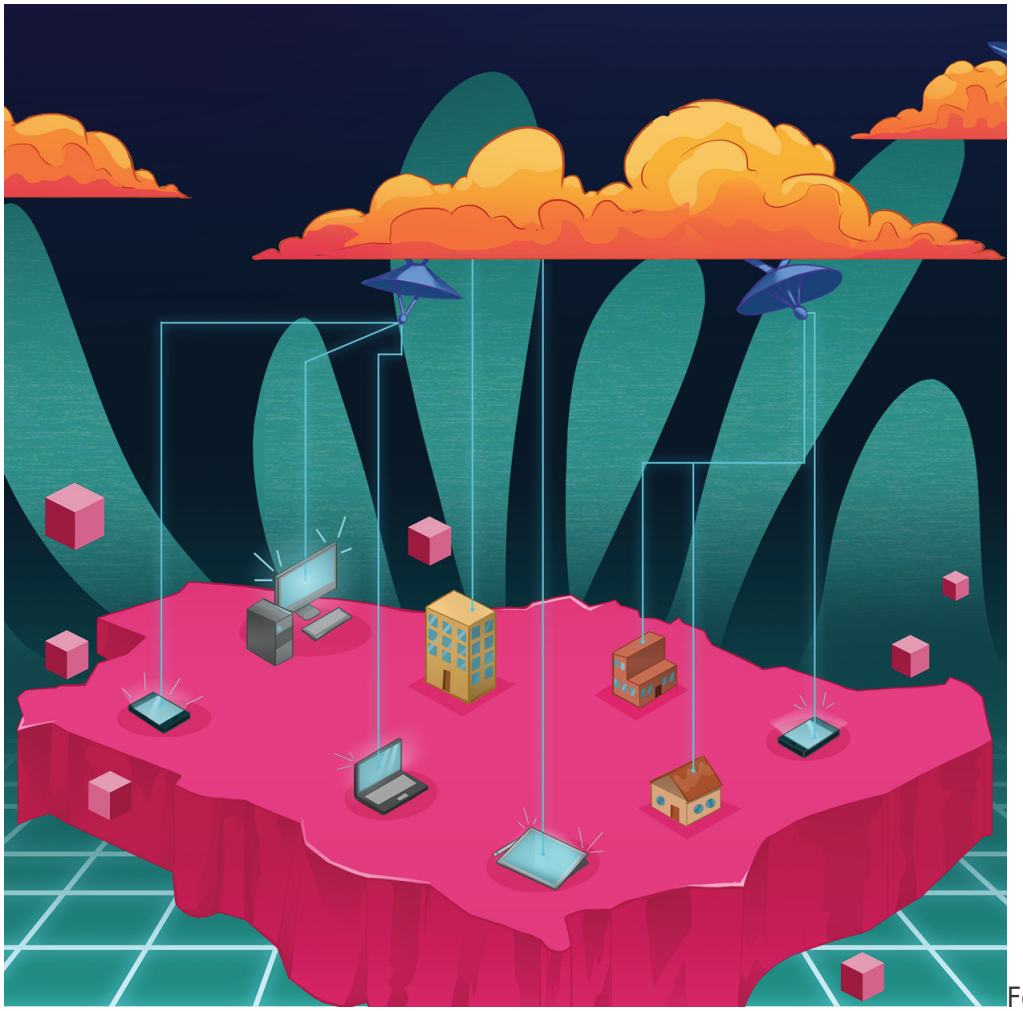
Saudi Arabia’s cloud computing regulatory framework 2.0

Nick O’Connell - Partner, Head of Digital & Data - Saudi Arabia - Digital & Data - Riyadh



Following public consultation in 2016, Saudi Arabia’s telecommunications regulator, the Communications & Information Technology Commission (‘CITC’), issued a cloud computing regulatory framework (the ‘Cloud Framework’), which came into effect in March 2018.

Also in 2018, the National Cybersecurity Authority (‘NCA’), the government agency responsible for cybersecurity, issued the Essential Cybersecurity Controls (‘ECC:2018’).The ECC:2018 contains a very broad restriction on the use of cloud services based outside the Kingdom. This has caused some concern for both cloud service providers and cloud customers.

In February 2019, Saudi Arabia’s Ministry of Communications and Information Technology published a document entitled ‘KSA Cloud First Policy’, showing that adoption of cloud services at the government level is very much on the government’s radar. The version set out on the Ministry’s website is still marked ‘draft’, so its exact status is unclear, but the document sets out a number of considerations relevant to the adoption of cloud computing by government and semi-governmental entities in the Kingdom. The stated goal is to accelerate the adoption of cloud computing services by mandating that government and semi-governmental entities consider cloud options when making new information technology investment decisions. The key drivers in the Cloud First Policy comprise: improving efficiency; enhancing agility and reliability; providing more robust cyber security; and increasing innovation.

Also in February 2019, the CITC issued amendments to the Cloud Framework. The nature of the amendments is largely focussed on ensuring that cloud customers, rather than cloud service providers, are responsible for key aspects of cloud services; in some ways it reads as if industry 'held the pen' on the amendments. Despite the amendments, there are still a number of ambiguities in the cloud framework and its application, and these would benefit from further review.

In this article, we briefly discuss the ECC:2018's restrictions on the use of cloud services located outside Saudi Arabia and outline key provisions of the Cloud Framework and the related February 2019 amendments. On the topic of the Cloud Framework, this article closely follows our earlier article, from March 2018, entitled CITC's New Cloud Computing Regulatory Framework in Saudi Arabia, adjusted to reflect the February 2019 amendments.

NCA's Essential Cyber Security Controls 2018; and the Law on Controls on the Use of Information and Communication Technologies in Government Agencies

The NCA is the government agency responsible for cybersecurity. The NCA's ECC:2018 applies to government agencies (including ministries, authorities, institutions and otherwise), entities and companies affiliated thereto, and private sector entities that own, operate or host critical national infrastructure. The recently issued Law on Controls on the Use of Information and Communication Technologies in Government Agencies 2019 includes a requirement for all government agencies to adhere to the policies, frameworks, standards, controls and guidelines related to cybersecurity issued by the NCA.

With regard to cloud computing, the ECC:2018 requires entities subject to its requirements to ensure that the hosting and storage of their data occurs in Saudi Arabia. This seems to be a very broad restriction on the use of cloud services based outside the Kingdom, and it is likely to have a significant impact on the cloud market in Saudi Arabia. Cloud service providers with infrastructure in the Kingdom are likely to do well; cloud service providers based outside the Kingdom are going to need clarity as to the impact on their business; and cloud customers in the Kingdom that are subject to the ECC:2018 are likely to need their cloud service providers to confirm compliance.

If ECC:2018 is not intended to operate as a blanket prohibition on the use of foreign cloud services by entities subject to the ECC:2018, then we would expect to see clarification issued by the NCA in the near future. (At the time of writing, the NCA has issued a draft Cloud Cybersecurity Control for public consultation. While only a draft, this document does not appear to pull back from the blanket prohibition on the use of foreign cloud services by government sector clients or those involved in critical national infrastructure).

Scope of application of the CCRF

The Cloud Framework, issued by the CITC in 2018 and amended in 2019, applies to any cloud service provided to cloud customers having a residence or customer address in Saudi Arabia. As originally drafted, these obligations were to 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. The February 2019 amendments have removed this wording and introduced wording to the effect that the obligations shall apply to the cloud service provider that has concluded the relevant cloud contract with the cloud customer in question.

Essentially, this change replaces wording that had the potential to lead to the broad application of the

Cloud Framework, including to cloud service providers that owned the relevant infrastructure, or that sold cloud services through local partners, but had no direct relationship with cloud customers. The new wording indicates that the Cloud Framework applies to cloud service providers that have contracted directly with cloud customers, and to cloud services provided to cloud customers in the Kingdom by such cloud service providers.

Regardless of whether a cloud customer has a residence or customer address in Saudi Arabia, where customer content or customer data is processed in a data centre (or other elements of a cloud system) located in the Kingdom, certain obligations can arise. These relate to major information security breaches, take down of unlawful or infringing content, and notification of violations of Saudi Arabia's Anti-Cyber Crimes Law 2007. In other words, regardless of whether a cloud customer is based in Saudi Arabia, if data centres or cloud infrastructure based in the Kingdom are utilised in delivering cloud services, these aspects of the Cloud Framework will apply.

Registration with CITC

The Cloud Framework has been amended to limit the requirement for prior registration with CITC. Now the registration requirement applies only to those controlling data centres, or other critical cloud system infrastructure, hosted in Saudi Arabia and used for the provision of cloud services. Previously, the registration requirement also extended to anyone controlling the processing of customer content that was categorised as 'Level 3', including private sector regulated industries subject to sector specific rules, and sensitive customer content from public authorities. This latter requirement has now been removed.

Cloud service providers registered with the CITC are required to comply with standards and business continuity, disaster recovery, and risk management related rules and guidelines, that CITC identifies as mandatory. 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

The February 2019 amendments to the Cloud Framework do not appear to have affected the information security classification provisions found therein, although further related guidance has been issued by CITC.

The four information security categories applicable to customer content as specified in the Cloud Framework 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; and
- **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 focused on information security), or whether the CITC plans to elaborate on what security mechanisms and processes it requires of each level, in practice.

Guidance issued by the CITC seems to indicate that the various information security classification levels may tie in with certain technical standards to be met by data centres hosting data falling within such classifications, although this is not entirely clear. Publicly available information on the cloud service providers that have registered with CITC, and the respective 'levels' for which they are registered, further confuses the situation. (At the time of writing, information published on the CITC website indicates that cloud service providers registered with CITC only fall within Level 1).

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 generally scope for cloud customers to opt for the application of a higher or lower level of information security. Presumably, where specific information security levels are to apply pursuant to other mandatory requirements (such as sector specific regulations), the cloud customer's ability to opt to apply a lower information security level is excluded.

The Cloud Framework sets out certain presumptions as to applicable information security levels for certain types of cloud content. The February 2019 amendments make clear that cloud customers must assume that these categorisations apply. 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, if the cloud customer wants a higher or lower information security level to apply, it needs to make this clear to the cloud service provider (presumably by implementing the required information security features available to it via the cloud platform). Otherwise, the cloud service provider may assume that the default levels specified in the Cloud Framework shall apply.

Transfer and location of customer content

The February 2019 amendments shift the responsibility for certain requirements relating to Level 3 customer content. Essentially, the obligation is now on cloud customers to ensure that:

- no Level 3 customer content is transferred outside the Kingdom unless this is specifically permitted under the laws or regulations of the Kingdom (other than the Cloud Framework); and
- no public clouds, community clouds or hybrid clouds are utilised for Level 3 customer content unless they are registered with CITC pursuant to the Cloud Framework.

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).

Reporting security breaches

The provisions relating to reporting of security breaches remain unchanged. 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 on the cloud service provider is subject to an exception, namely, where such disclosure or other processing is required to address an obligation on the cloud customer, pursuant to a foreign law to which the cloud customer is subject. This exception is, in turn, subject to any 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.

Basically, the exception that would permit a cloud service provider to provide a third party with customer content or customer data, or process such content or data for purposes other than those permitted in the relevant cloud services contract, would not apply if there is a contrary Saudi law obligation or if the cloud customer had confirmed to the cloud service provider, in advance, that the cloud service provider should not release or process such content or data.

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.

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. The February 2019 amendments include further language emphasising that this exception is to be read broadly.

Similarly, the Cloud Framework also makes clear that there is no obligation on cloud service providers to monitor their cloud systems for such content. (In the Cloud Framework as originally worded, there was no obligation on cloud service providers to 'actively and constantly' monitor their cloud systems. In the February 2019 amendments, this wording ('actively and constantly') has been removed, making it clear that the absence of such an obligation is broad.)

Cloud service providers are required to remove or block any unlawful content and infringing content from their data centre, or other element of a cloud system located in the Kingdom, 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.

In terms of liability, the February 2019 amendments introduced limitations favourable to cloud service providers. Previously, cloud service providers were not permitted to exclude liability for certain types of losses or damages, where such losses or damages were attributable to intentional or negligent acts or omissions of the cloud service provider (such as 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 February 2019 amendments have included wording to make clear that this restriction on the ability of cloud service providers to limit their liability applies only to liability relative to individual consumer cloud customers. A similar amendment is reflected in respect of the restriction on cloud service providers to rely on 'best efforts' clauses; this restriction now only applies relative to individual consumer customers.

What next?

It would be helpful for the NCA to issue more detailed guidance on how it expects the cloud related aspects of ECC:2018 to apply in the market. (See the next edition of Law Update for our analysis of the draft Cloud Cybersecurity Control.) In the meantime, foreign cloud service providers, and cloud customers

subject to the ECC:2018, would be well advised to consider their own circumstances and the potential impact on their businesses and operations.

Cloud service providers subject to the obligation to register with CITC were required to register within a month of the Cloud Framework coming into force. Information available on the CITC website seems to indicate that there has only been limited uptake on this, despite it being a mandatory requirement.

The CITC may issue model contracts and clauses, recommendations, and other guidance on the Cloud Framework, and on cloud computing in general. So far, CITC has issued some guidance on the Cloud Framework, and this was updated at the time the February 2019 amendments were issued. Although the guidance appears to be designed to be user friendly, some of the guidance could be understood as raising more questions than it answers.

Generally, 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 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 mandatory requirements.

Cloud customers should also familiarise themselves with the mandatory contractual requirements, and other rights, set out in the Cloud Framework.

For further information, please contact Nick O'Connell (n.oconnell@tamimi.com).