CITC’s New Cloud Computing Regulatory Framework in Saudi Arabia

by Nick O’Connell - n.oconnell@tamimi.com - Riyadh

March 2018

CITC’s new cloud computing regulation in Saudi Arabia

Following public consultation in 2016, Saudi Arabia’s telecommunications regulator, the Communications & Information Technology Commission (‘CITC’), has now issued a cloud computing regulatory framework (the ‘Cloud Framework’), which came into effect in . A key driver for the introduction of the Cloud Framework is the rapid change being experienced in the information technology sector. The CITC considers that the adoption of the Cloud Framework will provide increased regulatory clarity and encourage the adoption of cloud computing services in the Kingdom. In this article, we outline some of the key provisions of the Cloud Framework, raise some queries, and provide some recommendations.

Scope of application

The Cloud Framework applies to any cloud service provided to cloud customers having a residence or customer address in Saudi Arabia. These obligations apply to any cloud service provider that owns, operates, or offers access to data centres, or other elements of a cloud system, located in the Kingdom. Additionally, regardless of whether the cloud customer has a residence or customer address in Saudi Arabia, certain obligations relating to major information security breaches, takedown of unlawful or infringing content, and notification of violations of Saudi Arabia’s Anti-Cyber Crimes Law 2007, can also arise. In some instances the Cloud Framework appears to apply to cloud service providers outside the Kingdom.

Registration with CITC

Anyone controlling data centres, or other critical cloud system infrastructure, hosted in Saudi Arabia and used for the provision of cloud services, and anyone controlling the processing of customer content of a specific nature (including private sector regulated industries subject to sector-specific rules, and sensitive customer content from public authorities), is required to register with the CITC.

Cloud service providers registered pursuant to the Cloud Framework must disclose to CITC the location and main features of their data centres located in Saudi Arabia, as well as the foreign countries in which they use data centres for processing the data and content of Saudi-based cloud customers. (Cloud service providers are also required to notify cloud customers in advance if they will process data or content outside Saudi Arabia.)
Cloud service providers registered with the CITC are required to comply with standards that the CITC defines as mandatory, and comply with business continuity, disaster recovery, and risk management related rules and guidelines that CITC identifies as mandatory. (These mandatory standards, rules and guidelines do not appear in the Cloud Framework, and will be published by CITC from time to time.) If requested by cloud customers, cloud service providers also need to provide information on actual performance relative to service levels, as well as information on any certification standards followed by the cloud service provider.

Information security

Four information security categories applicable to customer content are specified in the Cloud Framework. These are (in summary):

- Level 1: Non-sensitive customer content of individuals, or private sector companies, not subject to any sector-specific restrictions on the outsourcing of data.
- Level 2: Sensitive customer content of individuals, private sector companies, not subject to any sector-specific restrictions on the outsourcing of data; and non-sensitive customer content from public authorities.
- Level 3: Any customer content from private sector-regulated industries subject to a Level 3 categorisation by virtue of sector-specific rules or a decision by a regulatory authority; and sensitive customer content from public authorities.
- Level 4: Highly sensitive or secret customer content belonging to relevant governmental agencies or institutions.

These levels are a means of categorising content, although they do not provide any clear direction on the corresponding level of information security that cloud service providers must provide to such content. It is unclear whether these levels were intended to conform to something like the requirements of The Uptime Institute's tier classification system (which are pointed at capacity, redundancy, fault tolerance, etc., and not specifically focussed on information security), or whether the CITC plans to elaborate on what security mechanisms and processes it requires of each level, in practice.

The application of these information security levels is subject to any other rules regarding information security requirements determined by other competent authorities in Saudi Arabia, and other rights and obligations of cloud customers relating to the outsourcing, transmission, processing or storage of content or data in a cloud system, specified elsewhere. Between Levels 1, 2 and 3, there is scope for cloud customers to opt for a higher or lower level of information security.

The Cloud Framework sets out certain presumptions as to applicable information security levels for certain types of information. For example, for natural persons resident in Saudi Arabia, there is a presumption that Level 1 shall apply; for private sector entities operating in Saudi Arabia, Level 2 shall apply. Ultimately, the onus is on each cloud customer to specify the level of information security that needs to apply to its content, failing which the cloud service provider may assume that the default levels specified in the Cloud Framework shall apply.

Reporting security breaches

There is a specific obligation on cloud service providers to notify cloud customers of any security breach or information leakage likely to affect the data or content of the cloud customers, or the services the cloud customers receive from the cloud service provider. Additionally, in the case of security breaches or information leakages relating to any Level 3 customer content, or to data or content of a significant number of cloud customers, or to a significant number of people in the Kingdom, there is a specific obligation to notify the CITC.

There is also an obligation on each cloud service provider to provide, on request of a cloud customer, information on the extent of insurance coverage for the cloud service provider's civil liability to the cloud customer. This information is intended to allow cloud customers to properly assess their own insurance needs and coverage.
Internal rules and policies on business continuity, disaster recovery, and risk management must be prepared by each cloud service provider. They must make summaries available to their customers, and to the cloud service providers with whom they work, upon request.

Protection of customer data

Generally, the provisions relating to protection of customer data are without prejudice to any higher

degree of protection required by law or contract.

The provisions relating to protection of customer data apply to cloud service providers who contract with cloud customers, as well as cloud service providers who do not have a direct contractual relationship with such customers but who determine (alone, or jointly with others) the purposes and means of processing cloud customer data.

Cloud service providers are prohibited from providing any third party with customer content or customer data, or processing such content or data for purposes other than those permitted in the relevant cloud services contract. This restriction is subject to exceptions, where cloud service providers are required to comply with the laws of another country in respect of cloud customers established in such other country, or where there is a Saudi law obligation on the cloud service provider to disclose, transmit, process, or use that content or data. Additionally, when customer data is categorised as Level 1 or Level 2, and the customer has expressly consented to non-application of the restriction, the restriction does not apply.
There is also a requirement that cloud service providers allow and enable cloud customers to access, verify, correct, or delete their customer data.
Some of the wording relating to protection of customer data echoes language found in modern personal data protection laws in other jurisdictions. To the extent that customer data is not necessarily ‘personal data’, and cloud customers are not necessarily ‘data subjects’, this does seem curious. It remains to be seen whether this wording will effectively introduce some modern personal data protection type obligations in Saudi Arabia.

Unlawful content and infringing content

The provisions relating to unlawful content and infringing content apply to cloud service providers who contract with cloud customers, as well as cloud service providers who do not have a direct contractual relationship with such customers but who determine (alone, or jointly with others) the purposes and means of processing cloud customer data.

The Cloud Framework makes clear that cloud service providers will not be administratively or criminally liable solely because unlawful content or infringing content has been uploaded, processed, or stored in their cloud systems. It also makes clear that there is no obligation on cloud service providers to monitor their cloud systems for such content.
Cloud service providers are required to remove or block any unlawful content and infringing content if directed to do so by the CITC (or other relevant authority). They are also required to notify the CITC (or other relevant authority) if they become aware of any customer content on their cloud systems that might violate Saudi Arabia’s Anti-Cyber Crime Law 2007.

Mandatory contractual requirements and unfair terms

The Cloud Framework sets out various minimum requirements for cloud contracts. These include: requirements relating to details of the cloud service provider; description of the cloud services; duration, charges, payment terms, termination; rules on processing customer content, and processes enabling it to be returned post-termination; service level type considerations; and a customer complaint mechanism.

Cloud service providers are not permitted to exclude liability for certain types of losses of damages, where such losses or damages are attributable to intentional or negligent acts or omissions of the cloud service provider. These include: loss or damage to customer content or customer data linked to the cloud service provider’s processing of such content or data; service parameters that do not conform to the contractually agreed terms or any requirements mandated by the Cloud Framework; and information security breaches. The practical implications of these apparent restrictions on limitations of liability require greater scrutiny.

What next?

Cloud service providers are required to register within a month of the Cloud Framework coming into force.

The CITC may issue model contracts and clauses, recommendations, and other guidance on the Cloud Framework, and on cloud computing in general.
Cloud service providers should review their own operations, and make sure they register with the CITC if required to do so. Being familiar with the new requirements with regard to removal, blocking, and filtering of content, will enable cloud service providers to put operational mechanisms in place to accommodate these obligations. Cloud service providers should also review their standard contractual documentation to make sure that it is consistent with mandatory requirements set out in the Cloud Framework. They should ensure that their sales teams are familiar with these new mandatory requirements.
Cloud customers should also familiarise themselves with the mandatory contractual requirements, and other rights, set out in the Cloud Framework.

Al Tamimi & Company's Technology, Media & Telecommunications team regularly advises clients on issues relating to cloud computing, data centres, data sovereignty, and other data related matters. For further information, please contact Nick O'Connell, Partner – Technology, Media & Telecommunications: n.oconnell@tamimi.com