  - Submitting regulations' drafts and any proposed amendments thereto and coordinating with government entities.
  - Representing Saudi Arabia in local, regional, and international agencies regarding electronic transactions and signatures.
- **Communications and Information Technology Commission**
  - Applying the law.
  - Licensing for practicing (Certification Service Provider) activity and verifying their compliance with the provisions.
  - Proposing regulations' drafts and bylaws relating to electronic transactions and submitting them to the Ministry.
  - Determining of the financial consideration for the license to provide pursuant to the approval of the Minister.
- **National Centre for Digital Certification**
  - Supervision of digital certification functions and management of its infrastructure.
  - Certifying certificates issued by foreign entities outside the Kingdom.
  - Issuing digital certificates related to Certification Services Providers.
  - Publishing and updating the list of licensed Certification Service Providers.
  - Coordination with the Commission in relation to licensing entities who want to provide digital certification services.
  - Providing technical support to the Commission in relation to its supervision of licensed certification service providers.
  - Notifying the Commission of any violations relating to the licenses of certification services providers.