

Regulations for the Provision of Cloud Computing Services

RS10

Forth Version

October 2023

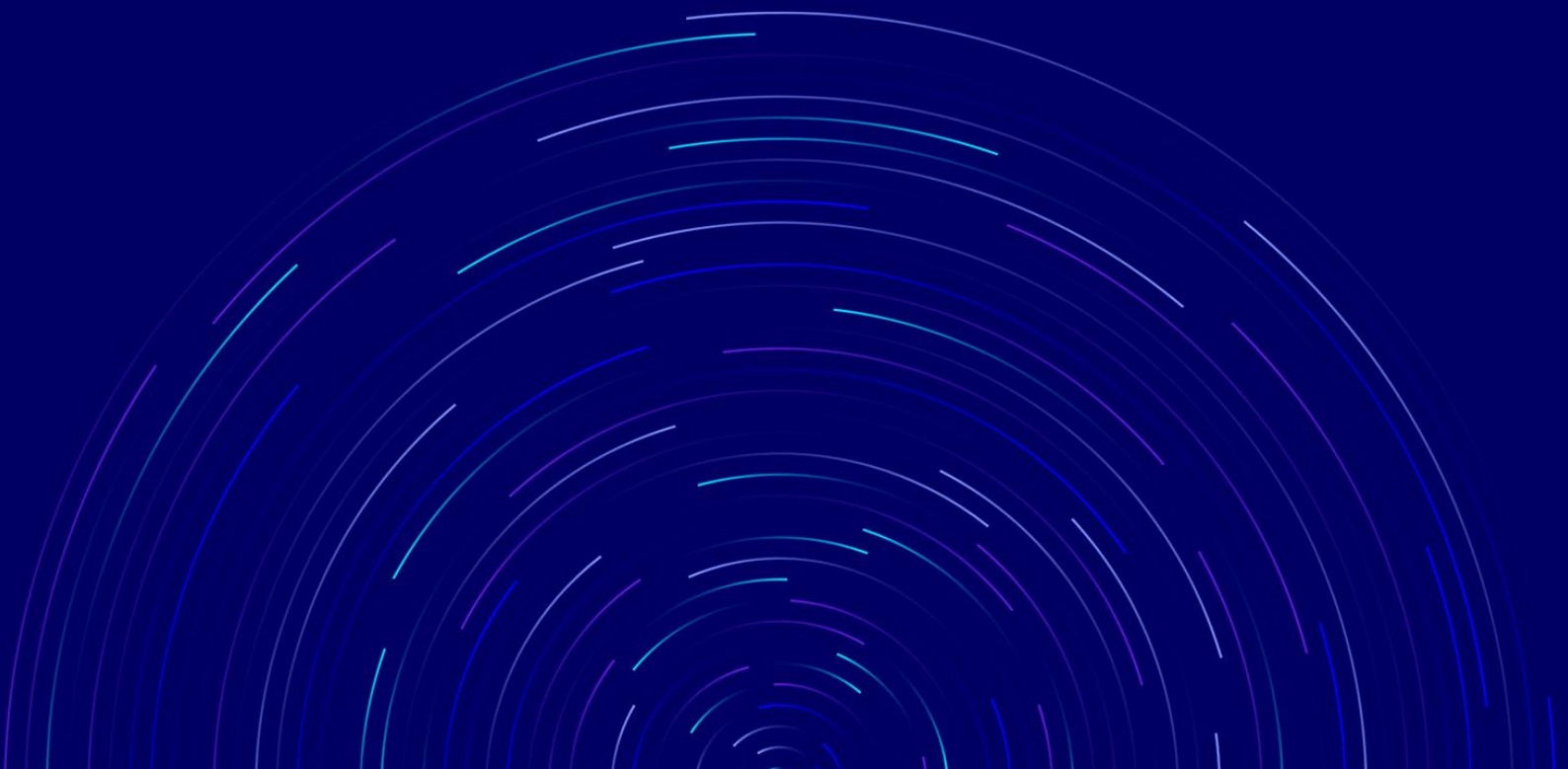
The disclaimer for English language text is not an official translation and is provided for information purposes only. It confers no rights and impose no obligation separate from those conferred or imposed by the original Arabic text formally adopted and published. In the event of any discrepancies between the English translation and the Arabic original, the Arabic original shall prevail.

Version Control Table

Version	Issue Date
Regulatory Framework for Cloud Computing First Version	January 2018
Regulatory Framework for Cloud Computing Second Version Second Version	January 2019
Regulations for the Provision of Cloud Computing Services RS10 Third Version	December 2020
Regulations for the Provision of Cloud Computing Services RS10 Forth Version	October 2023

Table of Contents

1	Introduction	4
2	Definitions:	4
3	Regulations.....	7
3-1	Scope	7
3-2	Registration to provide cloud computing services.....	7
3-3	Subscriber Data	7
3-4	Subscriber Data Protection	10
3-5	Law-Violating Content and IPR-Violating Content	11
3-6	Information about cloud computing service contracts and the mandatory minimum content	12
3-7	Subscriber Protection and Unfair Contract Terms	13
3-8	Quality Standards	14
3-9	Content Filtering.....	15
3-10	CST Powers	15
3-11	General Provisions	16



1 Introduction

Pursuant to the Law of Telecommunication and Information Technology (the ‘Law’) enacted by the Royal Decree No. M/106, dated 02/11/1443H, and its Implementing Regulations, and based on regulatory tasks assigned to Communications, Space and Technology Commission (CST) as per its amended Statute by the Council of Ministers Resolution No. 133, dated 21/5/1424H, which includes powers related to regulating telecommunications and information technology services in the Kingdom, and in accordance with the development of telecommunications markets in the Kingdom and the experiences of other countries, the CST has issued the Regulations for the Provision of Cloud Computing Services to encourage digital transformation, motivate adopting cloud technologies and using it in all sectors, availing an attractive investment environment, and recruiting multinational leading companies in this sector.

2 Definitions:

- 2-1 Words and phrases used in the Law of Telecommunications and Information Technology and its Implementing Regulations shall have the same meanings when used herein, unless stated otherwise. The following words and phrases shall have the meanings assigned thereto:
- 2-1-1 **“Cloud Computing”**: The use of a pool of flexible, scalable, and sharable physical and virtual resources (for example, servers, operating systems, networks, programs, applications, and storage equipment) in addition to providing and managing services automatically upon request.
- 2-1-2 **“Cloud Computing Services” or “Computing Services”**: Providing information and telecommunication technology services through cloud computing, which includes, but is not limited to, storing, transmitting, or processing subscriber content in a cloud computing system. Cloud computing services are divided into three basic services:
- 2-1-2-1 **“Software as a Service (SaaS)”**: The services provided to cloud computing subscribers to use cloud service provider applications that run on cloud platforms and infrastructure. Applications can be accessed from different cloud computing subscribers' devices through a server-based software interface (thin client), similar to a web browser (such as the web-based email). A subscriber does not manage or control the underlying cloud infrastructure that includes the network, servers, operating systems, storage, or even individual application capabilities, except perhaps for some user-specific application configuration settings. Examples may include, but are not limited to, Enterprise Resource Planning (ERP) systems, Customer Relationship Management (CRM) systems, and communications software (e-mail and instant messaging).
- 2-1-2-2 **“Platform as a Service (PaaS)”**: The services provided to cloud computing subscribers in publishing applications developed or purchased by the consumer from a cloud service provider on cloud platforms and infrastructure. These applications are developed using programming languages and tools that are supported by the cloud service provider, and the consumer does not manage or control the platform and the underlying cloud infrastructure, which includes the network, servers, operating systems, or storage. However, the consumer controls published applications and possibly application hosting environment configurations. Examples may include, but are not limited to, application development, databases and a database management system (DBMS), testing tools and developer tools.
- 2-1-2-3 **“Infrastructure as a Service (IaaS)”**: The primary computing resources (processing, storage, networking, etc.) provided to subscribers of cloud

computing. The subscriber is free to choose the software to be published and run, which may include operating systems and applications. The subscriber does not manage or control the underlying cloud infrastructure, but rather the operating systems, storage and published applications, and may have limited control over some network components (such as security systems). Examples may include, but are not limited to, virtual machines, mainframe computers, IT facilities / hosting services.

- 2-1-3 **“Cloud Computing Service Provider (CCSP)”**: Any person who provides cloud computing services to any entity or individual, whether directly or indirectly, such as a service provider, service broker, service aggregator, service reseller provider, or service provider agent; and this is as follows:
 - 2-1-3-1 **“Service Provider”**: Any person who provides cloud computing services to any entity or individual through data centers owned and managed partially or completely by the same person.
 - 2-1-3-2 **“Cloud Computing Service Broker”**: Any person acting as an intermediary between one or more cloud computing service providers and cloud computing subscribers.
 - 2-1-3-3 **“Cloud Computing Service Aggregator”**: Any type of cloud computing brokers who aggregate and combine many of their services into one or more combined packages they provide to cloud computing subscribers.
- 2-1-4 **“Cloud Computing Subscriber”**: Any person to whom the cloud computing service provider agrees to provide his services under a “cloud computing contract” or other commercial relationship between the service provider and such person.
- 2-1-5 **“Cloud Computing User”**: Any natural person (individual) who uses the services of the cloud computing service providers provided to the cloud computing subscriber according to the relationship between such subscriber and the cloud computing user. This individual may be a user and a subscriber at the same time, if a “cloud computing contract” is concluded to provide “computing services” to a single cloud individual “user”.
- 2-1-6 **“Cloud Computing Contract”**: Any agreement entered between a cloud computing service provider and its subscribers to provide such services.
- 2-1-7 **“Cloud Computing System”**: The electronic information system which includes hardware, software and network elements owned, controlled, operated, leased or otherwise from the resources the cloud computing service provider relies on to provide its services to cloud computing subscribers. A cloud computing system may include one or more data centers, among other things.
- 2-1-8 **“Public Cloud Computing”**: Any cloud computing system available for open use by an entity or an individual.
- 2-1-9 **“Community Cloud”**: Cloud computing system provided for the exclusive use of a closed group of “cloud computing subscribers” who share some social, business, administrative or other goals.
- 2-1-10 **“Private Cloud Computing”**: Cloud computing system available for the exclusive use of only one cloud computing subscriber.
- 2-1-11 **“Hybrid Cloud Computing System”**: Any combination of two or more public, private and/or community cloud computing systems, which are linked together, whether by a standard or special technology that enables transmission of data and applications.

- 2-1-12 **“Data Center”**: The facility that contains essential cloud computing infrastructure and its supporting components, which are hosted on the same site, and are used at least partially for storing and/or processing subscriber content and data.
- 2-1-13 **“Content”**: Any programs, texts, files, sound recordings, images, animations, captions, information, personal or commercial data, or any other data in any form.
- 2-1-14 **“Subscriber Content”**: Any content provided or produced by a cloud computing subscriber that is saved or processed in the cloud computing system in accordance with the cloud computing contract for the purpose of providing cloud computing services through such system to the subscriber.
- 2-1-15 **“Subscriber Data”**: Any data falling under at least one of the following categories mentioned below, to the extent that it is or was part of the subscriber content or previously produced by the cloud computing service provider in relation to one or more cloud computing subscribers thereof.
- 2-1-15-1 Any data related to a natural person who is specifically identified directly or indirectly as a cloud-computing user, specifically by referring to an identification number or one or more elements that allows the user to be identified by.
- 2-1-15-2 Any data related to business activities, business information or financial affairs of the cloud computing subscriber, including but not limited to, the subscriber’s rates, employee data, products, customers, financial statements, audit data, security, commercial data, or product development data, even if such data or information is publicly available, without prejudice to the powers of relevant authorities.
- 2-1-15-3 Any data produced by the cloud computing service provider that relates to the service subscriber activity log, billing system, usage volume, statistics, or information of his use of services provided by the cloud computing service provider.
- 2-1-16 **“Subscriber Address”**: The cloud computing subscriber address: either submitted in the cloud computing service contract, or through the billing system, and if the two are different and only one of them is in the Kingdom, the Subscriber Address shall be the address located in the Kingdom.
- 2-1-17 **“Third-Party Content”**: Any content, whether in electronic form, taken, or derived from anyone other than a cloud computing service provider or cloud computing subscriber, and provided to the subscriber through or in conjunction with a cloud computing subscriber's use of its services.
- 2-1-18 **“Law-Violating Content”**: A subscriber or third-party content that violates the Kingdom's laws.
- 2-1-19 **“Intellectual Property Right Infringing (IPR) -Violating Content”**: A subscriber or third-party content that infringes intellectual property rights.
- 2-1-20 **“Residence”**: Permanent or temporary residence in accordance with the Kingdom’s laws. This does not include accommodation of people who are on a short visit to the Kingdom or on transit.
- 2-1-21 **“Service Credits”**: The compensation mechanisms provided by the cloud computing service provider to its subscribers in the event that the service provider’s performance does not meet the standards stipulated in the “cloud computing service contract”, or required under the provisions of these regulations. Service Credits can include, but are not limited to, discounts on current or future bills, and adding time for "cloud computing services" at the end of the billing cycle for free.

- 2-1-22 "Service Level Agreement": A service level agreement between a cloud computing service provider and a cloud computing subscriber that defines the quality of cloud computing services provided to the subscriber in terms of a set of measurable standards related to cloud computing.

3 Regulations

3-1 Scope

- 3-1-1 The provisions of these Regulations shall apply in relation to the cloud computing services provided to subscribers residing in or having a subscriber's address in the Kingdom.
- 3-1-2 Regardless of the subscriber's residence or address, the processing or storing of the content or data of any subscriber temporarily or permanently in data centers, or in other elements of the cloud computing system, located in the Kingdom, shall be subject to the provisions listed below:
- 3-1-2-1 Paragraph. (3-5-4) and Paragraph (3-5-5) of this Article (Removing law-violating content, or IPR-violating content, at the request of CST or any other competent authority) and Paragraph (3-5-6) of this Article below about (Notifying CST of violations of Anti-Cyber Crime Law).
- 3-1-2-2 The exceptions referred to in Paragraph (3-4-3-1) of this Article below.
- 3-1-2-3 Paragraph (2-3) of this Article (Registration to provide cloud computing services) below.
- 3-1-3 Any obligations arising from Paragraph (3-1-1) of this Article above shall be binding on the cloud computing service provider who entered into a cloud-computing contract with the concerned subscriber(s).
- 3-1-4 Unless otherwise specified in these Regulations, these provisions shall be mandatory and not subject to any amendment during the validity of the contract agreement.

3-2 Registration to provide cloud computing services

- 3-2-1 No service provider has the right to exercise direct or effective control over the data center or the essential infrastructure of a cloud computing system hosted and used in the Kingdom, in whole or in part, for the purpose of providing cloud computing services, before performing the correct and complete registration with CST; provided that it uses the communications infrastructure, including international communications, through those authorized by CST.
- 3-2-2 The registration requirements and procedures described in the "Guide for Cloud Computing Service Providers" document and published on the CST's website in its approved Arabic version shall be mandatory for those who meet the registration requirements in accordance with what is stated in Paragraph (3-2-1) of this Article.
- 3-2-3 CST may register service providers in a qualifying category to overcome the challenges of registering them in one of the registration categories referred to in Table No. 2, provided that CST specifies the requirements and procedures for this.

3-3 Subscriber Data

Subscriber Data Classification

Subscriber data may be subject to different levels of classification depending on the guidelines issued by the National Data Management Office or the relevant regulatory authorities overseeing the subscriber. The classification level will be determined by the requirements for preserving the subscriber's data, its confidentiality, integrity, and availability, as indicated in Table 1 and Table 2 below, and shall be subject to the provisions of Paragraph (3-3-4)

Table 1: Subscriber Data Classification

Subscriber Data Classification	Classification Level	Description
Data of Saudi Government Agencies	Top Secret	Data is classified as (Top Secret) if unauthorized access to this data or the disclosure of such data or content leads to serious and exceptional damage that cannot be remedied or repaired on: • National interests, including breaching agreements and treaties, harming the Kingdom's reputation, diplomatic relations and political affiliations, or the operational efficiency of security or military operations, the national economy, national infrastructure, or government business. • The performance of government agencies, which can be harmful to the national interest. • Broader individual health and safety and the privacy of senior officials. • Environmental or natural resources.
	Secret	Data is classified as (Secret) if unauthorized access to this data or the disclosure of such data or content leads to serious and exceptional damage: • National interests, including partially harming the Kingdom's reputation, diplomatic relations and political affiliations, or the operational efficiency of security or military operations, the national economy, national infrastructure, or government business. • Causes a financial loss at the organizational level that leads to bankruptcy, the inability of the entities to perform their duties, a serious loss of competitiveness, or both. • Causes serious harm or injury that affects the life of a group of individuals. • Leads to long-term damage to environmental or natural resources. • Investigating major cases as specified by law, such as terrorism financing cases.
	Restricted	Data is classified as (Restricted) if unauthorized access to or disclosure of this data or its content leads to: • A limited negative impact on the work of government agencies or economic activities in the Kingdom, or on the work of a specific person. • Limited damage to any entity's assets and limited loss on its financial and competitive position. • Limited damage in the short term to environmental or natural resources.
	Public	Data is classified as (Public) when unauthorized access to or disclosure of this data or its content does not result in any of the effects mentioned above - in the event that there is no effect on the following: • National interest • Entity activities • Interests of individuals • Environmental resources
Data of Non-Government Agencies	Data Received from Saudi Government Agencies : Such data shall be classified as received from the government agency based on the levels specified above.	
	Other Data not covered by the above, provided that what is issued by the National Data Management Office or the sector regulators supervising the subscriber shall be taken into consideration.	

Table 2: Categories of Registration of Service Providers

(C) ²	(B)	(a)	Service Provider Registration Category ¹ Data Classification	
			Top Secret	Data of Saudi Government Agencies
			Secret	
			Restricted	
			Public	Data of Non-Government Agencies
✓				
✓	✓			
✓	✓	✓		
Classified as received from the government agencies			Data Received from Saudi Government Agency	Data of Non-Government Agencies
✓	✓	✓	Other Data:	

3-3-1 The provisions of these regulations shall not prejudice any laws, regulations, directives, codes of conduct, internal instructions, implementation policies, organizational or other administrative rules in force in the Kingdom related to the following:

3-3-1-1 The right of cloud computing subscribers - if any - to outsource, transmit, process, or store shared content, or any data, or information in the cloud computing system, taking into account the requirements for outsourcing.

3-3-1-2 The obligation of cloud computing subscribers - if permitted by CST - to ensure that the outsourcing, transmission, processing, or storage is subject to some restrictions, in addition to those specified in these regulations.

3-3-2 The service provider may exclude some or all of the cloud computing subscriber's commercial data from the definition of the subscriber's data mentioned in Paragraph (2-1-15), subject to the cloud subscriber's prior consent.

Subscriber Data Classification Responsibility

3-3-3 Cloud computing subscribers shall choose the appropriate data classification from among the classifications specified in Table 1 mentioned in Paragraph (3-3-1), or any other similar list provided for this purpose by the cloud computing service provider, which meets their specific needs, obligations and duties. Subscribers whose data is classified as (Data of Saudi Government Agencies) must contract with a service provider registered with CST.

3-3-4 The service provider shall notify its cloud computing subscribers, in writing or electronically, of the category in which it is registered with the CST, provided that it includes the level of classification of the subscriber's data shown in Table 1 and Table 2 mentioned in Paragraph (3-3-1).

¹The service provider registration category is the category for which the service provider is qualified to deal with subscriber data according to the subscriber data classification shown in Table 1 and Table 2. The "Guide for Cloud Computing Service" document explains the special requirements for each category.

²To deal with government agencies' data that are classified as Secret and Top Secret, it requires referring to CST to obtain the necessary approvals in accordance with the applicable laws, regulations, policies, and governance models in the Kingdom.

Subscriber Content Site and Transfer

- 3-3-5 The cloud computing service providers registered with CST and cloud computing subscribers must not transfer any content from the data of Saudi government agencies outside the Kingdom for any purpose, or in any form, whether permanently or temporarily (for example, temporary storage and backup, or similar purposes), unless it is explicitly stated that it is permitted according to the laws or regulations in the Kingdom, other than these Regulations.
- 3-3-6 Cloud computing subscribers may not transfer, store, or process shared content from Saudi government agencies' data to any public cloud computing system, community cloud computing system or hybrid cloud computing system belonging to a service provider within the Kingdom, unless the cloud computing service provider is properly registered with CST in accordance with the provisions of Article 2 (2-3) above.
- 3-3-7 Cloud computing service provider registered with CST shall notify their service subscribers in advance and obtain their consent if their content will be transferred, stored or processed outside the Kingdom permanently or temporarily.

Reporting Subscriber's information or documents breaches

- 3-3-8 The cloud computing service provider shall notify CST and its subscribers without undue delay of any breaches of the user information or its documents - that it is aware of- and CST shall notify the National Data Management Office if these breaches affect or are likely to affect government agencies, or a large number of people in the Kingdom due to its reliance on the services of one or more cloud computing subscribers that have been affected by the breach
- 3-3-9 Cloud computing service providers shall notify cloud computing service subscribers of any insurance coverage provided by cloud computing service providers against any civil liability for these subscribers. Information relating to insurance coverage should include at least the basic characteristics as long as this may be reasonably required for cloud computing subscribers to assess their exposure to risk, and to make a decision about their insurance coverage accordingly.

3-4 Subscriber Data Protection

- 3-4-1 The provisions of this Paragraph. (3-4) of this Article shall be binding on cloud computing service providers who:
 - 3-4-1-1 Enter into a cloud computing contract with the cloud computing subscriber, in addition to:
 - 3-4-1-2 Those who specify the goals and means of processing the data of the relevant subscriber alone or jointly with others; although they are not a party to the concerned subscriber's computing contract.
- 3-4-2 Without prejudice to the laws of a foreign jurisdiction regarding cloud computing subscribers subject to those laws, the cloud computing service provider may not:
 - 3-4-2-1 Provide or authorize any other party to providing any content or data related to the cloud-computing subscriber.
 - 3-4-2-2 Process or use content or data pertaining to the cloud-computing subscriber for purposes other than those permitted under the "cloud computing agreement" with the concerned subscriber. The service provider shall disclose (according to detailed document designated thereto) any powers it has to view any data stored in its possession in the Kingdom or that has been processed or transferred in or through it, or to decode such data, or to assist any third party or allow it to view or decipher such data. The service provider shall not implement any new powers in this regard without obtaining CST's explicit and prior written approval.

- 3-4-3 The obligations of the cloud computing service providers mentioned in Paragraph. (3-4-2) of this Article above shall not apply in relation to any subscriber's content or data that meets one of the following two conditions:
- 3-4-3-1 If the service providers are required by the cloud computing subscriber to disclose, transmit, process or use the subscriber's content or data in accordance with the laws of the Kingdom, or
- 3-4-3-2 If the subscriber's data (non-governmental entities) is of another type of data, and the relevant cloud computing subscriber expresses his prior explicit consent (whether in the form of sharing or not sharing), whereby the subscriber has the right to withdraw at any time in the future.
- 3-4-4 Service providers shall grant subscribers the right and the technical ability to access, verify, correct, and delete their data in a manner that does not contradict what is issued by the National Data Management Office regarding personal data.
- 3-4-5 The obligations of service providers mentioned in Paragraph (3-4-4) above shall be complied with, without prejudice to the rights of the cloud computing service providers in relation to the subscriber data mentioned in paragraph (2-1-15-3) as long as this is necessary:
- 3-4-5-1 For subscriber billing purposes; or
- 3-4-5-2 For the purpose of fulfilling the obligations of cloud computing service providers in accordance with any of the laws in force in the Kingdom.
- 3-4-6 The provisions of Paragraph (3-4) above shall apply without prejudice to any statutory, regulatory or contractual provisions applicable in the Kingdom that provide a high degree of protection and related rights and obligations, regarding any categories of personal or commercial data, or that form part of subscriber data covered by these regulations.

3-5 Law-Violating Content and IPR-Violating Content

- 3-5-1 The provisions of Paragraph (3-5) shall apply to cloud computing service providers:
- 3-5-1-1 Those who have entered into a "cloud computing contract" with their subscribers, and
- 3-5-1-2 Those who exercise control over the processing of the relevant "subscriber's content", even though they are not a party to the cloud computing contract with the concerned subscriber, whether alone or jointly with others.
- 3-5-2 In accordance with the provisions of Paragraph (3-5), the cloud computing service provider shall not assume any responsibility based on the fact that the subscriber's content violates the law of the content, or infringes the intellectual property rights of others, which has been downloaded, processed, or stored in a cloud computing system of the cloud computing service provider, without prejudice to the applicable laws.
- 3-5-3 Nothing in these regulations shall be construed as a legal obligation on cloud computing service providers to monitor their cloud computing system, in order to identify the content violating the law, or subscriber's content that infringes any intellectual property rights of others.
- 3-5-4 If the CST or any other competent authority in the Kingdom has directed the cloud computing service providers in writing to remove any content that violates or infringes any intellectual property rights of others from any data center or any other element of the cloud computing system located in the Kingdom that is used or relied upon by service providers in providing cloud computing services in accordance with the

provisions of Paragraphs (3-1-1) and (3-1-2) above, the service providers shall ensure that the content that violates or infringes any intellectual property rights of others:

- 3-5-4-1 Has been removed from any data center or any other element of the cloud computing system in the Kingdom; or
- 3-5-4-2 Make it inaccessible in the Kingdom, (if so required under the Kingdom's international obligations) and/or any other competent authority.
- 3-5-5 Cloud computing service providers may, on their own initiative, or at the request of a third party, remove or make inaccessible in the Kingdom and/or in any other country any subscriber's content that violates or infringes intellectual property rights of others from their cloud computing system, provided that:
 - 3-5-5-1 This is in accordance with the provisions of the cloud computing contract; and
 - 3-5-5-2 That the cloud computing service provider provides sufficient notice to the affected cloud-computing subscriber.
- 3-5-6 With the exemption of what is related to Cybersecurity, cloud computing service providers must notify CST and/or any competent authority, without undue delay, if they discover the existence of any content or any other information in the cloud computing system, which may be violating the laws and legislations of the Kingdom.
- 3-5-7 Cloud computing service providers must refer any third party - except for the competent authorities - who has a complaint regarding a violating content or a content violating intellectual property rights of others in their cloud computing system to the competent authorities in the Kingdom unless they decide to address this complaint directly in accordance with Paragraph (3-5-5) of this Article above.
- 3-5-8 Cloud computing service providers shall have the right to notify the subscriber that a content pertaining to him has been found as violating the law pertaining to content, or that his content infringes any intellectual property rights of others on its cloud computing system and such content has been removed, unless the CST or any other competent authority prevents the cloud computing service provider from doing so. The CST and/or any other competent authority may not prevent the cloud computing service provider from doing so without providing a relevant justification, especially if the failure of the cloud computing service provider to notify the subscriber of the content being removed threatens to entail any liability on the cloud computing service provider.
- 3-5-9 The provisions of Paragraph (3-5) shall apply without prejudice to the obligation of the cloud computing service provider to cooperate with the competent authorities in the Kingdom in accordance with any applicable laws or instructions, or any obligation embedded in the registration procedures with the CST in the matters pertinent to the application of regulations related to the law-violating content or the content that infringes the intellectual property rights of others.
- 3-5-10 The cloud computing service provider shall grant its subscribers all necessary statutory licenses to use any software, or any other intellectual property work protected by the system and provided under the cloud computing contract in proportion to the term (if applicable) and the scope of such contract.
- 3-6 **Information about cloud computing service contracts and the mandatory minimum content**
 - 3-6-1 Before signing the contract with the subscriber, the service provider shall provide clear and transparent information to the subscriber about the topic of the service, terms of use, levels of service, the payment mechanism to be applied, and the category in which

he is registered with CST, provided that it includes the level of classification of the subscriber's data shown in Table 1 and Table 2 mentioned in Paragraph (3-3-1).

3-6-2 The obligation indicated above shall be applied, without prejudice to any other additional information that may be needed by the cloud computing service provider to communicate with subscribers, if this is so required by applicable rules or obligations contained in the registration procedures.

3-6-3 Without prejudice to any other obligations stipulated in these regulations, the cloud computing service provider shall ensure that the following information as a minimum is included in cloud computing service contracts:

3-6-3-1 Information of the cloud computing service provider, business address, and full contact details.

3-6-3-2 A statement of the services to be provided and their permitted uses.

3-6-3-3 Cloud computing contract term (if applicable), applicable fees, terms of payment and termination of the contract.

3-6-3-4 Rules related to handling subscriber content, including its processing, or the processing to enable a cloud computing subscriber to return it to its original source upon termination of the cloud computing contract.

3-6-3-5 Information regarding availability, terms and conditions of any service level agreement ("SLA") that a cloud computing service provider can make available to its subscribers.

3-6-3-6 Procedures for resolving subscribers' complaints.

3-6-3-7 The applicable judicial law for the interpretation of the cloud computing contract or resolving any disputes, provided that it cannot nullify any of the provisions of these regulations, or any other obligatory laws applied in the Kingdom that may not be nullified by choosing other international laws.

3-6-4 Cloud computing service providers shall provide its subscribers with a customer care service to resolve any complaints thereof. This service shall not prejudice any other legal remedies and dispute settlement procedures that are available under the law, including these regulations.

3-6-5 Cloud computing service providers and subscribers have the right to refer their disputes, collectively or individually, to any dispute resolution procedures made available by the CST and in accordance with its regulations, without prejudice to, for example, but not limited to, any other alternative procedures for resolving disputes, or provisions of the law that may be followed pursuant to the applicable law.

3-6-6 Upon terminating the cloud computing contract with a cloud computing subscriber, the service provider shall enable the subscriber to obtain a copy of his cloud computing content for a certain period of time and with the specific means and format in accordance with the cloud computing contract

3-7 Subscriber Protection and Unfair Contract Terms

3-7-1 The cloud computing service provider shall bear responsibility before the CST and its individual subscribers for any acts or negligence on its part, or by its agents, or subcontractors or employees (who are acting within the framework of their agency, employment, or sub-contract with the service provider), according to what is stated in this Article (3-7) or any other laws in force in the Kingdom, regardless of whether or not these acts or neglect may have occurred inside or outside the Kingdom.

3-7-2 The cloud computing service providers shall not have the right to disclaim their liability stipulated in the contract before their subscribers for the loss and damage

mentioned below, if such loss and damage could logically, wholly or partially, be attributed to intentional acts, negligence or omission by the service provider.

- 3-7-2-1 Any loss or damage to the subscriber's content or data, if this is related to the processing of the cloud computing service provider, or any other handling of the content or data of such subscriber.
- 3-7-2-2 Quality, performance, accessibility, duration of downtime, or other similar service standards that do not match the obligations of the service provider under the cloud computing contract with the concerned subscriber, or with any other mandatory statutory provisions.
- 3-7-3 The "best endeavors" clause used in the cloud computing contract shall not exempt the service provider from its liability to individual cloud computing service subscribers for the acts or omission intentionally committed or are due to gross negligence.
- 3-7-4 Cloud computing subscribers shall bear the burden of proving that any loss or damage referenced in Paragraphs (3-7-1) and (3-7-2) of this Article are logically attributable, in whole or in part, to intentional acts, negligence, or omission on the part of the cloud computing service provider.
- 3-7-5 Notwithstanding the above and without prejudice to the applicable laws, cloud computing service providers may:
 - 3-7-5-1 Exclude or limit their liability for any indirect damage or lost revenue or profit, provided that this occurred unintentionally to the cloud computing subscriber;
 - 3-7-5-2 Limit their liability to the maximum reasonable extent, which may include, but not limited to, one or more of the following: offering alternative solutions, refunding the sum of fees paid or owed by a cloud computing service subscriber under their contract with the cloud computing service provider, and/or compensating the cloud computing service subscriber through service credits;

3-8 Quality Standards

- 3-8-1 Service providers registered with CST shall:
 - 3-8-1-1 Provide suitable mechanism for the cloud computing subscribers to view actual completion level for any requirements related to a service level agreement (if applicable) for the last 12 months or the period that has elapsed since the commencement of the cloud computing contract, whichever is the shortest.
 - 3-8-1-2 Provide suitable mechanism for the cloud computing subscribers to view authentication system or standards met by the service providers in relation to the relevant cloud computing services.
 - 3-8-1-3 Adhere to any documentation plans and/or standards that can be defined as mandatory by virtue of a decision from the CST regarding the type of the cloud computing service provided by the service provider.
- 3-8-2 Service providers shall provide cloud computing service subscribers and the service providers who work with them a summary of the implemented policies and procedures of business continuity, disaster recovery, and risk management of service providers.
- 3-8-3 The service providers registered with the CST in accordance with Article 2 (2-3) above shall prove to the CST, at its discretion, when applying for registration that their "cloud services" will be of acceptable quality and sufficiently reliable through general standards based on the following:
 - 3-8-3-1 Applicant resources dedicated to cloud computing.

3-8-3-2 Relevant experience.

3-8-3-3 Conformity with the applicant's technical standards, including the relevant standards set by CST in the guidelines, manuals or practice behaviors, exceptional standards, or any other approved technical standards that exceed those established or are equivalent thereto according to CST's absolute discretion.

3-9 Content Filtering

3-9-1 The cloud computing subscriber's content or data in the cloud computing system to which these regulations apply may be excluded from filtering the content according to a decision by the CST if the subscriber's content or data:

3-9-1-1 Cannot be accessed directly by any of the cloud computing users or Internet users in the Kingdom; or

3-9-1-2 Can be accessed through private cloud computing environments or through dedicated communication networks established between the service provider's connections and the subscriber's controlled connections.

3-9-2 The provisions of Paragraph (3-9-1) must be applied without prejudice to any other regulations or decisions issued by other competent authorities in the Kingdom, with regard to content filtering.

3-10 CST Powers

3-10-1 Any breach of the provisions of these Regulations, or the CST's other regulations shall be subject to the penalties that may be imposed by the CST pursuant to its regulations without prejudice to any penalties that may be imposed under any other applicable laws and regulations in the Kingdom, including the Anti-Cyber Crime Law issued by Council of Ministers Resolution No. 79, dated 07/03/1428H, and approved by Royal Decree No. 17/M, dated 08/03/1428H, and the Electronic Transactions Law issued by Council of Ministers Resolution No. 80, dated 07/03/1428H, and approved by Royal Decree No. 18/M, dated 08/03/1428H, and any other provisions that may amend or replace it in the future.

3-10-2 The service provider registered with CST shall provide CST with any report or information requested within the requirements for the application of this document within the specified period and as stated in the CST's request, and it shall be responsible before the CST for any failure that results from that. In addition, CST will treat these documents and information with complete confidentiality, according to its absolute discretion.

3-10-3 The service provider registered with the CST shall cooperate to the maximum extent with CST's inspectors and facilitate their tasks and make available all possible resources of the service provider to carry out the inspection or audit or follow up on compliance, including: Reviewing the service provider's systems and providing the inspector with all the required documents that confirm the service provider's compliance with these regulations. CST will treat these documents and information with complete confidentiality. The CST has the right to appoint an independent auditing body to carry out inspections, audits, and controls.

3-10-4 The CST has the right to issue guidelines, model cloud computing contracts, paragraphs, or recommendations or other texts with the aim to:

3-10-4-1 Clarify any aspects of the current regulations; and

3-10-4-2 Provide guidance to cloud service providers, cloud computing subscribers, and generally about any aspects of cloud computing.

3-10-4-3 Supplement or amend these Regulations through mandatory or optional detailed executive decisions.

3-10-5 In the event that the service provider does not comply with the obligations contained in this document, The CST has the right to take legal actions against the service provider, including suspending or canceling the registration or any other procedure decided by the CST in accordance with its terms of reference.

3-11 General Provisions

3-11-1 Cloud computing service providers and cloud computing subscribers shall abide by the laws, regulations, controls, decisions, rules, and policies issued by the competent authorities in the Kingdom, including - but not limited to - the National Cybersecurity Authority, the National Data Management Office, and the Saudi Authority for Intellectual Property.

3-11-2 Cloud computing service providers may not apply any laws or regulations or accommodate requests that may conflict with the laws or security requirements in force in the Kingdom without obtaining the CST's explicit written consent.

3-11-3 The service providers registered with the CST shall develop the necessary procedures to ensure the continuity of services; this includes assessing the potential risks and documenting them in a risk register, and developing and implementing business continuity management system.



هيئة الاتصالات والفضاء والتقنية
Communications, Space &
Technology Commission