

ELECTRONIC TRANSACTIONS LAW NO (85) OF 2001

ELECTRONIC TRANSACTIONS LAW NO (85) OF 2001

Article (1)

This Law shall be called the “Electronic Transactions Law for the year 2001” and shall come into effect as of the lapse of three months from the date of its publication in the Official Gazette.

Article (2)

The following words and expressions, wherever stated in this Law, shall have the meanings ascribed thereto hereunder unless the context indicates otherwise:

Transactions:	An action or set of actions occurring between two parties or more for establishing obligations upon one party, or mutual obligations between more than one party relating to the conduct of business, a civil obligation, or any government department.
Electronic Transactions:	Transactions conducted by electronic means.
Electronic:	The technology utilizing electrical, magnetic, optical or electro-magnetic means or any other similar means in the interchange and storage of information.
Information:	Data, texts, images, forms, sounds, codes, databases, computer software and the like.
Electronic Data Interchange (EDI):	Electronic transfer of information from one person to another using information processing systems.
Data Message:	Information generated, sent, received or stored by electronic or similar means, including Electronic Data Interchange (EDI), electronic mail, telegram, telex or telecopy.
Electronic Record:	A record, contract, or data message generated, sent, received or stored by electronic means.
Electronic Contract:	An agreement concluded in whole or in part by electronic means.
Electronic Signature:	Data in the form of letters, numbers, codes, characters or in other forms, incorporated in, attached to or logically associated with a data message, in electronic, numeric, optical, or other similar means, whereby it enables

	[authentication] identifying the signatory and distinguishing such from others by virtue of the signature, and for the purpose of indicating the signatory's approval of the content of the data message.
Information processing System	An electronic system used for generating, sending, receiving, processing or storing data messages or for handling data messages in any other respect.
Electronic Agent:	A computer program or other electronic means used independently to implement an action or respond thereto for the purpose of generating, sending, or receiving a data message without review or action by an individual.
Originator:	A person by whom or on whose behalf, a data message is generated or sent prior to its receipt or storage by the addressee.
Addressee:	The person who is intended by the originator to receive the data message.
Security Procedures:	Procedures employed for the purpose of verifying that an electronic signature or record is that of a specific person, or for detecting changes and errors in an electronic record after its generation. Such procedures include the use of analytical methods to identify codes, words and numbers, decryption, callback or any other method or procedures which serve this purpose.
Security Certificate:	A certificate issued by a licensed or competent entity for the purpose of verifying the electronic signature of a specific person in accordance with the adopted security procedures.
Identification Code:	The code assigned by a licensed or competent entity for the purpose of securing the electronic contracts of a certain person, and whereby it is used by the addressee in order to distinguish the records of such a persons from other records.
Financial Institution	Any licensed bank or financial institution authorized to make financial transfers in accordance with the provisions of the Laws in force.
Illegal entry :	Any financial entry in the client's account resulting from an electronic message sent in the client's name without the client's

	knowledge, approval or authorization.
--	---------------------------------------

General Provisions

Article (3)

- A- The aim of this Law is to facilitate the use of electronic means in conducting transactions, subject to the provisions of any other law, and without amending or annulling any of these provisions.
- B- In the application of this Law, due regard shall be had to international commercial custom and technological advances pertaining to electronic transactions.

Article (4)

The provisions of this Law shall apply to the following:

- A- Electronic transactions, electronic records, electronic signatures and any electronic data messages.
- B- Electronic transactions adopted in whole or in part by any governmental department or public institutions.

Article (5)

- A- Unless otherwise provided for in this Law, the provisions of this Law shall apply to transactions between parties which have agreed to conduct their transactions by electronic means.
- B- For the purposes of this Article, an agreement between a party to conclude a specific transaction by electronic means shall not oblige any of the parties to conclude other transactions by such means.

Article (6)

The provisions of this Law shall not apply to:

- A- Contracts, instruments or documents that are governed by special legislation and prepared in a certain form, or in accordance with specific procedures, including the following:
 - 1- Wills and amendments thereto;
 - 2- Waqfs and amending conditions thereof;
 - 3- Transactions disposing of immovable property, including related powers of attorney, title deeds, and

- transactions creating real rights in respect thereof, with the exception of lease contracts;
- 4- Power of attorney instruments and transactions relating to personal status;
 - 5- Contract termination or revocation notices relating to water or electrical services, health insurance or life insurance;
 - 6- Bills of statements, court proceedings, judicial notification and courts decisions.
- B- Securities, except for cases provided for in special instructions issues by the competent authorities pursuant to the Securities Law in force.

Electronic Records, Contracts, Messages and Signatures

Article (7)

- A- Electronic records, contracts, messages, and signatures shall be deemed to produce the same legal effect as written documents, instruments and signatures pursuant to the provisions of legislation in force and with respect to enforceability and admissibility as evidence.
- B- None of the items mentioned in Paragraph (A) of this Article shall be denied legal effect solely on the ground of being conducted by electronic means, provided they are compliant with the provisions of this Law.

Article (8)

- A- An electronic record shall have the same legal effect as an original form, and be deemed equivalent thereto, subject to all of the following conditions:
1. The information set forth therein is capable of being retained and stored whereby it is accessible for later reference at any time.
 2. The record is capable of being retained in the form in which it had been generated, sent, received or in any other form whereby the accuracy of information set forth therein when it was generated, sent or received can be readily established.
 3. The information set forth in the record is indicative of the originator, addressee and the date and time of sending and receipt.

- B- The conditions stated in Paragraph (A) of this Article shall not apply to information in the record incorporated to facilitate its sending and receipt.
- C- The originator and addressee may establish fulfillment of the conditions set forth in Paragraph (A) of this Article through a third party.

Article (9)

- A- If the parties have agreed to conduct a transaction by electronic means in a case where the applicable law requires providing, sending or delivering the related information to others in writing, this requirement may be deemed satisfied if the recipient is capable of printing and storing this information and referring back to it subsequently through accessible means.
- B- If the sender inhibits the addressee's ability to print, store or maintain an electronic record, the record shall not be binding upon the addressee.

Article (10)

- A- Where legislation requires a document to be signed or stipulates consequence for non signature, an electronic signature on an electronic record shall satisfy the requirements of this legislation.
- B- The validity of an electronic signature and its attribution to the signatory may be proved by a method which identifies the signatory and indicates consent thereof about the information set forth in the electronic record that bears the signature, whereby such a method is considered reliable for this purpose, in context of the circumstances of the transaction, including the parties' agreement to using such a method.

Article (11)

If a legislation requires that a certain document shall be maintained for documentation, evidentiary, or auditing purposes or other like purposes, the electronic record shall be deemed to fulfill this requirement, unless a subsequent legislation stipulates that the record must be maintained in writing.

Article (12)

Articles (7) to (11) of this Law shall not be applicable in any of the following cases:

- A- If a legislation in force requires sending or providing certain information to a related person in writing but also allows otherwise by agreement;
- B- If it was agreed to send or communicate certain information by first class mail, express mail or regular mail.

Article (13)

An electronic message shall be a valid mean of declaration of will regarding offer or acceptance for contractual purposes.

Article (14)

An electronic message is deemed to be that of the originator if it was sent by the originator himself, or on behalf thereof, or by an electronic agent programmed, by or on behalf of the originator, to operate automatically.

Article (15)

- A- An addressee is entitled to regard a data message issued by the originator and to act on that assumption in any of the following cases:
 - 1- If for the purposes of verifying that the data message is issued by the originator, the addressee applies an information processing system previously agreed to with the originator.
 - 2- If the data message as received by the addressee has resulted from the actions of a person subordinate to, or acting on behalf of the originator, and who is authorized to access the electronic methods used by either of them to identify the originator.
- B- The provisions of Paragraph (A) of this Article shall not apply in the following two cases:
 - 1- If the addressee receives a notice from the originator that the data message is not that of the originator, in which case the addressee shall act on this assumption, whereas the originator remains liable for any results prior to the notice.
 - 2- If the addressee knew, or should have known, that the data message was not that of the originator.

Article (16)

- A- If the originator requests in the data message, or agrees with the addressee, that the receipt of the data message be acknowledged, this shall be deemed fulfilled if the recipient informs the originator of receipt electronically or otherwise, or indicates such by any measure or conduct.
- B- Where the originator has stated that the data message is conditional on receipt of the acknowledgement, the data message is treated as though it has never been sent until the acknowledgement is received.
- C- If the originator requests that the receipt of the data message be acknowledged, but does not specify a time for such, or condition the data message upon receipt of acknowledgement, and if such acknowledgement is not received within a reasonable time, the originator may *sic* [serve] the addressee notice to send the acknowledgement within a set period, subject otherwise to treating the data message as if it has not been sent.
- D- The notice of receipt does not by itself establish that the content sent corresponds to the content received.

Article (17)

- A- Unless otherwise agreed between the originator and the addressee, the sending of a data message shall occur when it enters an information processing system outside the control of the originator or the person who sent the data message on behalf of the originator.
- B- If the addressee has designated an information processing system for the purpose of receiving data messages, the message shall be deemed to have been actually received upon its entry into such a system. However, if the message is sent to a system other than the designated system, the message shall be deemed to have been received upon the addressee's retrieval of the message for the first time.
- C- If the addressee has not designated an information processing system for the purpose of receiving data messages, the message shall be deemed to have been received at the time of its entry into any information processing system of the addressee.

Article (18)

- A- Unless otherwise agreed between the originator and the addressee, the data message shall be deemed to be dispatched at the place where the originator has its place of business, and shall be deemed to be received at the place where the addressee has its place of business. If the

originator or the addressee does not have a place of business, reference is to be made to the habitual residence.

- B- Where the originator or the addressee has more than one place of business, the place of business is that which has the closest relationship to the underlying transaction. Where this may not be determined, the principal place of business shall be deemed to be the place of dispatch or receipt.

Transferable Electronic Note

Article (19)

- A- An electronic note shall be transferable if it meets the requirements of negotiable instruments under the Commercial Code with the exception of the requirement of writing, and provided the drawer has agreed to the note's negotiability.
- B- The electronic retention of a check in accordance with the provisions of Article (8) of this Law shall be deemed legal, if the data contained on the front and back side of a check can be accessed for later reference.
- C- Articles (20), (21), (22), (23) and (24) of this Law shall apply to electronic checks only upon approval of the Central Bank of Jordan, whereby approval criteria shall be set forth in instructions issued for this purpose.

Article (20)

The holder of an electronic note shall enjoy the rights associated with a transferable record if the information processing system employed to generate and transfer the note is capable of evidencing transfer of right in respect thereto and of verifying the identity of the beneficiary and transferee.

Article (21)

- A- An information processing system shall be deemed reliable for evidencing transfer of the right in the note in accordance with the provisions of Article (20) of this Law, if this system allows for generating, storing and transferring the electronic note subject to the following two conditions jointly:
 - 1- The authoritative copy of the transferable note is uniquely identifiable and unalterable, with due regard to the provisions of Paragraph (C) of this Article.

2- The authoritative copy of the note sets forth the name of the person to whose benefit the note is drawn, the note's transferability, and beneficiary's name.

B- The authoritative copy shall be sent and maintained by the person asserting control or its designated custodian.

C-

1- Copies or revisions of the authoritative copy that are modified or changed can be made only with the consent of the person asserting control over the note.

2- It shall be indicated on each revised copy of the note whether it is authorized or not.

3- Each copy of the authoritative copy shall be readily identifiable as an identical copy of the authoritative copy.

Article (22)

Except as otherwise agreed, the holder of an electronic note shall assert control over the transferable note and shall enjoy the same rights and defenses as the holder of the written note in accordance with any other legislation and provided all applicable requirements are met.

Article (23)

An obligor under a transferable note shall enjoy the same rights and defenses as an obligor under written transferable notes.

Article (24)

If objection is made against the enforcement of a transferable electronic note, the person seeking to enforce the note shall provide reasonable proof that he is in control of the note. Such proof may include presentation of the authoritative copy of the transferable note and of related business records, for the purpose of verifying the terms of the note and establishing the identity of the person having control over it.

Electronic Transfer of Funds

Article (25)

The transfer of funds by electronic means shall be deemed as an acceptable method of payment. This Law shall in no way affect the rights of persons in accordance with other relevant laws in force.

Article (26)

Any financial institution practicing the electronic transfer of funds in accordance with the provisions of this Law and the regulations issued pursuant thereto shall:

- A- comply with the provisions of the Central Bank of Jordan Law, the Banks Law, and all relevant regulations and instructions issued pursuant thereto;
- B- take the measures necessary to ensure secure services for clients and maintain banking confidentiality.

Article (27)

A client shall not be liable for any illegal entry to its account affected by an electronic transfer that occurs after the client notifies the financial institution of the likelihood of access to its account by another party, the loss of the client's card, or of the likely disclosure of the client's identification code, and after requesting the institution to cease electronic transfer activities on the account.

Article (28)

Notwithstanding the provisions stated in Article (27) of this Law, the client shall be deemed liable for illegal uses of the client's account by means of an electronic transfer, if it is established that this is attributed largely to the client's negligence and that the financial institution has exercised its duties reasonably to forestall illegal use of the account.

Article (29)

The Central Bank of Jordan shall issue the required instructions for regulating the electronic transfer of funds, including those governing approving electronic means of payment, identification of entries resulting from illegal transfers, procedures for rectifying errors, disclosure of information and any other matter pertinent to electronic banking activities, including information that must be provided by financial institutions to the Central Bank.

Securing the Electronic Records and Electronic Signature

Article (30)

- A- For the purposes of verifying that an electronic record has not been altered as of a specific date, the record shall be considered a secure electronic record as of the date of its verification, provided such verification is conducted according to security procedures

that are accredited, or commercially acceptable, or mutually agreed upon by the pertinent parties.

- B- The security procedures shall be deemed commercially acceptable, if they are applied with due regard to the commercial circumstances pertaining to the transacting parties, including the following:
- 1- The nature of the transaction;
 - 2- The level of sophistication of each party to the transaction;
 - 3- The volume of similar commercial transactions concluded by either party;
 - 4- The availability of alternative procedures rejected by any party;
 - 5- The cost of the alternative procedures;
 - 6- The procedures in general use for such a transaction.

Article (31)

If through the application of a used security procedures, it is established that such procedures are accredited, or commercially accepted, or agreed upon between the parties concerned, the electronic signature shall be deemed secure if it has the following attributes:

- 1- It is unique to the person using it;
- 2- It is capable of identifying its holder;
- 3- It is generated by means of that person and under his control;
- 4- It is affixed to the electronic record in a manner which does not allow alteration of the record after its signature without alteration of the signature.

Article (32)

- A- Unless otherwise proven, it shall be presumed that:
- 1- a secure electronic record has not been altered or modified as of the date of applying the security procedures;
 - 2- The secure electronic signature is affixed by the person to whom it is attributed, with the intention of indicating his approval of the document's content.
- B- An electronic record or signature which is not secure does not have any authoritativeness.

Article (33)

An electronic record or any part thereof that bears a secure electronic signature shall be deemed a secure record in whole, or in respect of the said part, as the case may be,

if the signature is generated during the validity period of an accredited security certificate and it corresponds to the identification code indicated in the certificate.

Article (34)

A security certificate bearing the identification code shall be deemed accredited in the following cases:

- A- If it is issued by a licensed or competent entity;
- B- If it is issued by an entity licensed by a recognized competent authority in another country;
- C- If it is issued by a governmental department, institution or by a body duly authorized for this purpose;
- D- If it is issued by a body accepted by the transacting parties.

Penalties

Article (35)

Any person who creates, makes public, or submits a security certificate for fraudulent purposes or any illicit purpose shall be subject to a penalty of imprisonment for a period of no less than three months and no more than two years, or a fine of no less than (3000) three thousand dinars and no more than (10000) ten thousand dinars, or to both penalties jointly.

Article (36)

Any person who submits to an entity engaged in the practice of securing documents false information with the intent of issuing, invalidating, or canceling a security certificate shall be subject to a penalty of imprisonment for a period of no less than one month and no more than six months, or a fine of no less than (1000) one thousand dinar and no more than (5000) five thousand dinars, or to both penalties jointly.

Article (37)

Any entity engaged in the practice of securing documents which submits false information in a registration application, or discloses confidential information of any of its clients, or violates the regulations and instructions issued pursuant to this Law documents shall be subject to a fine of no less than (50000) five thousand dinars.

Article (38)

Any person who commits an act that constitutes a crime pursuant to legislation in force by using electronic means shall be subject to the penalty of imprisonment for a period no less than three months and no more than one year, or a fine of no less than (3000) three thousand dinars and no more than (10000) ten thousand dinars, or to both penalties jointly. In case the said legislation provides for higher penalties than under this Law, the higher penalties shall apply.

Final Provisions

Article (39)

The competent entities charged with implementing the provisions of this Law and the responsibilities assigned thereto shall be determined by Cabinet decisions.

Article (40)

The Cabinet shall issue all the regulations necessary for implementing the provisions of this Law, including those covering the following:

- A- The fees charged by any government department or public institution for conducting electronic transactions.
- B- The procedures for issuing security certificates, the authority competent to do such, and the applicable fees.

Article (41)

The Prime Minister and Ministers shall be responsible for the implementation of the provisions of this Law.

11 December 2001
Final sent to Nancy on 25 April 2002

Abdallah II Ibn El Hussein