Cloud Computing

Regulatory Framework

Version 2

Table of Contents

1. Introduction

1.1 Pursuant to Article 3 of the Telecom Act (the 'Act') the telecommunications sector must be regulated to, among other objectives, 'ensure creation of favorable atmosphere to promote and encourage fair competition in all fields of telecommunications.'

1.2 Council of Ministers Resolution no. 133 dated 21/5/1424H confirmed that the powers of the Communications and Information Technology Commission (the 'Commission') extend into information technology, requiring the Commission to:

1.2.1 Implement the policies, plans and programs approved for the development of information technology and set out the appropriate procedures.

1.2.2 Propose regulations and their amendments related to information technology, and pursue approval of these regulations from the appropriate authorities.

1.2.3 Issue the necessary licenses in accordance with the terms and acts related to them.

1.3 The Information and Communications Technology (ICT) sector is undergoing rapid change. Adoption, by the Commission, of the present Regulatory Framework on Cloud Computing will generate benefits by encouraging Cloud Computing Services in the Kingdom and providing increased regulatory clarity.

2. Definitions

2.1 The terms and expressions defined in the Act and its Bylaw shall have the same meaning in this Regulatory Framework.

2.2 The following terms and expressions shall have the meaning assigned to them hereunder:

2.2.1 'Cloud Computing' shall mean the use of a scalable and elastic pool of shareable physical or virtual resources (such as servers, operating systems, networks, software, applications, and storage equipment) with self-service provisioning and administration on-demand.

2.2.2 'Cloud Computing Services' (or 'Cloud Services') shall mean information and communications technology (ICT) services provided through Cloud Computing, which include, but are not limited to, the storage, transfer or processing of Customer Content in a Cloud System. The mere storage and processing of customer information (such as the name, contact details or information on past transactions) by a Person who provides services to these customers other than Cloud Computing Services does not constitute a Cloud Computing Service.

2.2.3 'Cloud Service Provider' ('CSP') shall mean any Person providing Cloud Services to the public either directly or indirectly, such as a Cloud Provider, Cloud Broker, Cloud Aggregator, reseller or agent of a Cloud Provider, whereby:

2.2.3.1 'Cloud Provider' shall mean any Person providing Cloud Services to the public through Datacenters it owns and/or manages itself, in whole or in part.

2.2.3.2 'Cloud Broker' shall mean any Person that acts as an intermediary between one or more CSPs and Cloud Customers.

2.2.3.3 'Cloud Aggregator' shall mean a type of Cloud Broker that packages and integrates several Cloud Services into one or more composite services that it offers to Cloud Customers.

2.2.4 'Cloud Customer' shall mean any Person to which a CSP agrees to provide Cloud Services based on a Cloud Contract or other business relationship between the CSP and that Person.

2.2.5 'Cloud User' shall mean any individual person making use of a CSP's Cloud Services provided to a Cloud Customer, based on a relationship between that Cloud Customer and the Cloud User. An individual person can be both a Cloud User and a Cloud Customer if the Cloud Contract is concluded for the provision of Cloud Computing Services to a single Cloud User.

2.2.6 'Cloud Contract' shall mean an agreement for the provision of Cloud Services, concluded between a CSP and a Cloud Customer.

2.2.7 'Cloud System' shall mean an electronic information system comprising hardware, software and networking elements that are owned, controlled, operated, leased or otherwise relied on by a CSP to supply Cloud Services to Cloud Customers. A Cloud System may comprise one or more Datacenters, among other elements.

2.2.8 'Public Cloud' shall mean a Cloud System provisioned for open use by the public.

2.2.9 'Community Cloud' shall be a Cloud System provisioned for the exclusive use of a closed group of Cloud Customers sharing certain social, business, administrative or other objectives.

2.2.10 'Private Cloud' shall mean a Cloud System provisioned for the exclusive use of a single Cloud Customer.

2.2.11 'Hybrid Cloud' shall mean a combination of two or more Cloud Systems (Private, Public and/or Community Clouds) that are bound together by standardized or proprietary technology that enables data and application portability.

2.2.12 'Datacenter' shall mean a facility consisting of computing infrastructure and supporting components, which are housed in the

same location and used, at least in part, for the storage and/or processing of Customer Content and Customer Data.

2.2.13 'Content' shall mean any software, text, files, audio, video, images, graphics, animations, illustrations, information, personal, business or other data, in any format.

2.2.14 'Customer Content' shall mean any Content provided or generated by a Cloud Customer that is stored or processed in a Cloud System pursuant to a Cloud Contract for the provision of Cloud Services through that Cloud System to that Cloud Customer.

2.2.15 'Customer Data' shall mean any data falling under at least one of the following categories, insofar as that data are, or have been, part of the Customer Content or are, or have been, generated by the CSP with regard to one or more of its Cloud Customers or Cloud Users:

2.2.15.1 any data relating to a Cloud User that is or can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors which allow that Cloud User to be identified;

2.2.15.2 any data relating to a Cloud Customer's business activities, business information or financial affairs. Such data can include, for example, the Cloud Customer's prices, data on its personnel, product or client lists, its financial, audit and security data, and its business and product development data, even if such data or other information are in the public domain. Notwithstanding the above, a CSP may exclude some or all of a Cloud Customer's business data from the above definition of Customer Data, subject to the Cloud Customer's prior consent;

2.2.15.3 any data generated by, or for, the CSP concerning the Cloud Customer's activity log, billing, usage volume, statistics or other Cloud Customer-specific information associated with its use of the Cloud Services offered by the CSP.

2.2.16 'Customer Address' shall mean a Cloud Customer's (i) address provided in the Cloud Contract or (ii) invoicing address, and if the two are different and only one of them is in the KSA, Customer Address shall mean that address.

2.2.17 'Third Party Content' shall mean any Content, in electronic form, obtained or derived from any Person other than the CSP or the Cloud Customer and made available to the Cloud Customer through, or in conjunction with, the Cloud Customer's use of the Cloud Services. Such Content can include, without limitation, data, information, software, documents, images, audio or video.

2.2.18 'Unlawful Content' shall mean Customer Content or Third Party Content that is unlawful under the laws of the Kingdom.

2.2.19 'Infringing Content' shall mean Customer Content or Third Party Content that infringes a Person's intellectual property rights.

2.2.20 'Residence' shall mean a permanent or temporary residence in the Kingdom under the Kingdom's laws. It shall not include a temporary presence of Persons on a short visit or transiting through the Kingdom.

2.2.21 'Service Credits' shall mean compensation mechanisms offered by a CSP to a Cloud Customer if the CSP's actual performance fails to meet the standards that are set in the Cloud Contract or are otherwise required under this Regulatory Framework. Examples of Service Credits can include discounts on current or future bills, and time of Cloud Services added at the end of a billing cycle free of charge.

2.2.22 'Service Level Agreement' shall mean an agreement between a CSP and a Cloud Customer that defines the quality of the Cloud Services to be delivered to that Cloud Customer in terms of a set of measurable properties specific to Cloud Computing.

3. Regulatory Framework

3.1 Scope

3.1.1 The provisions of this Regulatory Framework shall apply with regard to any Cloud Service provided to Cloud Customers having a Residence or Customer Address in the Kingdom.

3.1.2 Regardless of the Cloud Customers' Residence or Customer Address, the processing or storage of any Customer Content and Customer Data, permanently or occasionally, in Datacenters or other elements of a Cloud System that are located in the Kingdom shall be subject to the provisions listed below:

3.1.2.1 Article 3.3.13 (reporting on major information security breaches), below;

3.1.2.2 Articles 3.5.4 and 3.5.5 ('take-down' of Unlawful Content or Infringing Content, upon the Commission's or other authorized entities' notice or by own initiative), and 3.5.6 (notification of violations of Anti-Cyber Crime Law), below; and

3.1.2.3 The exception referred to in Article 3.4.3.1, below.

3.1.3 Any obligations resulting from Article 3.1.1, above, shall be binding on the CSP who has concluded the Cloud Contract with the Cloud Customer(s) in question.

3.1.4 Unless specified otherwise in this Regulatory Framework, these provisions shall be mandatory and not subject to any modification through contractual agreement.

3.2 Registration requirements

3.2.1 No Person may engage in the exercise of direct or effective control over Datacenters or other critical Cloud System infrastructure hosted in the Kingdom and used, in whole or in part, for the provision of Cloud Services before making a valid and complete registration with the Commission.

3.2.2 The information to be provided for the above registration, the form to be used, and the applicable procedure and time limits shall be determined by decision of the Commission.

3.3 Information security

Customer Content

Classification

3.3.1 Customer Content can be subject to different levels of information security, depending on the required level of preservation of the Customer Content's confidentiality, integrity and availability, as defined in the table below and subject to the provisions of Articles 3.3.4 to 3.3.6, below:

Classification of Customer Content by level of required information security	Categories of Customer Content
Level 1	• Non-sensitive Customer Content of individuals or private sector companies, not subject to any sector-specific restrictions on the outsourcing of data. • Customer Content qualifying for Level 2 or Level 3 treatment, for which the Cloud Customer elects Level 1 treatment.
Level 2	• Sensitive Customer Content of individuals, not subject to any sector-specific restrictions on the outsourcing of data. • Sensitive Customer Content of private sector companies or organizations, not subject to any sector-specific restrictions on the outsourcing of data. • Non-sensitive Customer Content from public authorities. • Customer Content qualifying for Level 1 or Level 3 treatment, for which the Cloud Customer elects Level 2 treatment.
Level 3	• Any Customer Content from private sector-regulated industries subject to a level categorization by virtue of sector-specific rules or a decision by a regulatory authority • Sensitive Customer Content from public authorities. • Customer Content qualifying for Level 1 or Level 2 treatment, for which the Cloud Customer elects Level 3 treatment

Level 4	Highly sensitive or secret Customer Content belonging to relevant governmental agencies or institutions

3.3.2 This Regulatory Framework shall be without prejudice to any rules applying to any Customer Content requiring a higher level of information security, including but not limited to Level 4 Customer Content, as may be determined by other competent authorities of the Kingdom.

3.3.3 The provisions of this Regulatory Framework shall be without prejudice to any applicable law, regulation, guideline, code of conduct, internal instruction, corporate policy or any other legal, regulatory, administrative or corporate rule, concerning:

3.3.3.1 the Cloud Customers' right, if any, to outsource, transmit, process or store in a Cloud System Customer Content or any data or information;

3.3.3.2 the Cloud Customers' obligation to ensure that, if allowed, any such outsourcing, transmission, processing or storage should be subject to certain information security or data protection restrictions or safeguards, in addition to those specified to this Regulatory Framework.

Responsibility for Customer Content Classification

3.3.4 Cloud Customers must presume that the following levels of information security apply by category of Cloud Customer:

3.3.4.1 for natural persons with a Residence in the Kingdom: Level 1;

3.3.4.2 for private sector legal persons, such as companies, other corporate entities, associations or organizations incorporated or with a Customer Address in the Kingdom: Level 2;

3.3.4.3 for any government or State services or agencies: Level 3;

3.3.4.4 for all other categories: Level 1.

3.3.5 Cloud Customers shall be responsible for selecting the information security level among those listed in the table of Article 3.3.1 or other similar list provided for such purpose by the CSP, which best matches their specific needs, duties, obligations and security requirements.

3.3.6 Cloud Customers shall be responsible for implementing all information security features required for part or the whole of their Customer Content.

Transfer and location of Customer Content

3.3.7 CSPs must inform any Cloud Customer, upon his request, of the information security features offered by the CSP or applied to the Cloud Customer's Customer Content. CSPs may also satisfy this obligation by making such information available in online format for Cloud Customers.

3.3.8 Cloud Customers must ensure that no Level 3 Customer Content is transferred outside the Kingdom, for whatever purpose and in whatever format, whether permanently or temporarily (e.g. for caching, redundancy or similar purposes), unless this is expressly allowed under the laws or regulations of the Kingdom, other than this Regulatory Framework.

3.3.9 Cloud Customers may not transfer, store or process Level 3 Customer Content to or in any Public Cloud, Community Cloud or a Hybrid Cloud, unless and for as long as the CSP is validly registered with the Commission pursuant to article 3.2, above.

3.3.10 Regardless of the level of information security (if any) required by the relevant Cloud Customer, CSPs registered under article 3.2 above must disclose to the Commission:

3.3.10.1 The location and main features of any of its Datacenters that are located in the Kingdom, and

3.3.10.2 The foreign country or countries of the location of any of its Datacenters used for the processing, storage, transit or transfer of Customer Data or Customer Content of Cloud Customers that have a Residence or Customer Address in the Kingdom.

3.3.11 Without prejudice to their obligations under Article 3.3.7, CSPs must inform their Cloud Customers in advance whether their Customer Content will be transferred, stored or processed outside the Kingdom, permanently or temporarily.

Reporting of security breaches

3.3.12 CSPs must inform Cloud Customers, without undue delay, of any security breach or information leakage that those CSPs become aware of, if such breach or leakage affects, or is likely to affect, those Cloud Customers' Cloud Content, Customer Data or any Cloud Service they receive from that CSP.

3.3.13 CSPs must inform the Commission, without undue delay, of any security breach or information leakage that those CSPs become aware of, if such breaches or leakages affect, or are likely to affect:

3.3.13.1 any Level 3 Customer Content,

3.3.13.2 the Customer Content or Customer Data of a significant number of Cloud Customers,

3.3.13.3 a significant number of Persons in the Kingdom because of their reliance on one or more Cloud Customers' services that are affected by the security breach or information leakage.

3.3.14 CSPs must inform their Cloud Customers, upon their request, of any insurance coverage that those CSPs have for any civil liability to those Cloud Customers. This information to the Cloud Customers must include at least the essential features of the CSP's insurance coverage, if these are reasonably required for Cloud Customers to assess their exposure to risk and decide on their own insurance coverage accordingly.

3.3.15 Cloud Providers must adopt internal rules and policies on business continuity, disaster recovery and risk management, and provide to their Cloud Customers or the CSPs they co-operate with, upon their request, a summary of these rules and policies.

3.4 Protection of Customer Data

3.4.1 The provisions of this Article 3.4 shall be binding upon CSPs who:

3.4.1.1 conclude a Cloud Contract with a Cloud Customer, as well as

3.4.1.2 those who, although not a party to such a Cloud Contract with the Cloud Customer concerned, alone or jointly with others determine the purposes and means of the processing of the relevant Cloud Customer's Customer Data in a Cloud System.

3.4.2 Save as required to comply with the laws of a foreign jurisdiction in respect of a Cloud Customer subject to the laws of that jurisdiction, CSPs may not:

3.4.2.1 provide or authorize another party to provide to any third party (including, but not limited to, any individuals, legal entities, domestic or foreign government or public authorities) Customer Content or Customer Data, or

3.4.2.2 process or use Customer Content or Customer Data for purposes other than those allowed under the Cloud Computing Agreement with the Cloud Customer concerned.

3.4.3 A CSP's obligations under Article 3.4.2, above, shall not apply with regard to any Customer Content or Customer Data that meets one of the following two conditions:

3.4.3.1 that CSP is required to disclose, transmit, process or use that Customer Content or Customer Data under the laws of the Kingdom; or

3.4.3.2 the Customer Data are Level 1 or Level 2 Data, and the relevant Cloud Customer provides its express prior consent

(whether in an 'opt-in' or an 'opt-out' form), which the Cloud Customer shall remain free to withdraw at any time in the future.

3.4.4 CSPs shall grant Cloud Customers the right and the technical capability to access, verify, correct or delete their Customer Data.

3.4.5 The CSPs' obligations under Article 3.4.4, above, shall be without prejudice to the CSPs' right to the Customer Data mentioned in Article 2.2.15.3, above, if and for as long as this is necessary

3.4.5.1 for the purposes of billing that Cloud Customer or

3.4.5.2 in order to meet the CSP's obligations under any applicable laws.

3.4.6 The provisions of this Article 3.4 shall be without prejudice to any applicable legal, regulatory or contractual provision conferring a higher degree of protection, and associated rights and obligations, with regard to any categories of personal or business data that form part of Customer Data or Customer Content covered by this Regulatory Framework.

3.5 Unlawful Content and Infringing Content

3.5.1 The provisions of this Article 3.5 shall be binding upon CSPs who:

3.5.1.1 conclude a Cloud Contract with a Cloud Customer, as well as

3.5.1.2 those who, although not a party to such a Cloud Contract with the Cloud Customer concerned, alone or jointly with others exercise control over the processing of the relevant Customer Content.

3.5.2 Subject to the provisions of this Article 3.5, a CSP shall not incur any administrative or criminal liability under this Regulatory Framework or any law, regulation, resolution, or instruction, including the Anti-Cyber Crime Law, based only on the fact that Unlawful Content or Infringing Content has been uploaded, processed or stored on the CSP's Cloud System.

3.5.3 Nothing in this Regulatory Framework shall be interpreted as a legal obligation for CSPs to monitor their Cloud System for Unlawful Content or Infringing Content.

3.5.4 If the Commission or any other authorized entity in the Kingdom orders in writing the CSP to remove any Unlawful Content or Infringing Content from a Datacenter or other element of a Cloud System located in the Kingdom that is used or relied on by the CSP for the provision of Cloud Services under the scope or Articles 3.1.1 or 3.1.2, above, the CSP shall be responsible for ensuring that such Unlawful Content or Infringing Content is:

3.5.4.1 removed from the Datacenter or other element of the Cloud System located in the Kingdom or

3.5.4.2 is rendered inaccessible in the Kingdom and/or (if this is required under the Kingdom's international obligations) any other jurisdiction.

3.5.5 CSPs may, at their own initiative or following a third party request, remove from their Cloud System or render inaccessible in the Kingdom and/or in any other jurisdiction any Unlawful Content or Infringing Content, provided that:

3.5.5.1 this is in accordance with the provisions of the Cloud Contract and

3.5.5.2 the CSP provides adequate notice to the affected Cloud Customer.

3.5.6 CSPs must notify the Commission and/or any other authorized entity, without undue delay, if they become aware of the presence of any Customer Content or other information on their Cloud System that may constitute a violation of Anti-Cyber Crime Law.

3.5.7 CSPs must refer any third parties complaining against Unlawful Content or Infringing Content on their Cloud System to the competent authorities in the Kingdom, unless they decide to address that complaint directly under the provisions of 3.5.5, above.

3.5.8 CSPs may inform a Cloud Customer that Unlawful Content or Infringing Content found in his Customer Content has been taken down unless the Commission and/or any other authorized entity prevents the CSP from doing so. The Commission shall not unreasonably refuse allowing a CSP to do so, particularly if a failure of the CSPs to inform the Cloud Customer about the taking down of its Cloud Content threatens to create any liability of the CSP.

3.5.9 The provisions of this Article 3.5 shall be without prejudice to the CSPs' obligation to co-operate with the Kingdom's authorities, pursuant to any applicable law or any commitments undertaken in their registration, in law enforcement matters associated with Unlawful Content or Infringing Content.

3.5.10 CSPs must grant their Cloud Customers all necessary and lawful intellectual property licenses for the use of any software or other legally protected intellectual work in the Cloud Services provided under their Cloud Contract, commensurate to the duration (if applicable) and scope of the Cloud Contract.

3.6 Information on Cloud Contracts and minimum mandatory content

3.6.1 Prior to the conclusion of a Cloud Contract with a Cloud Customer, CSPs must provide clear and transparent information to that Cloud

Customer on the object of the service, the conditions of use, Cloud Service levels, and applicable payment terms.

3.6.2 The above obligation shall be without prejudice to any other additional information that CSPs may need to communicate to Cloud Customers if so required under their registration or other applicable rules.

3.6.3 Without prejudice to any other obligation under this Regulatory Framework, CSPs must ensure that at least the following information is incorporated in their Cloud Contracts:

3.6.3.1 identification of the CSP, business address and full contact details;

3.6.3.2 description, and allowed use of the services to be provided;

3.6.3.3 Cloud Contract duration (if any applies), applicable charges, payment terms and termination;

3.6.3.4 rules on handling of Customer Content, including its processing and processes to enable Customer Content to be retrieved by the Cloud Customer upon the Cloud Contract's termination;

3.6.3.5 information on the availability, terms and conditions of any Service Level Agreement (SLA) that may be offered by the CSP;

3.6.3.6 a procedure for the resolution of Cloud Customer complaints;

3.6.3.7 applicable law for the interpretation of the Cloud Contract and the resolution of any disputes, it being understood that, if this is other than the law of the Kingdom, it may not override any of the provisions of this Regulatory Framework or any other mandatory rules of the Kingdom that may not be overridden through choice of law provisions;

3.6.4 CSPs must provide a Cloud Customer care service for the resolution of any Cloud Customer complaint. Such service shall be without prejudice to, any other legal remedy and dispute resolution procedure available under applicable laws, also including this Regulatory Framework.

3.6.5 Cloud Customers and CSPs shall have a right to refer their disputes, jointly or separately, to any dispute resolution procedure available before the Commission pursuant to Commission Statutes, without prejudice to any other, non-exclusive, alternative dispute resolution procedures or choice of law clauses that may be allowed under applicable law.

3.6.6 Upon termination of the Cloud Contract with a Cloud Customer, and if the Cloud Customer so requests, the CSP must:

3.6.6.1 provide to the Cloud Customer a copy of the Cloud Customer's Cloud Content stored on the CSP's Cloud System at the time of the Cloud Contract's termination, in a commonly used format, or

3.6.6.2 allow and offer the Cloud Customer the means to download such Cloud Content, in a commonly used format.

3.6.7 As an alternative to the options of Articles 3.6.6.1 and 3.6.6.2 above, the CSP may transfer the Cloud Customer's Cloud Content, in a suitable format, directly to another CSP of the Cloud Customer's choice, where this is technically feasible.

3.7 Cloud Customer protection and unfair Cloud Contract terms

3.7.1 CSPs shall be liable to their individual consumer Cloud Customers for any act or omission by the CSP, its agents, subcontractors or employees (acting within the framework of their agency, employment, or subcontracting relationship with the CSP), incurring liability to such Cloud Customers under this Article 3.7 or any other applicable laws of the Kingdom, regardless of whether such acts or omissions take place in the Kingdom or abroad.

3.7.2 CSPs may not contractually exclude their liability to their individual consumer Cloud Customers for the losses or damages listed below, if these may be reasonably attributed, in whole or in part, to intentional or negligent acts or omissions of those CSPs:

3.7.2.1 any loss of, or damage to, Customer Content or Customer Data, if this is linked to the CSP's processing of, or other interaction with, such Customer Content or Customer Data;

3.7.2.2 quality, performance, accessibility, downtime or other similar service parameters that do not conform with the CSP's obligations under its Cloud Contract with the Cloud Customer concerned or with the provisions of any mandatory legal provisions; and

3.7.2.3 information security breaches.

3.7.3 A 'best efforts' clause by a CSP in a Cloud Contract may not exclude its liability to individual consumer Cloud Customers for acts or omissions committed intentionally or through gross negligence.

3.7.4 Cloud Customers shall bear the burden of proof that any loss or damage referred to in Articles 3.7.1 and 3.7.2 above is reasonably attributed, in whole or in part, to intentional or negligent act or omissions of the CSP.

3.7.5 Notwithstanding the above, CSPs may:

3.7.5.1 Exclude or limit their liability for any indirect damage or any loss of revenue or profits, provided that this is caused nonintentionally to a Cloud Customer;

3.7.5.2 limit their liability by a reasonable maximum amount, which may include, among other alternatives, a function of the fees paid or due by the Cloud Customer under his Cloud Contract with the

CSP and/or compensate the Cloud Customer through Service Credits; and

3.7.5.3 in the case of liability for information security breaches or information leakage, limit their liability if the Cloud Customer (i) opts for an 'own coverage' solution, provided that such an option is offered by the CSP, or (ii) declines the redundancy or other solutions lawfully offered by the CSP to reduce information security risks.

3.7.6 Without limiting Article 3.7.5, CSPs may exclude or limit their liability to Cloud Customers that are not individual consumers to whatever extent the CSPs and those Cloud Customers agree in a Cloud Contract.

3.8 Quality and Industry Standards

3.8.1 CSPs registered with the Commission must:

3.8.1.1 Inform their Cloud Customers, upon request, of the actual levels of achievement of any SLA requirements (if applicable) for the last 12 months or the period since the start of the Cloud Contract, whichever is shorter;

3.8.1.2 inform their Cloud Customers, upon request, of any certification systems or standards that these CSPs meet with regard to their Cloud Services to the relevant Cloud Customer;

3.8.1.3 comply with any certification schemes and/or standards (including encryption standards) that may be defined as mandatory by a Commission decision with regard to the type of Cloud Services provided by that CSP;

3.8.1.4 comply with any rules or guidelines adopted by the Commission with regard to business continuity, disaster recovery and risk management.

3.8.2 Encryption by Cloud Customers or Cloud Users of Customer Data or Customer Content shall not affect the CSPs' obligations under this Regulatory Framework.

3.8.3 The Commission may issue, from time to time, decisions on mandatory or voluntary certification schemes and standards for Cloud Computing, which may vary depending on the required level of information security, the type of CSP or Cloud Customer concerned, or by other criteria.

3.8.4 Without prejudice to any more specific requirement that may be required under Article 3.8.3 above, CSPs subject to a registration under Article 3.2 , above, must demonstrate to the Commission's satisfaction, when applying for registration, that their Cloud Services will be of an acceptable quality and sufficiently secure by general industry standards, based on:

3.8.4.1 the applicant's resources dedicated to Cloud Computing,

3.8.4.2 its relevant experience,

3.8.4.3 and the technical standards complied with by that applicant including the standards listed by the Commission as relevant in Guidelines, Guides or Codes of Practice or, exceptionally, any other technical standards that are demonstrably equivalent or superior to those standards, to the Commission's satisfaction.

3.9 Content filtering

3.9.1 Customer Data or Customer Content in a Cloud System to which this Regulatory Framework applies may be excluded from content filtering by a Commission decision if such Customer Data or Customer Content:

3.9.1.1 is not directly accessible by any Cloud Users or Internet users in the Kingdom; or

3.9.1.2 is accessible only to Cloud Users of (i) a Private Cloud or (ii) a specific communications network limited to connections between a CSP and connections under the control of a single Cloud Customer.

3.9.2 The provisions of Article 3.9.1, above shall be without prejudice to any other rule or decision on content filtering that may be adopted by any other authorized entity in the Kingdom.

3.10 Commission powers

3.10.1 Any violation of the provisions of this Regulatory Framework shall be subject to the penalties that the Commission may impose under Commission Statutes, without prejudice to any penalties that may be imposed under any other applicable law in the Kingdom. Such other applicable law includes, in particular: the Anti-Cyber Crime Law (issued under the Council of Ministers Decision No. 79, dated 7/3/1428 H, and approved by Royal Decree No. M/17, dated 8/3/1428H) and the Electronic Transactions Law (issued under the Council of Ministers Decision No. 80 dated 7/3/1428 H and approved by Royal Decree No. M/18 dated of 8/3/1428H), and any provisions that may amend or replace them in the future.

3.10.2 The Commission may issue guidelines, model Cloud Computing contracts or clauses, guides, recommendations or other texts aimed at:

3.10.2.1 clarifying any aspect of the present Regulatory Framework;

3.10.2.2 providing guidance to CSPs, Cloud Customers and the public in general on any aspect of Cloud Computing;

3.10.2.3 complementing this Regulatory Framework through mandatory or voluntary detailed implementation provisions.

3.11 Entry into effect and transitional measures

3.11.1 Subject to the provisions of Article 3.11.2, below, this Regulatory Framework shall enter into force on 30 calendar days from its publication on the Commission's website, in the original Arabic version.

3.11.2 The CSPs' obligation to register with the Commission under Article 3.2, above, shall enter into force one month after this Regulatory Framework's entry into force.

3.11.3 Notwithstanding Article 3.11.2, above, CSPs may apply for a registration with the Commission immediately upon this Regulatory Framework's entry into force.