

Regulation of Cloud Computing in Saudi Arabia

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

September 2016

The internet data centre and cloud computing industry in the Middle East has huge potential. Media reports identify Aliyun, AWS, Cisco, EMC, Equinix, Hewlett Packard, Huawei and Virtustream as just some of the international players interested in the Middle East market. In this context, it comes as no surprise that Saudi Arabia's Communications and Information Technology Commission ("CITC") has recently invited public submissions in response to its proposed regulation of cloud computing.

CITC is the authority charged with the regulation of the information and communications technology sector in Saudi Arabia. CITC seeks to create a favourable environment for cloud computing services, and it is currently reviewing the existing regulatory framework to determine whether cloud-specific regulations are appropriate. In late July 2016, CITC invited feedback from interested parties on its proposed approach to the regulation of cloud computing in Saudi Arabia.

'Cloud Services' can be understood as ICT services involving the processing of user content via a scalable pool of physical or virtual resources (such as servers, operating systems and applications). Cloud services are cost effective, because the provision of infrastructure and other resources can be centralised via specialist cloud service providers, allowing multiple users to benefit without having to duplicate the resources used to deliver the services. Internet data centres can be understood as the physical premises from which cloud services are made available to users via computer networks.

Referring to Saudi Arabia's recently issued Vision 2030 objectives, CITC notes that the development of a strong cloud services industry in Saudi Arabia is a key part of creating a developed digital infrastructure, which is integral to today's advanced industrial activities.

In considering whether the current regulatory framework adequately provides for the development of a modern internet data centre and cloud computing industry, CITC has identified that there is currently no single cloud-specific law or regulation in Saudi Arabia. CITC identified a variety of laws and regulations with potential to impact on cloud computing in the Kingdom, including the Telecommunications Act (which vests regulatory power for the ICT sector in CITC, and which addresses issues such as lawful and unlawful interception), the Telecommunications Bylaw (which addresses licensing requirements for communications service providers and aspects of network security), the Electronic Transactions Law and the Anti-Cyber Crimes Law. Significantly, where government sector clients are likely to be big users of cloud services, CITC has also referenced Council of Ministers decision No. 81 of 1430H (2009), which requires government entities to host their websites on government networks or through providers with local hosting infrastructure and who are licensed by CITC.

Having reviewed the current regulatory landscape, and having undertaken a bench-marking exercise against other jurisdictions, CITC has concluded that it would be beneficial for users of cloud services, and for the development of the cloud industry in Saudi Arabia, to develop a cloud-specific regulatory regime. The objectives of this approach, as expressed in CITC's public consultation document, include:

- Providing clarity and regulatory certainty on the rights and obligations of the providers and users of cloud

computing services.

- Establishing a clear regulatory basis to manage potential security risks connected with the use of cloud services.
- Encouraging improved quality of cloud services.
- Encouraging investment in a local cloud industry.

Importantly, CITC has noted that the nature of cloud computing is such that services and business models are likely to be continually changing. As a result, it is important for a regulatory framework to be flexible – and in some way ‘future proof’. CITC has proposed a general regulatory framework that defines general rules and regulations applicable to cloud computing in Saudi Arabia, and an approach to licensing that sets out the different cases in which cloud service providers need to obtain a licence, whilst contemplating more detailed guidelines, codes of conduct and model clauses that CITC may issue to enhance the regulatory framework.

CITC is proposing a regulatory framework that applies to cloud computing services provided within Saudi Arabia, regardless of the location of the servers or the internet data centres from which the cloud services are provided or the jurisdiction from which the cloud service provider operates. Aspects of the proposed regulations will apply to cloud computing services provided from infrastructure located in Saudi Arabia, even if the user is based outside Saudi Arabia.

As for the licensing regime itself, CITC appreciates that not all cloud service offerings are the same. It is therefore proposing a multi-tiered approach to reflect different types of market players in the cloud space. Variables that it has taken into account when determining the licence options include: the extent of a cloud service provider’s commercial presence in Saudi Arabia, the extent to which the cloud service provider has direct dealings with consumers, the extent of information security requirements that might apply to the subject data, and whether or not the cloud service provider has control over critical infrastructure in Saudi Arabia.

The proposed regulations also touch on information security and data protection obligations, including in respect of requirements to classify data for information security purposes, obligations to permit users’ the right to access, verify and/or delete their user data, and obligations to report instances of security breaches and data breaches.

The proposed regulations include proposals regarding the liabilities and obligations of the parties if unlawful content (including content that infringes intellectual property rights) is processed via a licensed cloud service. Specifically, CITC’s view is that cloud service providers should not be responsible for actively monitoring user content in order to detect and remove or restrict illegal content – but they should be obliged to remove such content or render it inaccessible in Saudi Arabia if directed to do so by the CITC (or some other relevant authority), and otherwise to notify the relevant authorities if they become aware of illegal content.

Consumer protection is also considered, and the proposed regulations address issues such as minimum contractual terms, whether it is appropriate for certain types of liabilities to be limited or excluded, and the extent and nature of any customer support that cloud services providers should be required to provide.

This note is a very high level summary of some of the key issues raised in the public consultation document. The deadline for feedback on the twenty questions that CITC has specified in the public consultation document is 18 September 2016.

The full document is available here, on the CITC website:

<http://www.citc.gov.sa/en/mediacenter/pressreleases/Pages/20160724001.aspx>

Al-Tamimi & Company’s *Technology, Media & Telecommunications* team regularly advises on issues

relating to cloud computing, internet data centres, lawful interception, and data protection related issues. For further information please contact Nick O'Connell (n.oconnell@tamimi.com) or Andrew Fawcett (a.fawcett@tamimi.com).