This is an unofficial English translation of the Electronic Commerce and Transactions Law of the State of Qatar which will be adopted and applied by Supreme Council for Information and Communication Technology (ictQATAR). The Arabic version of the same Law is the definitive legal text.

Decree Law No. (16) of 2010 on the Promulgation of the Electronic Commerce and Transactions Law

We, Tamim Bin Hamad Al-Thani, Deputy Emir of the State of Qatar,

Having perused the Constitution,

The Civil and Commercial Code issued by Law No. (13) of 1990 and the laws amending it,

The Civil Code issued by Law No. (22) of 2004,

Decree Law No. (36) of 2004 Establishing the Supreme Council of Information and Communication Technology,

The Commercial Law issued by Law No. (27) of 2006, amended by Law No. (7) of 2010,

The Telecommunications Law issued by Decree Law No. (34) of 2006,

The Law No. (8) of 2008 regarding Consumer Protection,

The proposal by the Supreme Council of Information and Communication Technology, and

The draft law put forward by the Council of Ministers,

Have decreed the following:

Article (1)

The provisions of the Electronic Commerce and Transactions Law enclosed with this Law shall be effective.

Article (2)

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

Article (3)

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

Article (4)

All concerned authorities, each within its competence, shall implement this Law.
This Law shall be published in the Official Gazette.

Tamim Bin Hamad Al-Thani

Deputy Emir of the State of Qatar

Issued at the Emiri Diwan on: 9/9/1431 A.H.

Corresponding to: 19/8/2010 A.D.

This is an unofficial English translation of the Electronic Commerce and Transactions Law of the State of Qatar which will be adopted and applied by Supreme Council for Information and Communication Technology (ictQATAR). The Arabic version of the same Law is the definitive legal text.

ELECTRONIC COMMERCE AND TRANSACTIONS LAW

Chapter One

Definitions

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:

Accessible: the capability to view, gain access to, retrieve, use or obtain information.

Addressee: 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.

Automated message system: 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.

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

Certification certificate: a document issued by a certification service provider confirming the valid link between a signatory and the signature creation information.

Certification service provider: a person licensed to maintain public key infrastructure, to issue certification certificates and to provide related electronic signature services.

Commerce service: a service normally provided for remuneration, 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.

Consumer: a person who is acting for purposes other than those of his trade, business or profession.

Customer: a person engaging in a transaction as part of an electronic commerce service.

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

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

Electronic communication: any communication of information by means of telecommunications.

Electronic signature: letters, numbers, symbols or others affixed to a data message, which uniquely identify the signatory from others in order to indicate the signatory's approval on the data message.

Electronic transaction: any deal, contract or agreement concluded or performed, in whole or in part, through electronic communications.

Hosting services: 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.

Information: information in the form of text, codes, images, speech or sound.

Information system: programs and devices for generating, sending, receiving, displaying, processing, or storing information.

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.

"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.

Person: a natural or juridical person.

Personal information: 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.

Place of business: A non-transitory facility or installation used to carry on a business, including the provision of any service, exclusively used for that purpose.

Relying party: a person that acts on the basis of a certification certificate or an electronic signature.

Service provider: a person providing an electronic commerce service.

Signatory: a person that has legal right to access signature creation information, and acts either on its own behalf or on behalf of the person it represents to use the signature creation information to create an electronic signature.

Signature creation information: information, codes or private cryptographic keys used by the signatory to create an electronic signature.

Supreme Council: The Supreme Council of Information and Communication Technology.

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: 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: any form of transmission of signs, text, images or other by means of a telecommunications network, but does not include a broadcasting services.

Chapter Two

Application of the Law

Article (2)

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

1) documents relating to family and personal status.

2) documents that create interests in land.

3) documents that are required by law to be authenticated by the Notary Public.

4) negotiable commercial instruments in accordance with the provisions of the Commercial Law.

The Council of Ministers, based on the recommendation of the Supreme Council and for the public interest, may delete any of the exempt matters stipulated in the above-mentioned paragraph or add to them.

Chapter Three

Requirements of Electronic Transactions

Article (4)

In the context of contract formation or conducting transactions, an offer or acceptance of an offer may be expressed, in whole or in part, by means of electronic communications.

A contract or transaction shall not be denied validity or enforceability solely on the grounds that one or more electronic communications were used in its formation.

Article (5)

A data message is from and attributed to the originator if it was sent by the originator itself. A data message shall also be deemed to be that of the originator in the following cases:

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

2- if 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.

3- if 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 from the originator in the following two cases:

1- from the time when the addressee has received notice from the originator that the data message is not from the originator and had reasonable time to act accordingly.

2- the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the data message was not from the originator.

Article (7)

As between the originator and the addressee, an addressee may rely on the data message where the data message is from the originator and to act upon it. The addressee is not entitled to such reliance when it knew or should have known, had it exercised reasonable care or used any agreed procedure, that data message as received was subject to error resulting 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 on that treatment, except to the extent that it duplicates another data message and the addressee knew or should have known, had it exercised reasonable care 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 will be deemed as received by the addressee once the above-mentioned 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 is treated as though it was not sent, until the acknowledgement is received.

Where the originator has not previously 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, it is presumed that those requirements have been met.

Article (13)

Except in so far as it relates to the sending or receipt of the data message, Articles (9), (10), (11), (12) of this Law are not intended to determine the legal consequences that may flow either from that data message or from the acknowledgement of its receipt.

Article (14)

Unless otherwise agreed between the originator and the addressee of the data message, the dispatch of the data message occurs as follows:

1- when the data message enters an information system outside the control of the originator.

2- if the data message enters successively two (2) or more information systems outside the control of the originator, then, the dispatch 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 is determined as follows:

1- if the addressee of the data message has designated an electronic address for the purpose of receiving data messages, then, the time of receipt is when the data message is accessible by the addressee at that electronic address.

2- if the data message has been sent to the address of the addressee not designated by the addressee, then, the time of receipt is the time when the data message is accessible by the addressee or when retrieved by him/her, whichever is earlier.

Article (16)

Unless otherwise agreed between the originator and the addressee:

1- the data message is taken to have been dispatched at the place where the originator has its place of business. The data message is taken to have been received at the place where the addressee has its place of business.

2- if the originator or addressee has more than one place of business, the place of business that has a closer relationship to the underlying transaction shall be the applicable place of dispatch or receipt.

3- if the originator or addressee has more than one place of business and the provisions of the preceding paragraphs do not apply, the originator's or addressee's principal place of business shall be the applicable place of dispatch or receipt.

4- if 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 is not 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 does 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, has 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:

1- notifies the other party of the error as soon as possible after having learned of the error.

2- has not used or received any material benefit or value from the goods or services received from the other party that are the subject of the input error.

Chapter Four

The Effect and Evidential Weight of Electronic Transactions

Article (20)

Information in the data message shall not be denied legal effect, validity or enforceability solely on the grounds that they are in the form of a data message.

Information in the data message shall also not be denied legal effect, validity or enforceability solely on the grounds that it is merely referred to in that data message without details, provided that the data message clearly identifies how to have access to the details of this information, 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 any law requires information or a document to be in writing or identified consequences for the information or document not being in writing, that requirement is satisfied where the information or document is in the form of a data message, provided that the information or document is accessible so as to be used for subsequent reference by every person that has a right to access the information or document.

Article (22)

Where any law requires the signature of a person or identified consequences for the absence of the signature of a person, that requirement is satisfied if the conditions stipulated in Article (28) of this Law are met.

Article (23)

Where any law requires certain information or a document to be presented or retained in its original form or identified consequences for the information or document not being in its original form, that requirement is satisfied by presenting or retaining such information or document in the form of a data message provided that the following conditions are met:

1- 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.

2- 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 information and which does not alter the content of the information or document, and the reliability of the information or document shall be assessed in the light of the purpose for which the information or document was produced and in the light of all other relevant circumstances.

3- the data message is accessible so as to be used for subsequent reference by every person that has a right to access and use the information or document.

Article (24)

Where any law requires information or a document to be retained or stored and identified consequences for the information or document not being retained, that requirement is satisfied by retaining such information or document in the form of a data message, provided that the following conditions are met:

1- the information or document contained in the data message is accessible for subsequent reference by every person that has a right to access and use the information or document.

2- 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 in the data message as it was originally produced, sent or received.

3- 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 apply so as to prevent the admissibility of information or a document as evidence on the grounds that it is in the form of data message, or on the grounds that it is not in its original form if it is the only evidence that the person adducing it could be expected to obtain.

Article (26)

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

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

2. the processes and circumstances under which the integrity of the information or document contained in the data message was maintained.

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

4. 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:

1- the signature creation information are identified with the signatory and no other person.

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

3- any alteration to the electronic signature, made after the time of signing, is detectable.

4- 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 that 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 signature creation information is created by the signatory, each signatory shall comply with the following:

1- exercise reasonable care to avoid unauthorized use of its signature creation information.

2- without undue delay, utilize 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.

3- where a certification certificate is used to support the electronic signature, exercise reasonable care 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 above-mentioned requirements 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) of the Law have been met, or where an electronic signature is supported by a certification certificate, to verify the validity, origin, suspension or revocation of the certificate, or any limitation with respect to the certificate.

Article (32)

An electronic signature is 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 it 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 of 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:

1- act in accordance with representations made by it with respect to its practices.

2- exercise reasonable care to ensure the accuracy and completeness of all material representations made by it that are relevant to the certification certificate throughout its life cycle or that are included in the certificate.

3- 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 have 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:

1- the identity of the certification service provider.

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

3- 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:

(1) the identity of the certification service provider.

(2) any limitation on the purpose or value for which the signature creation information or the certificate may be used.

(3) the method used to determine the identity of the signatory.

(4) that the signature creation information is valid and have not been compromised.

(5) any limitation on the scope or extent of liability stipulated by the certification service provider.

(6) the method to give notice pursuant to this Law.

(7) 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:

1- the cost of obtaining the certification certificate.

2- the nature of the information being certified.

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

4- the existence of any statement or agreement limiting the scope or extent of the liability of the certification service provider.

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

Article (41)

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

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) of this Law.

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)

Parties may agree to the use of identified types of certification certificates provided that the agreement itself 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:

1- 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 of it, 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.

2- accreditation schemes for certification service providers.

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

4- fees to be paid by certification service providers and the rules for determining such fees.

5- reporting or other notification procedures.

6- 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:

1- the service provider does not initiate the transmission.

2- the service provider does not select the receiver of the transmission.

3- 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 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:

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

2- the service provider complies with the following:

A. does not make any modification to the information.

B. the conditions on access to the information.

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

D. 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.

E. 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.

3- 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:

1- 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.

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

3- the user of the hosting service was not acting under the authority of the service provider or with its approval.

Article (48)

The preceding Articles (45), (46) and (47) shall not affect 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:

1. the full name and address of the sender of the notice.
2. details of the location of the information in question.
3. details of the unlawful nature of the activity or information in question.

Article (50)

The preceding Articles stipulated in this Chapter do not limit the right of the competent governmental entities, in accordance with the applicable legal procedures, to oblige the electronic 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 information or activities.

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:

1- the name of the service provider.

2- the address of the service provider.

3- contact information relating to the service provider, including its electronic mail address.

4- 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

5- the details of the competent authority that the service provider is subject to its supervision, where the provision of the service requires an authorisation or license from that authority.

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

7- 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:

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

2. the applicable professional title and the country where that title has been granted.

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

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

Article (53)

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

1- be clearly identifiable as a commercial communication.

2- clearly identify the person on whose behalf the commercial communication is made.

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

A. be clearly and accurately identified.

B. clearly identify whether it includes any discounts, premium or gifts.

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

4- 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, provide the consumer, in a clear and comprehensible manner, with the terms and conditions of the contract, including the following:

1. the technical steps required to conclude the contract.
2. information regarding the service provider
3. a description of the main characteristics of the services or goods.
4. the prices of services and goods, and whether they are inclusive of tax and delivery costs.
5. arrangements regarding payment, delivery and implementation.
6. the validity of the offer and the price.
7. whether the consumer has the right to cancel the order.
8. 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 electronic service places his/her order through electronic communications, a service provider shall comply with the following:

1- make available to the consumer of the service appropriate, effective and accessible means which allow the consumer of the service to determine and correct input errors before placing of the order.

2- 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 they are addressed are capable of accessing it and the acknowledgement of receipt may take the form of the provision of an already paid service where that service is an electronic commerce service.

Parties who are not consumers may agree otherwise.

Article (57)

Unless the parties agree otherwise, 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)

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

(1) oversee the provision, use and development of electronic commerce and transactions means.

(2) issue licenses and authorisations necessary in accordance with the provisions of this Law and renew, suspend and terminate them.

(3) oversee the development of codes of conduct for the information technology sector and the practices of the service providers.

(4) 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.

(5) establish the criteria and framework for the protection of information including the personal information of the customer.

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

(7) 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 another.

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 require service providers or others in the field of electronic commerce and transactions to provide information necessary for exercising its powers, and the information shall be furnished in the form, manner and time as the Supreme Council specifies.

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 commerce and transactions.

Making any decisions in accordance with the provisions of this Law which a have different impact on any service provider or other participant in the field of electronic commerce and transactions 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 chairman and a number of members of expertise.

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

The Board of the Supreme Council shall issue the committee work system and the procedures applicable before it.

Article (65)

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

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

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

3- 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 to 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 on it, whichever is earlier.

Chapter Ten

Crimes 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:

(1) Unlawful access to any information system, data message or electronic 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.

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

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

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

(5) 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 with knowledge of forgery.

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

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

(8) 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.

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

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

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

(12) Violating any provision of Articles (51), (52), (53), (54), (55) and (59) of this Law.

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 crime.

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 crime.

Article (70)

In the case of conviction pursuant to the preceding Article, the juridical person that the person convicted follows 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 crimes 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 judicial seizure by a decision from the Attorney General in co-ordination with the Supreme Council, may seize and prove actions committed in violation of the provisions of this Law and in its implementing decisions.

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:

1- to a person who commits an action outside Qatar that makes him/her a perpetrator or an accomplice in a crime committed wholly or partially inside Qatar.

2- to a person who commits an action inside Qatar that makes him/her a perpetrator or an accomplice in a crime committed wholly or partially outside Qatar, if it is punishable under this Law and the law of the country where the crime took place.