Decree Law No 16 of 2010 Promulgating the Electronic Transactions and Commerce Law

Law Summary Record ● **Type:** Decree ● **Number:** 16

● **Date:** 19/08/2010 Corresponding to 10/09/1431 Hijri ● **Number of Articles:** 77

● **Status:** In force

Official Gazette : ● **Issue:** 9 Offcial Journal Issue

● **Publication Date:** 28/09/2010 Corresponding to 20/10/1431 Hijri ● **Page from:** 18

We, Tamim Bin Hamad Al-Thani, Deputy Emir of the State of Qatar,
Having perused the Constitution,
Law No. 13 of 1990 concerning the Civil and Commercial Procedure Law and amending laws thereof,
The Civil Law No. 22 of 2004
Decree Law No. 36 of 2004 establishing the Supreme Council of Information and Communication Technology,;
The Trade Regulation Law No. 27 of 2006 as amended by Law No. 7 of 2010;
The Telecommunications Law promulgated by Decree Law No. 34 of 2006;
Law No. 8 of 2008 concerning Consumer Protection;
The proposal of the Supreme Council of Information and Communication Technology, and
The draft Law submitted by the Council of Ministers,
Hereby promulgate the following Law:

Issuance Articles

Article 1 - Introduction

The provisions of the electronic transactions and commerce Law enclosed herewith shall apply.

Article 2 - Introduction

Where no specific provision is provided for in the attached Law, electronic transactions and commerce shall be governed by the relevant legislation regulating each of them.

Article 3 - Introduction

The Supreme Council of Information and Communication Technology shall issue the by-laws and decisions to implement the provisions of the enclosed Law.

Article 4 - Introduction

All concerned authorities, each within its jurisdiction, shall implement this Law, which shall be published in the *Official Gazette*.

Chapter One

Definitions

Article 1

Article 1

In the application of this Law, the following terms and expressions shall have the meanings assigned to each of them unless the context requires otherwise:

"**Person**": means a natural or juristic person;

"**Supreme Council**": means the Supreme Council of Information and Communication Technology (SCICT);

"**Electronic**": means technology based on using electrical, electromagnetic or optical means or any other form of similar technological means;

"**Electronic communication**": means any communication of information by means of telecommunications;

"**Automated message**" means a computer system or any other electronic or automated means used to initiate or respond to electronic communications or related actions, in whole or in part, without review or intervention by a natural person;

“**Information system**”: means programs and devices for generating, sending, receiving, displaying, processing, or storing information;

“**Data message**”: means information generated, sent, received, processed, stored or displayed by one or more information systems or by means of electronic communication;

“**Accessible**”: means the capability to view, gain access to, retrieve, use or obtain information;

“**Originator**” of a data message: a person by whom, or on whose behalf, the data message has been sent, generated or stored, but it does not include a party acting as an intermediary with respect to that data message;

“**Addressee**”: means a person who is intended by the originator of the data message to receive the data message, but does not include a person acting as an intermediary with respect to that message;

“**Information**”: means information in the form of text, laws, images, speech or sound;

“**Personal information**”: means information about an individual whose identity is apparent or can reasonably be ascertained either from that information or from a combination of that information and other information;

“**Electronic signature**”: means the inscription affixed to a data message in the form of letters, numbers, symbols or tokens with a unique feature used to identify the signatory and distinguish him from others for the purpose of indicating the signatory's approval of the data message;

“**Signature-creation data**”: means information, laws or special encryption keys used by the signatory in the creation of the electronic signature;

“**Signatory**”: means the person legally entitled to access signature creation data and to act personally or on behalf of a person in using such information for the creation of the electronic signature;

“**Certification service provider**”: means a person licensed to maintain an infrastructure of public keys, to issue certification certificates and to provide services related to electronic signatures;

“**Certification certificate**”: means a document issued by a certification service provider that affirms the validity of the link between a signatory and the signature creation data;

“**Electronic transaction**”: means any deal, contract or agreement concluded or performed, in whole or in part, through electronic communications;

“**Relying party**”: means a person that acts on the basis of a certification certificate or an electronic signature;

“**e-Commerce service**”: means a service normally provided for consideration, or a service of a non-commercial nature, provided by means of any combination of an information system and any telecommunications network or telecommunications service, including electronic government services;

“**Service provider**”: means a person providing an electronic commerce service;

“**Place of business**”: means a non-transitory facility or installation used to carry on a business, including the provision of any service, exclusively used for that purpose;

“**Customer**”: means a person engaging in a transaction as part of an electronic commerce service;

“**Consumer**”: means a person who is acting for purposes other than those related to his trade, business or profession;

“**Telecommunications**”: any transmission, emission or reception of signs, signals, writing, images, sounds, pictures, data or information of any kind by wire, radio, optical, other electromagnetic means of communications or any other similar communication means;

“**Telecommunications network**”: means any wire, radio, optical or other electromagnetic system for routing, switching or transmitting telecommunications services between network termination points including fixed and mobile terrestrial networks, satellite networks, electricity or other utility transmission systems to the extent used for telecommunications, circuit or packet switched networks including those used for Internet Protocol services, and networks used for the delivery of broadcasting services including cable television networks;

“**Telecommunications service**”: means any form of transmission of signs, text, images or other by means of a telecommunications network, but does not include broadcasting services;

“**Internet Protocol**”: any of the set of communications protocols defining standards for Internet network interoperability, transmissions and related applications, including the “Transmission Control Protocol” “TCP” and the “TCP/IP” protocol suite;

“**Hosting services**”: means electronic services that provide users with capabilities for storing information on the information systems of the service provider and making stored information accessible to other users of electronic commerce services;

“**Caching**”: means the temporary storage of information in one or more information systems, whereby information is stored to enable access to it on a frequent basis;

.

Chapter Two

Application of the Law

Article 2

The provisions of this Law shall apply to transactions between parties who agree to conduct transactions using electronic communications.

The consent of the person may be inferred from that person's conduct.

The governmental entities shall give explicit consent in relation to electronic transactions of which they are a party.

The competent governmental entities may, if so decided to carry out any of their duties by means of electronic communications, specify additional requirements or specifications.

Article 3

The provisions of this Law shall not apply to the following documents and transactions:

instruments and documents relating to family matters and personal status;

instruments and documents related to real-estate incorporeal dispositions;

instruments and documents that are required by law to be authenticated;

negotiable commercial instruments in accordance with the provisions of the Trade Regulation Law.

Based on the resolution of the Council of Ministers, the recommendation of the Supreme Council and for the public interest, it may be deleted or added to any of the exempt matters stipulated in the above-mentioned paragraph.

Chapter Three

Requirements of Electronic Transactions

Article 4

When concluding contracts or conducting transactions, an offer or acceptance thereof, may be expressed in whole or in part, by means of data message transmitted through electronic communications.

The use of one or more data messages in concluding contracts or conducting transactions shall not prejudice the validity or enforceability thereof.

Article 5

The data message shall be deemed to have been sent by the originator if it was sent by the originator itself. A data message shall also be deemed to be sent by the originator in the following cases:

Where the data message was sent by a person who had the authority to act on behalf of the originator in respect of the data message whenever sent by an information system or automated message system programmed to operate by, or on behalf of, the originator.

Where the addressee properly applied a procedure previously agreed to by the originator for that purpose in order to ascertain whether the data message was that of the originator.

Where the data message as received by the addressee resulted from the actions of a person whose relationship with the originator or with any agent of the originator enabled that person to lawfully gain access to a method used by the originator to identify the data message as its own.

Article 6

A data message shall not be deemed originated from the originator in the following two cases:

where the addressee receives a notice from the originator that the data message is not from the originator and that there is reasonable time to act accordingly.

Where the addressee knows or should have known, had it exercised the reasonable diligence or any agreed procedure that the data message was not from the originator.

Article 7

In the framework of the relation with the originator, an addressee may rely on the data message issued by the originator and to act accordingly. The addressee may not rely on the aforesaid data message when the addressee knows or should have known, had the addressee exercised reasonable diligence or used any agreed procedure, that data message as received was a result of an error from the process of telecommunication.

Article 8

The addressee is entitled to treat each data message received as a separate data message, and to act accordingly, except to the extent that it duplicates another data message and the addressee knows or should have known, had it exercised reasonable diligence or used any agreed procedure, that the data message was a duplicate.

Article 9

Where the originator has requested or agreed with the addressee, on or before sending the data message that the receipt of the data message be acknowledged, the data message shall be deemed as received by the addressee once the aforementioned acknowledgement is received by the originator. This does not imply that the content of the data message as sent corresponds to the content as received

Article 10

Where the originator has not identified or agreed with the addressee that the acknowledgement be given in a particular form or by a particular method, an acknowledgement may be given by any communication by the addressee, automated or otherwise, or any conduct of the addressee, sufficient to indicate to the originator that the data message has been received.

Article 11

Where the originator has stated that the data message is conditional on receipt of the acknowledgement, the data message shall be treated as though it was not sent, until the acknowledgement is received.

Where the originator has not stated that the data message is conditional on receipt of an acknowledgement, and where an acknowledgement has not been received by the originator, the originator may give notice to the addressee stating that the earlier data message requires acknowledgement and specifying a reasonable time by which the acknowledgement must be received, and if the acknowledgement is not received within the time specified, the originator may, upon notice to the addressee, treat the data message as though it was not sent, or exercise any other rights it may have.

Article 12

Where the received acknowledgement states that the data message met technical requirements, either agreed upon or set forth in applicable standards, those requirements shall be deemed to have been met.

Article 13

The provisions of Articles 9, 10, 11 and 12 of this Law shall not exceed sending or receipt of the data message to the legal consequences of sending the data message or the acknowledgement thereof.

Article 14

Unless otherwise agreed between the originator and the addressee of the data message, the time of dispatching the data message shall be determined as follows:

Where the data message enters an information system outside the control of the originator;

Where the data message enters successively to two or more information systems outside the control of the originator, then, the dispatch time of the data message occurs when it enters the first of those information systems.

Article 15

Unless otherwise agreed between the originator and the addressee of the data message, the time of receipt of a data message shall be determined as follows:

Where the addressee has designated an electronic address for receiving the data messages, then, the time of receipt is when the data message is accessed by the addressee at that electronic address.

Where the data message has been sent to an address not designated by the addressee, then, the time of receipt is the time when the data message is accessed by the addressee or when retrieved by the addressee, whichever is earlier.

Article 16

Unless otherwise agreed between the originator and the addressee:

the data message shall be deemed to have been dispatched from the place where the originator has its place of business. The data message shall be deemed to have been received at the place where the addressee has its place of business;

where the originator or addressee has more than one place of business, the place of business that has a closer relationship to the specific transaction shall be the applicable place of dispatch or receipt;

where the originator or addressee has more than one place of business which don't comply with the provisions of the preceding paragraphs, the originator's or addressee's main office shall be the applicable place of dispatch or receipt;

where the originator or addressee does not have a place of business, the applicable place of dispatch or receipt shall be the place where the originator or addressee ordinarily resides.

Article 17

A location shall not be a place of business merely because that is where equipment or any other part of an information system used by a party in connection with a transaction is located or where an information system used by a party in connection with a transaction may be accessed by other parties.

Article 18

The sole fact that a party makes use of a domain name or electronic mail address connected to a specific country shall not create a presumption that its place of business is located in that country.

Article 19

Where a natural person makes an unintentional entry or any error in entering information in a data message exchanged with the automated message system of another party and the automated message system does not provide the person with an opportunity to correct the error, that person, or the party on whose behalf that person was acting, shall have the right to withdraw the portion of the data message in which the input error was made provided that the person or the party on whose behalf that person was acting:

notifies the other party of the error as soon as possible after having learned of the error;

where the input error relates to goods or services, not uses the goods or services or any benefit or material value thereof

Chapter Four

Effects and Authenticity of Electronic Transactions

Article 20

Information in the data message shall not lose its legal effect, validity or enforceability solely on the grounds that it is in the form of a data message.

Information in the data message shall also not lose its legal effect, validity or enforceability solely on the grounds that it is merely referred to in that data message without details, where the data message clearly identifies how to access the details of this information, and the information is accessible so as to be used for subsequent reference by every person that has a right to access and use the information and the method for accessing the information is clearly identified in the data message and does not place an unreasonable burden on any person that has a right to access the information.

Article 21

Where the law stipulates that an instrument, document or transaction be drawn up in writing or otherwise identifies certain consequences for non abidance, the instrument, document or transaction shall be deemed to have fulfils this condition, where the instrument, document or transaction are in the form of accessible data message.

Article 22

Where the law stipulates that an instrument, document or transaction must carry signature or otherwise identifies legal consequences for non abidance, a dully electronic signature pursuant to Article 28 of this Law shall fulfil this condition.

Article 23

Where the law stipulates that information be presented or retained in its original form or otherwise identifies legal consequences for non abidance, that requirement shall be deemed satisfied by presenting or retaining such information or document in the form of a data message provided that the following conditions are met:

The integrity and reliability of the information, from the time when it was first produced in its final form as a data message until the time that the information is subsequently accessed and presented, can be reasonably demonstrated.

The standard for assessing integrity of the data message in accordance with the preceding article shall be whether the information has remained complete and unaltered, apart from any change which arises from the mere communication, storage or display of the data message and which does not alter the content thereof. The reliability of the information shall be assessed in the light of the purpose for which the data message was produced and in the light of all other relevant circumstances.

The data message can be accessible so as to be used for subsequent reference by every person that has a right to access and use the information therein.

Article 24

Where the law stipulates that an information, instrument or document be retained or otherwise, identifies legal consequences for non abidance, such requirement shall deemed to have been met if the information, instrument or document are retained in the form of a data message, provided that the following conditions are met:

The information contained in the data message is accessible for subsequent reference by every person that has a right to access and use the information therein.

The data message is retained in the format in which it was originally produced, sent or received, or in a format that can be demonstrated to accurately represent the information contained therein as it was originally produced, sent or received.

Such information, if any exists, is retained as enables the identification of the origin and destination of the data message and the date and time when it was originally sent or received.

Article 25

Nothing shall prevent the acceptance of an instrument, document or transaction as evidence on the grounds that it is in the form of data message, albeit not in its original form if it is the only evidence that the person asserts.

Article 26

When assessing the evidential weight of information, instrument or a document in the form of a data message, regard shall be given to the following:

the processes and circumstances under which the data message was generated, stored or communicated;

the processes and circumstances under which the integrity of the instrument, document or information contained in the data message was maintained;

the processes and circumstances under which the originator of the data message was identified; and

any other relevant process or circumstances.

Article 27

A contract formed by the interaction of an automated message system and a natural person, or by the interaction of automated message systems, shall not be denied validity or enforceability on the sole ground that no natural person reviewed or intervened in each of the individual actions carried out by the automated message systems or the resulting contract.

Chapter Five

Electronic Signature

Article 28

An electronic signature shall have evidential weight if the following conditions are met:

the signature creation information are identified with the signatory and no other person;

the signature creation information were, at the time of signing, under the control of the signatory and of no other person;

any alteration to the electronic signature, made after the time of signing, is detectable;

where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to such information after the time of signing is detectable.

The Supreme Council shall issue decisions to determine which electronic signature processes and technologies satisfy the provisions of the preceding provisions.

Article 29

Where initiating an electronic signature, the signatory shall comply with the following:

exercise reasonable diligence to avoid unauthorised use of its signature creation information.

without undue delay, utilise means made available by the certification service provider pursuant to Articles 36 and 37 of this Law to notify any person that may reasonably be expected by the signatory to rely on the electronic signature or to take the necessary measures in support of the electronic signature if the signature creation information has been compromised, or circumstances give rise to a substantial risk that the signature creation information may have been compromised.

where a certification certificate is used to support the electronic signature, exercise reasonable diligence to ensure the accuracy and completeness of all material representations made by the signatory that are relevant to the certification certificate throughout its life cycle or that are to be included in the certification certificate.

Article 30

A signatory shall bear the legal consequences of its failure to satisfy the aforementioned requirements as stipulated in the preceding Article.

Article 31

A relying party shall bear the legal consequences of its failure to take reasonable steps to ensure that the requirements of the electronic signature stated in Article 28 herein have been met, or where an electronic signature is supported by a certification certificate, verify the validity, origin, suspension or revocation of the certificate, or any limitation thereon.

Article 32

An electronic signature shall be deemed legally effective, regardless of the geographic location where the electronic signature is created or used, or the geographic location of the place of business of the signatory.

Article 33

An electronic signature created or used outside the State of Qatar shall have the same legal effect in Qatar if the electronic signature offers an equal level of reliability that is not less than the level of reliability required under Article 28 of this Law.

Article 34

Without prejudice to Article 28 of the Law, parties may agree to the use identified types of electronic signatures provided that the agreement is valid under the law.

Chapter Six

Certification Service

Article 35

Where a certification service provider provides services to support an electronic signature, that certification service provider shall:

act in accordance with representations provided thereby with respect to its practices;

exercise reasonable diligence to ensure the accuracy and completeness of all material representations provided thereby that are relevant to the certification certificate throughout its validity or that are included in the certificate;

employ trustworthy systems, procedures and human resources in performing its services in accordance with the criteria determined by the Supreme Council.

Article 36

A certification service provider shall provide the signatory with means that enable the signatory to submit a notice that the signature creation information has been compromised and offer the signatory a timely revocation service.

Article 37

A certification service provider shall provide reasonably accessible means that enable a relying party to ascertain from the certification certificate the following:

the identity of the certification service provider;

that the signatory had control of the signature creation information at the time when the certificate of certification was issued;

that signature creation information was valid at or before the time when the certificate of certification was issued.

Article 38

A certification service provider shall provide reasonably accessible means that enable a relying party to ascertain the following:

the identity of the certification service provider;

any limitation on the purpose or value for which the signature creation information or the certificate may be used;

the method used to determine the identity of the signatory;

that the signature creation information is valid and have not been compromised;

any limitation on the scope or extent of liability stipulated by the certification service provider;

the method to give notice pursuant to this Law;

whether a timely revocation service is offered.

Article 39

The certification service provider shall revoke or suspend the certification certificate upon the request of the owner of the certificate or under any other circumstances that require suspension or revocation of the certificate. The Supreme Council shall issue a decision specifying those circumstances along with the criteria.

The certification service provider shall also immediately notify the owner of the certification certificate regarding the revocation or suspension of the certificate and the reasons therefor and shall cease the suspension or revocation should the reason no longer exists.

The certification service provider shall be responsible for the damages incurred by a person acting in good faith as a result of the failure on the part of the certification service provider to take action to revoke or suspend the certification certificate in the circumstances stated in the first paragraph of this Article.

Article 40

A certification service provider shall bear the legal consequences of its failure to comply with the requirements of the preceding Articles of this Chapter, including, but not limited to, the liability for damages caused to any person who reasonably relies on a certification certificate that is affected by the failure to comply. In assessing this liability of the certification service provider, the following factors shall be taken into account:

the cost of obtaining the certification certificate;

the nature of the information being certified;

the existence and extent of any limitation on the purpose for which the certification certificate may be used;

the existence of any statement or agreement limiting the scope or extent of the liability of the certification service provider;

any wrong doing by the relying party including negligence or misconduct.

Article 41

In determining whether a certification certificate is legally effective, no regard shall be given to the geographic location where the certificate is issued or where the place of business of the issuer is located.

Article 42

A certification certificate issued outside the State of Qatar shall have the same legal effect as a certificate issued in the State of Qatar if the certification certificate has been issued by an accredited certification service provider and offers a level of reliability that is at least equivalent to the level of reliability required under Articles 35, 36, 37, 38 herein.

The Supreme Council shall specify the criteria and the procedures regarding the adoption of the certification certificates issued by foreign entities outside the State of Qatar.

Article 43

Persons may agree to the use identified types of certification certificates provided that the agreement is valid under the law.

Article 44

The Supreme Council shall issue regulations and decisions to regulate the activity of the certification service providers and in particular the following:

the criteria and terms for issuing licenses necessary to carry out the activity of the certification service provider and their renewal, suspension, the licensing procedures, the term of license, its renewal, suspension, revocation, assignment thereof, the obligations of the licensee along with the criteria and procedures for the suspension of the activity of the licensee and the consequences arising therefrom;

accreditation schemes for certification service providers;

standards for the form and content of certification certificates and other service-related practices or procedures;

fees to be paid by certification service providers and the rules for determining such fees;

reporting or other notification procedures;

financial penalties and fines applicable to the breach of the regulatory rules governing the activities of the certification service providers.

Chapter Seven

Transmission and Storage of Information

Article 45

The electronic commerce service provider shall not be liable for the transmission of information of the electronic commerce service provided or requested by a user of the service or for the provision of access to a telecommunications network or telecommunications service, in the following cases:

the service provider does not initiate the transmission;

the service provider does not select the receiver of the transmission;

the service provider does not select or modify the information contained in the transmission.

The transmission and provision of access mentioned in the preceding paragraph shall include the automatic, intermediate and transient storage of the information transmitted for the sole purpose of carrying out the transmission in the telecommunications network and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.

Article 46

A service provider shall not be liable for the automatic, intermediate and transient storage of the electronic commerce service information provided by the user of the service, which is transmitted by means of a telecommunications network or service, in the following cases:

where such storage was made for the purpose of making more efficient transmission of the information to other users of the service upon their request; and

the service provider complies with the following:

does not make any modification to the information;

the conditions on access to the information;

the applicable rules regarding the updating of the information, recognized and used by similar service providers;

does not interfere with the lawful use of technology recognised and used by similar service providers, to obtain data on the use of the information;

acts without delay to remove or to disable access to the information stored when it actually knows that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled or that a court or a competent governmental entity has ordered such removal or disablement;

or the end user has selected a caching option in using the electronic commerce service that materially alters the cache configuration established by the service provider.

Article 47

The service provider that provides hosting services shall not be liable as a result of those services in the following cases:

Where the service provider does not have actual knowledge of unlawful activity or information associated with particular hosting services or is not aware of facts or circumstances which make it apparent that such activity or information was unlawful;

Where the service provider acts without delay to remove or to disable access to the affected services or information when the service provider knows of the unlawful activity or information associated with particular hosting services.

the service provider the user of the hosting service was not acting under the authority of the service provider or approval thereof.

Article 48

The preceding Articles 45, 46 and 47 shall not affect the legal obligations arising out of any contract.

Article 49

In applying the preceding provisions of paragraph 2(e) of Article 46 and paragraph 1 of Article 47, the actual knowledge of the electronic commerce service provider or the hosting service provider, as the case may be, shall be determined through all the relevant matters and circumstances including whether the service provider has received any notice identifying the following:

the full name and address of the sender of the notice;

details of the location of the information in question;

details of the unlawful nature of the activity or information in question.

Article 50

The preceding Articles stipulated in this Chapter shall not prejudice the right of the competent governmental entities, in accordance with the applicable legal procedures, to oblige the e- commerce service provider or a hosting service provider to take certain measures to inform them of any illegal information or activities and to request any information to determine the identity of the person engaging in such illegal activities and information.

Chapter Eight

Consumer Protection

Article 51

Without prejudice to the provisions of Law No. 8 of 2008 regarding Consumer Protection, a service provider shall make available to the users of its services and to any competent governmental entity in the form and manner which is easily, directly and continuously accessible, the following information:

the name of the service provider;

the address of the service provider;

contact information relating to the service provider, including its electronic mail address;

the details of the commercial register or any other equivalent means to identify the service provider, if the service provider was registered in a trade or similar register available to the public;

the details of the competent authority that the service provider is subject to, where the provision of the service requires an authorisation or license from that authority;

codes of conduct that the service provider is subject to and whether and how those codes can be viewed electronically;

any other information that the Supreme Council deems necessary in order to protect the consumers of the electronic commerce services.

Article 52

The service provider that exercises a regulated profession which requires a specific license or an authorisation to practice it, shall make available the following:

the details of professional entity or institution with which the service provider is registered;

the applicable professional title and the country where such title has been granted;

the professional rules or other rules applicable to the service provider in the country of authorisation or license, and the ways to access them;

any other information that the Supreme Council deems necessary to protect the consumers of the e- commerce services.

Article 53

Any electronic communication which constitutes or forms part of an e- commerce service of commercial nature, and is provided by a service provider, shall satisfy the following requirements:

be clearly identifiable as a commercial communication;

clearly identify the person on whose behalf the commercial communication is made;

regarding any promotional offers or competitions, the following requirements shall be satisfied:

be clearly and accurately identified;

clearly identify whether it includes any discounts, premium or gifts;

any conditions which must be met to qualify are not misleading or deceptive and presented clearly, unambiguously and are easily accessible;

shall not violate public order or public morals.

Article 54

The service provider shall not send, or require others to send, any electronic communications of commercial nature to any consumer without the explicit consent of the consumer regarding that dispatch.

The consent of the consumer regarding the dispatch shall be presumed to have been obtained in the case of an existing relationship with the service provider which meets the apparent expectation of the consumer to receive the electronic communication provided that the content of the electronic communication is relevant to the purpose for which this relationship has been established and provided that the service provider provides the addressee of the electronic communication with the appropriate opportunity and means to opt out from receiving any further electronic communications, at any time.

The Supreme Council may issue additional rules relating to unsolicited electronic communications.

Article 55

Where the electronic communication relates to an order to conclude a contract of commercial nature, a service provider shall, prior to an order being placed, furnish the consumer, in a clear and comprehensible manner, with the terms and conditions of the contract, including the following:

the technical steps required to conclude the contract

information regarding the service provider;

a description of the main characteristics of the services or goods;

the prices of services and goods, and whether they are inclusive of tax and delivery costs;

arrangements regarding payment, delivery and implementation;

the validity of the offer and the price;

whether the consumer has the right to cancel the order;

whether the contract will be stored or retained by the service provider, the accessibility, storing, copying and retention of the contract by the consumer and the means for that.

Article 56

Where the consumer of an e- commerce service places his/her order through electronic communications, a service provider shall comply with the following:

make available to the consumer of the service, appropriate, effective and accessible means which allow the consumer of the service to dtect and correct input errors before placing of the order;

acknowledge receipt of the order to the consumer of the service without undue delay and using appropriate electronic communications.

The order or the acknowledgement of receipt shall be deemed to be received when the parties to whom the order or the acknowledgement are addressed are capable of accessing them and the acknowledgement of receipt may take the form of the provision of an already paid service where that service is an e- commerce service.

Parties who are not consumers may agree otherwise.

Article 57

Save as otherwise agreed by the parties, the consumer shall have, where contracts have been concluded by electronic communications, the right to rescind or terminate the contract within three (3) days from the date of entering into the contract as long as the service provider does not fully implement the contract in a manner that serves the purpose of the contract during that time and the consumer does not use the goods or products which he/she receives nor receive any benefit or value from them.

Article 58

Unless the service provider and the consumer agree on another period for delivery or contract performance, the consumer may terminate the contract with a service provider where delivery or other performance of the contract is delayed for a period exceeding thirty (30) days and shall be entitled to a refund to any payments made by him/her under the contract for the products, services or other contract performance affected by this delay.

A consumer shall have no obligation to pay for any goods, products or services that were not ordered by him/her nor pay for the cost of returning such goods including any goods or products delivered to the consumer by the service provider by mistake.

A service provider shall have an obligation to notify the consumer of any delay or other difficulties experienced by it that have substantial effect on the contract performance.

Article 59

The service provider shall identify, at or before collection of such information, the purposes for which personal information about the customer is collected. The service provider shall not, except as permitted or required by law, or with the consent of the customer to which the personal information relates, collect, use, retain or disclose customer personal information for undisclosed or unauthorised purposes.

The service provider shall be responsible for any records of customer personal information or any records of customer electronic communications, in the custody or control of the service provider or its agents.

The service provider shall take reasonable steps to ensure that the personal information of the customer and related records are protected by security safeguards that are appropriate to their importance.

Chapter Nine

Powers of the Supreme Council

Article 60

In its capacity as the supreme authority entrusted with regulating the telecommunications and information technology matters, the Supreme Council shall act to enable the use of e-transactions and commerce in a simple manner and may in particular, for the purposes of achieving this, carry out the following:

oversee the provision, use and development of electronic transactions and commerce means;

issue, renew, suspend and terminate licenses and authorisations necessary in accordance with the provisions of this Law;

oversee the development of codes of conduct for the information technology sector and the practices of the service providers;

take appropriate legal actions and measures to ensure that service providers and other persons falling under the jurisdiction of this Law comply with the provisions of this Law, its regulations and its implementing decisions;

establish the criteria and framework for the protection of information including the personal information of the customer;

set the appropriate criteria and standards to protect the consumers that use electronic transactions or electronic commerce services

issue decisions to determine the fees for the licenses, authorisations and services provided by the Supreme Council and the rules for assessing the remuneration for those services in accordance with the provisions of this Law.

Article 61

The Supreme Council shall be solely responsible for the management of the ".qa" country-code top-level domain (ccTLD), and may delegate management of the ".qa" ccTLD to third parties.

The Supreme Council shall issue the decisions regarding management and mechanisms of domain names in the State of Qatar including imposition of any relevant fees or remuneration and shall set out the dispute resolution procedures relating to domain names.

Article 62

The Supreme Council may request from the service providers or other stakeholders in the field of electronic transactions and commerce, the necessary information for the exercise of its functions, in the form and manner and in the time specified thereby.

Article 63

The regulations, decisions, orders and rules issued by the Supreme Council pursuant to the provisions of this Law shall be transparent and non-discriminatory with respect to service providers and other participants in the field of electronic transactions and commerce.

Making any decisions in accordance with the provisions of this Law which have a different impact on any service provider or other participant in the field of electronic transactions and commerce shall not be deemed discriminatory, if such decisions are due to the different circumstances particular to each of them.

Article 64

A committee shall be established at the Supreme Council named "Grievances and Dispute Settlement Committee" and shall consist of a chairperson and a number of members of expertise.

A decision shall be issued by the Board of Directors of the Supreme Council naming the chairperson and members of the Committee.

The committee work system and the procedures applicable shall be issued by a decision of the Board of the Supreme Council.

Article 65

The Grievances and Dispute Settlement Committee shall carry out the following:

decide on grievances against decisions issued by the Supreme Council in accordance with the provisions of this Law;

resolve disputes that may arise between service providers in accordance with the provisions of this Law;

resolve disputes that may arise between service providers and users dealing with them in accordance with the provisions of this Law.

Article 66

A decision by the Grievances and Dispute Settlement Committee shall be final and the concerned parties may appeal the decision before the administrative circuit at the Court of First Instance.

No suit shall be accepted regarding any of the grievances or disputes stipulated for in the preceding Article, except after a decision is issued by the Committee, or sixty days from the date of the submission of the grievance or dispute to the Committee have lapsed without a decision thereon, whichever is earlier.

Chapter Ten

Offences and Penalties

Article 67

Without prejudice to any provision for a more severe punishment stipulated under any other law, any person who deliberately commits any of the following shall be subject to imprisonment not exceeding two (2) years and/or a fine not exceeding three hundred thousand (300,000) Riyals:

Unlawful access to any information system, data message or e- commerce service or related transaction, including by circumventing security measures and with the intent of obtaining information or making any other illegal use of the information system, data message or electronic commerce service or related transaction.

Providing false or misleading information to the Supreme Council or misusing the certification services.

Creating, publishing or using electronic signatures or certification certificates for unlawful purposes.

Destroying or damaging a data message, electronic signature, certification certificate or any other electronic medium.

Knowingly forging a data message, electronic signature, a certification certificate or any other electronic medium by imitation, modification, issuance or by any other means or using any of them.

Providing false information to the certification service provider or false electronic signature information to any party relying on this signature under this Law.

Illegally accessing, copying, reproducing or obtaining the electronic signature system or the signature creation data of another person.

Steeling the identity of a person or falsely claiming to represent him/her in applying for, accepting or requesting the suspension or revocation of certification certificate.

Publishing, circulating or providing a certification certificate that contains or refers to false information.

Intercept or commit illegal interference with any information system, electronic communication or electronic commerce service.

Carrying out the activity of the certification service provider without obtaining a License in this regard from the Supreme Council.

Violating any provision of Articles 51, 52, 53, 54, 55 and 59 herein.

Article 68

The court shall issue a ruling, in case of conviction according to this Law, in addition to any other penalty it sees appropriate to confiscate the tools used in committing the offence.

The court may issue a ruling to publish the conviction verdict in two daily wide-spread newspapers and on the open electronic information networks and at the expense of the convicted person.

Article 69

The person responsible for the actual management of the juridical person shall be punished with the same penalties assigned to the acts committed in violation of the provisions of this Law if proven that such person was aware of such acts or the breach of his/her duties rendered upon him/her by that management had contributed to the offence.

Article 70

In the case of conviction pursuant to the preceding Article, the corporate person overseeing the convicted shall pay the same fine stipulated under Article 67 of this Law or with a fine equal to that which imposed on the person responsible for the actual management, if convicted with a fine not imprisonment.

Article 71

The penalty shall be doubled in case of repetition of the violation. A person shall be considered a repeat offender if he/she committed any of the offences stipulated in this Law within three years from the date of the completion of the penalty or the penalty extinguishment period.

Article 72

The employees of the Supreme Council, who are vested with powers of law enforcement by a decision from the Public Prosecution in co-ordination with the Supreme Council, may seize and investigate actions committed in violation of the provisions of this Law and its implementing by-laws.

In this respect, they may enter related premises, have access to electronic records, documents, equipment and any other related things and request data or clarifications as they deem necessary and issue the relevant reports.

Article 73

The provisions of this Law shall apply to:

a person who commits outside Qatar an action that makes such person a perpetrator or an accomplice in an offence committed wholly or partially inside Qatar;

a person who commits inside Qatar an action that makes such person a perpetrator or an accomplice in an offence committed wholly or partially outside Qatar, if it is punishable under this Law and the law of the country where the offence took place.

Please do not consider the material presented above Official