دولة الكويت
مجلس الوزراء
الجهاز المركزي لتكنولوجيا المعلومات
The Central Agency For Information Technology

Law No. 20 of 2014 Concerning

Electronic Transactions

His Highness the Amir of the State of Kuwait

Sheikh Sabah Al-Ahmad Al-Jaber Al-Sabah

May Allah protect him

H. H. Sheikh

Nawaf Al-Ahmad Al-Jaber Al-Sabah

Crown Prince of the State of Kuwait

HH Sheikh

Jaber Mubarak Al-Sabah

Prime Minister of the State of Kuwait

Contents

Law No. 20 of 2014 Concerning

Electronic Transactions

- Having perused the constitution,
- Decree No. 5 of 1959 for the real estate registration law and its amending laws.
- The penal law promulgated by law No.16 of 1960 and its amending laws.
- The penal procedures and trials law promulgated by law No.17 of 1960 and its amending laws.
- The authentication law promulgated by Law No. 4 of 1961 and its amending laws.
- Law No. 5 of 1961 organizing legal relations with a foreign element.
- Law No. 32 of 1968 concerning cash, the Central Bank of Kuwait, regulation of the banking profession and its amending laws.
- The Decree Law No. 15 of 1979 concerning civil service and its amending laws.
- The Civil and Commercial Proceedings Law, promulgated by decree law No.38 of 1980 and its amending laws.
- Decree law No. 39 of 1980 concerning proof in civil and commercial matters and its amending laws.
- The Civil Law issued under No. 67 of 1980 and its amending laws.
- The Law of Commerce promulgated by decree law No. 68 of 1980 and its amending laws.
- Law No. 22 of 1982 concerning civil information system.
- Law No. 51 of 1984 concerning civil status and its amending laws.
- Law No. 1 of 1993 concerning the protection of public funds and its amending laws.
- Law No. 64 of 1999 on the copyrights protection of intellectual property.
- Law No.7 of 2010 concerning setting up the Capital Markets Authority and regulating the securities activity.

- Law No.7 of 2010 concerning setting up the Public Authority for Anti-Corruption.
- And the Law Decree No. 24 of 2012 concerning the establishment of the Public Authority for Combating Corruption
- Companies Law Decree Law No. 25 of 2012 concerning companies Law.
- Law No. 106 of 2013 concerning Anti-Money Laundering and Counter-Terrorism Financing
- Decree issued on 04.04.1979 concerning the civil service regulations
- Decree No. 266 of 2006 on the establishment of the Central Agency for Information Technology and the amending decrees.
- The National Assembly has approved the following Law, which we have ratified and promulgated.

Chapter One
Definitions

Article (1)

In the implementation of the provisions of this Law, the following words and expressions shall have the meanings set forth next to each of them as follows:

Electronic: Anything related to information technology having electrical, digital, magnetic, optical, electromagnetic capabilities or similar capabilities whether wired or wireless and the technologies developed in this field.

Electronic Writing: All letters, numbers, symbols or any other sings affixed to an electronic, digital, optical media or any other similar means that have an understood significance and can be retrieved later.

Electronic Data: Any data with electronic characteristics in the form of texts, symbols, sounds, drawings, pictures, computer programs or databases.

Electronic data processing system: An electronic system for the creation, entry, retrieval, sending, receiving, extraction, storage, display or processing of information or electronic messages.

Electronic Medium: An electronic means and mechanism used in electronic information storage.

Electronic Document or Record: A collection of data or information created, stored, extracted, copied, sent, communicated or received completely or partially via electronic means, either through a hard medium or any other electronic medium, and can be retrieved in perceivable form.

Electronic Message: Electronic data sent or received through electronic means regardless of the extraction method upon receipt.

Creator: The natural individual or juridical person that sends the document or record via an electronic message, or that is found to having created or sent the document or record before saving it.

Shall not be considered a creator the person who provides services related to receiving, processing or saving the electronic document or record and other related services.

Addressee: The natural individual or juridical person to whom the creator intended to send the document or record.

Shall not be considered an addressee the person who provides services related to receiving, processing or saving the electronic document or record

and other related services.

Electronic Transaction: Any transaction or agreement entered into or executed fully or partially via electronic means and correspondence.

Automated Electronic System: An electronic computer software or system especially designed to independently initiate an action or respond to an action, completely or partially, without the intervention or supervision of any natural person at the time of initiating an action or responding to the same.

Electronic Signature: The data that take the form of letters, numbers, symbols, signs or others. Such data is necessarily listed in, attached to or associated with an electronic document or record through electronic, digital, optical or other means. The data has the nature that identifie and distinguishes the person who signed the document or record.

Protected Electronic Signature: The electronic signature fulfilling the conditions of Article (19) of this law.

Electronic Signature Tool: A program or electronic data prepared uniquely to work independently or jointly with other programs and electronic data on placing the electronic signature of a certain person on the document. Such process includes any systems or devices that generate or capture unique data such as symbols, algorithms, letters, numbers, private keys or profile identification numbers or properties.

Signatory: The natural individual or juridical person who owns the data and tool for the creation of an electronic signature. He shall sign for himself or on behalf of his deputy or legal representative the electronic document, record or message using such tool and data.

Electronic Payment: The process of transferring and paying money via electronic means.

Means of Electronic Payment: The means through which the person can make electronic payments.

Financial Institution: The bank, financial company or investment company "financing activity" or exchange company subject to the supervision of the Central Bank of Kuwait or any instruction authorized to make cash transfers or electronic payments in accordance with the provisions of the applicable laws.

Illegal Record: Any financial record on the account of the customer as a result of an electronic message sent in his name without his knowledge, consent or authorization.

Authentication Services Provider: The natural individual or juridical person who is authorized or licensed by the competent authority to issue electronic

authentication certificates, provide any other services or carry out tasks related thereto and to the electronic signatures and organized under the provisions of the law.

Electronic Authentication Certificate: A certificate issued by the licensee body, legalizing that the electronic signature is affixed by a specific person and confirming the relation between the person affixing the signature and the signature creation data, pursuant to accredited authentication procedures.

Time Stamp: The information provided by the authentication services provider, whereby the date and time of the creating, sending and receiving the electronic documents and messages is accurately specifies to be deemed an evidence against all.

The Competent Authority: The body which the state assigns to supervise the issuance of licenses necessary for carrying out electronic authentication and electronic signature services and other services in the field of electronic transactions and information.

Encryption: The process of converting a simple text, text document, or electronic message into encoded or scattered symbols that cannot be read without being decoded to the original status.

The Competent Minister: The minister assigned by the Council of Ministers.

Chapter Two
General Provisions

Article (2)

The provisions of this law shall govern the electronic records, messages, transactions, documents and signatures related to the civil, commercial and administrative transactions. They shall also govern any dispute arising out of the use of the same unless the parties agree otherwise or if it is found that another law is applicable.
However, the provisions of this law shall not apply to the following:

A. Transactions and issues related to personal status, endowment, and wills;
B. Real estate title deeds and the resulting original or consequential real rights;
C. Promissory notes and negotiable bills of exchange; and
D. Any event that the law requires to be expressed in a written document or to be documented or the making of which is subject to a specific provision in another law.

Article (3)

Each of the electronic record, document, message, transaction and signature, in the field of civil, commercial and administrative transactions, shall have the same legal effects of written records, documents, and signatures in terms of its binding effect upon the parties thereto or its force as proof or evidence whenever carried out pursuant to the provisions of this law.

Article (4)

No person is obliged to accept dealing through electronic means without his consent. The consent of the person shall be concluded through his positive behavior that the case circumstances shall leave no doubt in indicating. The approval of government bodies to electronic dealing should be explicit regarding the electronic data to which they are a party.

Article (5)

The approval, acceptance and all matters related to contracting, including any amendment, or recantation in approval or acceptance, may be expressed wholly or partially via electronic transactions. The expression shall not lose its

validity, effect or enforceability just because it has been carried out via one electronic correspondence or more.

Article (6)

The hard copy of the electronic document or record shall be deemed an evidence against all before the court for the official document, and shall be deemed an evidence against the person who placed his electronic signature on the unoffical document to the extent each of them confirms to the original document. The same applies whenever the electronic document or record and the electronic signature are uploaded to the electronic medium in accordance with the conditions set forth in Articles 19 and 20 of this law.

Article (7)

Provisions of the Law of Evidence in Civil and Commercial Matters shall govern the authentication of the official and unofficial electronic documents or records, their hard copies, the electronic signature and the electronic writing regarding what has not been provided for in this law or its executive bylaws.

Chapter Third
Document or electronic record

Article (8)

Two automated electronic systems including two electronic information systems or more may enter into a contract if such systems are pre-prepared and programmed to carry out such tasks. The contract shall be valid, in force and effective at law whenever its conditions have been fulfilled and whenever such systems carry out their tasks properly in spite of the absence of any personal or direct intervention by any natural person in the process of concluding the contract. The legal action may be completed between an electronic system, owned by a natural or a juridical person, and a natural person only if the later is aware or should have been aware of the fact that that system will complete this legal action.

Article (9)

The electronic document or record effective at law should fulfill the following conditions together:

A. The electronic document or record should be saved the way it was created, sent or received, or in any other way easy to prove the accuracy of data contained therein upon creation, sending or receiving.
B. The data contained in the electronic document or record should be maintainable and storable so as to be retrieved at any time.
C. The data contained in the electronic document or record should identify the creator or sender, date and time of sending or receiving the same.
D. The document or record should be saved in an electronic format pursuant to the conditions and rules set by the competent authority to which supervision of this activity is subject.

The provisions of this Article shall not prejudice the provision of any other law which explicitly stipulates saving the document, record, data or information in a specific electronic format according to a specific electronic processing system or following specific procedures, or sending the same via a specific electronic medium. Additionally, the provisions of this Article shall not be incompatible with any additional requirements established by the government concerning the storage of electronic records subject to its jurisdiction.

Article (10)

The data associated with the document or record for the purpose of facilitating its sending or receiving should not necessarily fulfill the conditions set forth in the preceding Article.

Any person may use the services of another person who obtains a license in storing and retrieving documents and data if required by law to be saved subject to the fulfillment of the conditions set forth in the preceding Article.

The provisions of the preceding Article shall not prejudice the provisions or other laws or any specific procedures established by the government concerning the storage of documents.

Article (11)

A. If the creator has himself issued the document or record.
B. If the addressee has used an election data processing system, which he has already, agreed with the creator to be used for this purpose.
C. If the addressee has received the electronic document or record as a result of procedures done by any person who belongs to the creator or his representative who have access to the electronic means used by either of them to identify the creator.

The electronic document or report may not be deemed an evidence against the creator in the two following cases:

1. If a notice is served to the addressee informing him that the electronic document or record is not issued by the creator. Therefore, the addressee should act on the basis that the creator has not issued the document or record. The creator shall hold the responsibility for any consequences that occurred prior to the receipt of such notice unless proven that the electronic document or record is not actually issued by the creator.
2. If the addressee becomes aware or was able to learn that the creator did not issue the electronic document or record.
3. The addressee shall have the right to consider each electronic message received as an independent correspondence. He shall act accordingly unless he learnt or was able to learn, if he exercised the due diligence of the natural person or used any agreed procedure, that the electronic message was a duplicate.

Article (12)

If the addressee is requested by the creator, by means of an electronic document or record, to serve a notice to the latter acknowledging the receipt of the electronic document or record or has agreed previously on the same, the addressee's notice to the creator served through an electronic means or any other means, or the taking of any act or procedure indicating that he received the electronic document or record shall be considered a consent to that request or an implementation of the agreement.

If the creator makes the effect of the electronic document or record conditional upon receiving a notice from the addressee acknowledging receipt of the electronic document or register, the electronic document or register shall have no legal effect unless such notice is received.

If the creator requested the addressee to serve a notice acknowledging the receipt of the electronic document or record and the latter did not serve such notice, the creator shall have the right, within a reasonable period, to serve a warning to the addressee informing him that he should send a notice within a specific period. Otherwise, the electronic document or record will be deemed void if the creator did not receive the notice within this period.

The notice acknowledging the receipt shall not be considered in itself an indication that the content of the electronic document or record that received by the addressee is identical to the content of the electronic document or record sent by the creator.

Article (13)

The electronic document or record shall not be binding to the addressee if the creator precludes the possibility of retrieving, printing, storing or maintaining the electronic document or record by the addressee.

Article (14)

The electronic document or record may be kept for the purposes of evidence, documentation or any other purpose. The same shall be considered an evidence binding the parties thereto, all unless a specific provision in another law requires the keeping of a written evidence.

Article (15)

The electronic document or record shall be deemed sent from the time it was entered into data processing system which is not subject to the control of

the creator or the person who sent the electronic document or record on his behalf unless otherwise agreed between the creator and addressee.
If the addressee has agreed with the creator on the electronic data processing system for receiving the electronic document or record, the same will be deemed delivered when entered to the system. If the message was sent to a system other than the one agreed upon, it shall be deemed sent from the time it was sent for the first time by the creator and seen by the addressee.
If the addressee did not agree with the creator on processing system to receive data messages, the time of messages receipt shall be the time it was entered to the electronic data processing system of the addressee. This applies if the creator and addressee were not using the same electronic data processing system, then the sending in this case shall be deemed complete from the time this electronic document or record came into the attention of the addressee.

Article (16)

The electronic document or record shall be deemed sent from the place where the creator's headquarter is located, and shall be deemed received in the place where the addressee's headquarter is located. If either has a headquarter, his place of residence shall be deemed his headquarter unless the creator of the electronic document or record and the addressee have agreed otherwise.
If the creator or the addressee had more than one headquarter, the headquarter more relevant to the transaction shall be deemed the place of sending or receipt. In case approximation was not possible, the principal headquarter of each shall be deemed the place of sending or receipt.

Article (17)

The time stamp affixed by the authentication services provider on any electronic document or record that is electronically signed, shall be deemed an evidence of date and time of creating, sending and receiving the electronic document or record.

Chapter Four
Electronic Signature

Article (18)

The legal effect of the electronic signature shall not be disregarded in terms of its validity and applicability merely because it is in an electronic form. The protected electronic signature in the domain of civil, commercial and administrative transactions shall have the same effect allocated to the written signature as stipulates in the provisions of the Law of Evidence in Civil and Commercial Matters whenever the technical controls set out in this law and the Executive By-law hereof in respect of the creation and completion thereof have been observed.

Article (19)

The signature shall be deemed a protected electronic signature if it meets the following conditions:

The possibility of identifying the signatory.

Exclusively linking the signature with the signatory himself.

The implementation of the signature using a sage signature tool under the exclusive control of the signatory himself at the time of signing.

The possibility of detecting any change in the data associated with the protected signature or in the relationship between the date and the signatory.

The Executive By-law of this law specifies the technical controls to do the same.

Article (20)

The person who uses the protected electronic signature shall submit the electronic authentication certificate indicating the validity of the signature pursuant to the nature of limitations and conditions imposed on the certificate; while taking the steps required to verify the validity of the signature, and the certificate and the validity thereof, and subject to to any agreement or past dealing of the party who relies on such certificate and the party that has certified the data contained therein or the party to which the issue of the certificate is attributed.

Article (21)

A. The signatory must take into account the following matters:

A. To take reasonable care and precaution to avoid the illegal use of his signature tool and data by others.
B. To initiate without delay to notify the competent authority or concerned persons, when he has sufficient evidence, that his electronic signature has been subject to unlawful use.
C. To pay careful attention in using the electronic authentication certificate, to ensure the accuracy and completeness of the significant data relevant to this certificate throughout the validity period thereof.

Article (22)

The competent authority referred to shall regulate carrying out electronic authentication services and electronic signature services, and proceeds in particular with the following:

A. To issue and renew licenses necessary for the conduct of electronic authentication services and electronic signature services, monitor and supervise the activities of electronic authentication services providers pursuant to the provisions of the law, the Executive B-law thereof and regulations of the authority.
B. To specify the standards of the electronic verification and the electronic signature with a view to setting the technical specifications thereof.
C. To receive complaints concerning the electronic verification and the electronic signature and take the necessary action.
D. To verify the technical advice on the dispute that may arise between the parties concerned with electronic verification and the electronic signature activities.

Article (23)

The Public Authority for Civil Information, in coordination with the competent authority, shall supervise the construction, design and management of the infrastructure of both the electronic authentication and signature in the State of Kuwait. The authorities set forth in the preceding Article of this law undertake the liaison and coordination with the Public Authority for Civil Information in accordance with the controls and conditions set by the Public Authority for Civil Information in coordination with the competent authorities in this regard.

Article (24)

The activity of issuing electronic authentication certificates may not be carried

out without obtaining the license from the competent authority pursuant to the procedures, conditions and guarantees set forth in the Executive By-Law of this Law. The licensee shall be responsible for the proper implementation of such procedures, conditions and guarantees. The said authority shall approve the foreign competent authorities in the field of electronic authentication certificates issuance in which case such certificates shall have the same strength as evidence allocated to the similar certificates issued by similar local issuers all pursuant to the rules and procedures set forth by the Executive By-law.

Article (25)

The competent authority shall, at any time, in the case of any violations, issue a decisions to cancel the license, withdraw the accreditation of the foreign authority specialized in the issuance of electronic authentication certificates, to stop the force of either until removing causes of the violations, especially in the following two cases:

A. Violating the terms of the license or accreditation,
B. Losing any of the conditions or guarantees on the basis of which the license or accreditation was granted. And such shall be applied pursuant to the procedures and laws set forth in the Executive By-law of this law.

Chapter Five
Use of the electronic documents and signatures by the government

Article (26)

Without prejudice to any of the provisions of any other law, any governmental entity may, for the purpose of carrying out its competencies, do the following:

A. Accept the deposit, submittal, creation or maintenance of documents in the format of electronic documents or records.
B. Issue any permit, license, decisions or approval in the format of electronic documents or records.
C. Accept the fees or any other payments settled electronically.
D. Offer government tenders of any type and receive the offers electronically.

Article (27)

If any governmental entity stipulates to perform any of the tasks set forth in the preceding Article electronically, it shall have the right to determine the following:

A. The method of format through which the electronic documents will be created, deposited, saved, submitted or issued without prejudice to the provisions of data privacy and protection.
B. The method, style, manner and procedures of offering tenders and receiving offers.
C. The type of the required electronic signature.
D. The method and format through which such electronic signature will be attached to the electronic document or record, as well as the standard to which the authentication service provider when it is given the document or record to maintain or deposit shall fulfill within the limit of standards and specifications set by the competent authority pursuant to Article 22 of this law and the Executive B-law thereof.
E. Appropriate control processes and procedures to ensure the integrity, security, and confidentiality of the electronic documents and records, payments or fees.
F. Any other properties, conditions or provisions which govern the process of sending paper documents, pursuant to what the Executive By-law of this law stipulates.

Chapter Six
Electronic Payment

Article (28)

Money transfer via electronic means is an acceptable way for settling payments. This law does not, in any way, affect the rights of others established under the laws or any other agreement.

Article (29)

Any financial institution which carries out electronic payment business pursuant to the provisions of this law and the Executive By-Law therefore, and the regulations issued thereto, shall comply with the following:

A. Adhere to the provisions of Law No. 32 of 1968 concerning cash, the Central Bank of Kuwait, regulation of the banking profession and other laws and instructions issued in this regard, and Law No. 106 of 2013 Anti-Money Laundering and Counter-Terrorism Financing.
B. Take the necessary procedures for the provision of safe services to the customers and maintain the banking secrecy in accordance with the legal standards followed in this regard.

Article (30)

The customer shall not hold the responsibility of any illegal record on his bank account by electronic payment if he initiates to inform the financial institution, before making such record, that he stopped the force of his electronic signature due to concerns that others might have access to this account, that he may lose the electronic payment means, or that it has been found that others have access to his electronic signature

The customer shall hold the responsibility for any illegal usage of his account by electronic payment if it is proved that his negligence has led or contributed basically and that the institution has done its duty to prevent the illegal use of that account.

In electronic payments, no amendment or change shall be made to the electronic document or record once sent by the creator. Any cancellations must be done using an independent electronic document or record.

Article (31)

The Central Bank shall issue the necessary instructions for the banking and

financial institutions subject to its supervision regarding the regulation of electronic payment including the adoption of electronic payment means; the consequences of the record resulting from the illegal transfer; procedures of errors correction and disclosure of data, and any other matters related to electronic banking including the data which the Central Bank obliges the financial institutions to provide according to the law.

The penalties set forth in Article 85 of the said Law No. 32 of 1968 shall apply to the institution violating the instructions.

Chapter Seven
Privacy and Data Protection

Article (32)

In none of the causes authorized by law, governmental bodies, agencies, public institutions, companies, non-governmental bodied or employees thereof may not unlawfully access, disclose or publish any personal data or information registered in the records or systems of electronic processing related to positional affairs, personal status, health status or elements of the financial disclosure of persons or other personal information registered at the authorities referred to in this Article or employees thereof by virtue of their positions, unless such was done with the approval of the concerned person to which such data or information belong or his legal representative or by means of a reasoned judicial statement.

The institutions referred to in the above paragraph of this article shall state the purpose of collecting the mentioned data and information. The collection of such data and information shall be carried out within the limits of this stated purpose.

Article (33)

Except for the personal data and information, which the government security bodies keep in its records and electronic processing systems for reasons of national security of the country, the person may request any of the above mentioned entities to access the personal data or information registered as set forth in the preceding article, if such information or data belong to him or any of his legal representatives. Hey may also obtain a formal extract of this data and information. The said bodies should respond his request.

The Executive By-law of this law sets forth the procedures and controls which govern the individual's access of such personal data and information.

Article (34)

Without prejudice to the provisions of preceding articles, government bodies, specific natural person and individuals may obtain from the bodies set forth in Article (32) above whatever they need of the information registered in their own records or electronic processing systems. Such shall be obtained subject to the approval of the concerned body after the verification of the applicant's status, nature of this data or information, usefulness or purpose of the same of

any other conditions deemed necessary.
The body to which the application is submitted, may reject the request and inform the applicant thereof within thirty days of submission. The lapse of the specifies period without deciding on the request will be considered a rejection thereof. The applicant may complain against the rejection decision to the president of the authority within sixty days from the date of his being notified of the rejection decision or the lapse of the period provided for in the preceding paragraph without deciding on the request.
The decisions of the head of the administrative body or the lapse of thirty days from the date of complain without deciding on the request shall be deemed a final decision of rejection.
The person who obtains any data pursuant to the provisions of this Article may not use the same for any purpose other than the purpose on which the body agreed to grant him the information.
The Executive By-law of this law sets forth the controls to be followed in this regard and the states fees thereof.

Article (35)

All bodies mentioned in Article (32) may not do the following:

A. Collect, register, or process any personal data or information of these mentioned in Article (32) in illegal methods or way or without the consent of the concerned person or his representative.
B. Use the referred personal data or information registered in their documents or information system for purposes other than those to which it was collected.

The bodies shall do the following:

A. Verify the accuracy of personal information or data stated in Article (32) and registered in their information systems, complete and update the same regularly.
B. Take the appropriate measure to protect the personal data and information referred to in Article (32) against loss, damage, disclosure, replacement with incorrect data or information, or addition of untrue information thereto.

Article (36)

A. Individuals are allowed to request the bodies referred to in Article (32) to delete or amend any of their personal data or information which the

bodies keep in their records or electronic processing systems if they were found to be invalid or non-conforming with reality. The Individuals may also request such information to be replaced according to the amendments thereto.

B. The Executive By-law of this law sets forth the procedures and controls that must be followed regarding the requests submitted by individuals for the deletion or amendment of their personal data registered at one of the aforementioned bodies.

Chapter Eight
Penalties

Article (37)

Without prejudice to any stricter penalty stipulates by any other law, shall be punished with imprisonment for a period of three years as a maximum and a fine of no less than five thousand dinars and not exceeding twenty thousand dinars as, or either of them, any person who:

A. Deliberately and illegitimately logs-in the electronic data processing system, prevents access to the system, causes damage of the same, or obtains the numbers or data of credit cards or other electronic cards to be used to steal the funds of others.
B. Issues an electronic authentication certificate or carries out any of the electronic authentication services without first obtaining a licenses from the competent authority.
C. Cases damage or defect to an electronic signature, system, signature tool, document or record or forged any of the same by way of synthesis, modification or alteration in any other way.
D. Knowingly uses a defective or false electronic signature, system, signature tool, document or record.
E. Unlawfully access, by any means, an electronic signature, system, document or record, breaks into the system, hinders or vacates the performance of the same.
F. Violates the provisions of Article 32 and items "a and b" of the first paragraph of Article 35 of this law. The tools, programs or devices used in the commission of this crime may be confiscated without prejudice to the rights of persons acting in good faith.

In all cases, the summary of the final judgment of convention shall be published in two daily newspapers issued in Arabic Language at the expense of the convicted person. The same shall be published on the open electronic communication network in accordance with the rules set forth by the Executive By-law.

The punishment shall be doubled in the event where any of the said crimes is repeated.

Article (38)

Shall be punished by imprisonment for a period of one year as a maximum and a fine not less than thousand dinars and not exceeding ten thousand

dinars as a maximum, or either of them, any licensee who obtains the license for providing electronic authentication services if he provides any incorrect data in the application for registration submitted to the competent authority or violates the terms of the license.

Article (39)

Without prejudice to the personal criminal responsibility of the perpetrator, the person responsible for the actual management of the juridical person shall be punished with the same penalties for the acts committed in violation of the provisions of this law if his negligence and breach of duties imposed by such managed have contributed to the occurrence of the crime knowingly.

The juridical person shall be jointly responsible for the judged financial penalties and compensation if the violation was committed by one of the employees working on behalf of this person or for him.

Article (40)

The public prosecution alone shall have jurisdiction over investigation, action and pleading in the crimes set forth under this Law and related crimes.

Article (41)

The competent personnel who are specifies by the competent minister in a resolution issued by him, shall have the judicial power to monitor the implementation of this law, by-laws and decisions implementing the same; write the necessary minutes in case of violation of its provisions; and forward the same to the public prosecution for investigation and taking action.

Article (42)

The public prosecution may accept the request for a conciliation submitted by the person who has committed, for the first time, one of the crimes provided for in this law whenever the accused submits a conciliation request to the public prosecution, and pays an amount of one thousand dinars to the treasury of the court before referring the case to the competent court. The acceptance of the conciliation request shall terminate the criminal case and all the effects thereof.

Article (43)

The provisions of this law shall not be included in the provisions of special legislations.

Article (44)

The competent minister shall issue the Executive By-law of this Law within a period of six months from the date of its publication in the Official Gazette.

Article (45)

The prime minister and ministers, each within his field of jurisdiction, shall enforce this law.

Article (46)

This Law shall be published and shall be effective from the date of the publishing hereof in the Official Gazette.

Amir of Kuwait

Sabah Al-Ahmad Al-Jabber Al-Sabah

Issued at Al-Seif Palace on 11 Rabi Al-Akhir 1435 AH

Corresponding to: 11 February 2014 AD

EXPLANATORY MEMORANDUM

Law No. 20 of 2014 Concerning

Electronic Transactions

The world is witnessing a tremendous development in the field of communications that are based on the exchange of information through modern communication network; either those that pass through the international telecommunications network (the Internet) or other means of communication and electronic systems technically linked with computers as a means for the exchanging, broadcasting, archiving and retrieving information. The access to such means has become available to the public. Transactions and exchange of information through these sophisticated electronic means has also become a broad concept that covers all the commercial, industrial, cultural, and legal activities and all areas of daily life.

Electronic trade transactions, like other electronic transactions conducted through the modern means of communication, doe not resort to paper documents, but rely on electronic messages, which consist of calculated information. Electronic trade transactions are also related to commercial activities with a broad concept which is not limited to electronic transactions undertaken by state agencies, bodies or institutions, companies or individuals. They as well serve the operations of an international nature due to the universality of the means of communication; namely (the Internet), linking all the countries simultaneously.

Electronic transactions have made an upward growth and now constitute a significant percentage of the total domestic and international transactions due to its speed in the conclusion and implementation of agreements, contracts and transactions, and because they provide instant connection and communication between the parties to the transaction.

Whereas Kuwait is one of the leading Arab countries in the introduction of modern systems for the development of economic and commercial aspects; and whereas it is preparing to be a global financial center seeking to apply the electronic government system in support of its overall development and advance the development and modernization of all spheres of life. Ever since, it became necessary to cope with this growing development in the electronic means of communication to be used in commercial transactions and others. Such required the preparation of a legalization to govern these transactions and set the appropriate rules and controls. Therefore, the attached law was

established to be consistent with the developed considerations and objectives. The law was established under the guidance of the model law adopted by the United Nations and the comparative electronic transaction laws in the Arab and Western countries.

The law includes eight chapters:

The first chapter in Article (1) included the definitions of technical term explaining its significance in the text of the law. Such definitions were meant to be flexible so as to accommodate any new modern technologies.

Chapter two of the Law included the general provisions. Article (2) included the scope of application and established the important role in the validity of the provisions of this law and the transactions governed by such provisions. Article (2) also specifies the types of areas, which are generally about everything related to electronic documents and signatures, governed by the provisions of this law. This Article established a significant rule which is respect of the both parties' agreement on choosing the application of the provision of this legalization or excluding the same pursuant to the principle of "control of the will". The Article also specifies the transactions and document which are not governed by the law exclusively and which are excluded from the scope of its validity due to its privacy that is inconsistent with the nature of this law; namely the matters of personal status, endowment, wills, deeds and transaction related to property rights or negotiable bills of exchange, or documents which the law requires to be in the form of official or authenticated documents.

Article (3) of the law stipulates the consideration of each of the electronic record, document, message, transaction and signature as effective at law whenever carried out pursuant to the provisions of this law.

Article (4) established the principle of "control of the will" in the acceptance of dealing through electronic means learnt from the positive behavior taken as an approval. The last paragraph of the Article was added requiring the explicit approval of the government bodies on electronic trading.

Article (5) established a significant principle regarding the validity of the hard copy of the electronic document or record as an evidence before the court; whether the document was official or unofficial to the extent the it matches the original as long as the electronic document or record exists on the medium.

Article (7) stipulates that the general rules of the Law of Evidence govern the validation of the official and unofficial electronic documents, electronic signature and electronic writing if nothing in this law or the Executive By-law thereof addresses such matters.

Chapter Three was concerned with the electronic document or record. It regulated the legal recognition of electronic documents or records in Articles 8 and 9. Article 8 allowed concluding a contract between electronic systems while Article 9 specifies the conditions of the electronic document effective at law. The last paragraph granted the government the right to add requirements for keeping electronic documents.

Article (10) did not require the availability of the conditions set forth in the preceding article in the information attached to the electronic document or record the purpose of which is to facilitate its sending and receiving.

Article (11) specifies the conditions of considering the document as an evidence and the cases where the same is not considered as an evidence against the creator. The last paragraph that considered each electronic message as an independent correspondence was added.

Article (12) regulated the notices of electronic document.

Article (13) stipulates that in order for the document to be binding on the addressee, he shall be able to print, store and keep the same.

Article (14) stipulates that document may be kept as an evidence or for documentation.

Article (15) addresses the time of entering the document to the electronic data processing system.

Article (16) stated that the document shall be sent from the place of the creator's headquarter.

Article (17) stated that the time stamp affixed by the electronic services provider shall prove the date, and time of the creation of the electronic document or record.

Chapter Four deals with the electronic signature. Article (18) specifies the legal effect of the electronic signature, and that it is equally effective in evidence to the written signature.

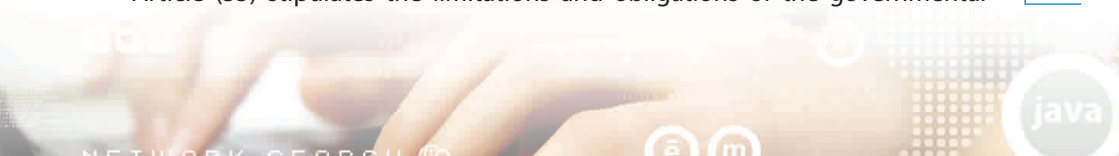
Article (19) identified the conditions of a protected electronic signature.

Article (20) stipulates the need to provide an electronic authentication certificate indicating the validity of the signature on the party of the signing party.

Article (21) stipulates the obligations of the signing party to take reasonable care, initiate informing the competent authority if he has any evidence on attacks on his electronic signature, and pay careful attention in using the electronic authentication certificate.

Article (22) stipulates that the competent authority is responsible for regulating carrying out electronic authentication services.

Article (23) is an added article that stipulates that the Public Authority for Civil Information, in coordination with competent authorities, is responsible for establishing and designing the basics of electronic authentication and signature in Kuwait.
Article (24) stipulates the conditionality of obtaining a license from the competent authority to carry out the issuance of electronic authentication certificates.
Article (25) stipulates that the competent authority shall have the right to cancel a license or withdraw an accreditation once the foreign authority for the issuance of electronic authentication certificates commits a violation.
Chapter Five came under the title of Use of the electronic documents and signatures by the government.
Article (26) stipulates that any governmental body may have the right to accept, submit or keep documents in order to perform its competence.
Article (27) gave the governmental body the right to determine the method of format in which electronic documents are to be saved or deposited.
Chapter Six handled electronic payment.
Article (28) addresses the acceptance of money transfer by electronic means.
Article (29) stipulates that every financial institution exercising electronic payment shall adhere to several restrictions.
Article (30) defines the negative and positive responsibility of the client. The client is not responsible for any illegal record on his bank account but he is responsible for the illegal use of his account via electronic payment if neglected.
Article (31) gave the Central Bank the authority of issuing instructions to the banking and financial institutions in relation to the regulations of electronic payment.
Chapter Seven was entitled "privacy and data protection". Article (32) addresses the confidentiality that the government bodies should keep in regard to the registered personal data and information.
Article (33) defines the exception that the security governmental bodies enjoy in storing data related to national security. Otherwise, the individuals have the right to obtain the extract of any official statement.
Article (34) stipulates the right of the governmental bodies and individuals in obtaining data and the extent of the estimation of the administrative body the approval of which is required to verify the position of the applicant, nature of data and the purpose thereof.
Article (35) stipulates the limitations and obligations of the governmental



bodies regarding electronic data.

Article (36) addresses the right of individuals to request the competent authorities stipulates in Article (32) to delete or amend personal information.

Chapter Eight addresses the new penalties and criminalization. Article (37) specifies the electronic crimes, which include the illegal log-in to the electronic data processing system, issuance of authentication certificates without a license, causing damage or impairment of the electronic signature, using a defective or false electronic signature, document or record knowingly, unlawfully accessing the electronic signature or system, or violating the provisions of Article (32) and items A and B of the first paragraph of Article (35). The penalty imposed thereon is an imprisonment of a period not exceeding 3 years and a fine not less than five thousand dinars and not exceeding twenty thousand dinars, or either of those penalties with the right of confiscation and publication.

Article (38) convicts the submission of invalid data in the registration application submitted by the licensee who obtains the license for providing electronic authentication services. The penalty imposed is an imprisonment of a period not exceeding 1 year and a fine not less than three thousand dinars and not exceeding ten thousand dinars, or either of these penalties.

Article (39) specifies the responsibility of the natural individual, and decides on punishing the person responsible for the actual management with the same penalties imposed due to the violations of the provisions of the law.

Article (40) grants the public prosecutor, alone, the jurisdiction over investigation, action and pleading in the crimes set forth under this Law and related crimes.

Article (41) grants the judicial to the competent personnel who are specified by the competent minister in a resolution issued by him.

Article (42) stipulates the admissibility of the public prosecution of the consolation request from the person who committed the crime for the first time.

Article (43) addresses the non-prejudice to the provisions contained in the legalizations.

Article (44) assigns the competent minister to issue of the Executive By-law.

Article (45) assigns the prime minister and ministers to enforce this law.

Article (46) stipulates that the law shall be published and shall be effective from the date of approving the Executive By-Law.