

## Saudi Arabia: a unique and unconventional framework for cloud computing services

An introduction to the Communications and Information Technology Commission's new regulation on cloud computing.

---

<b>Submitted</b>	13 February 2018
<b>Applicable Law</b>	Saudi Arabia
<b>Topic</b>	<a href="#">Information, Communication &amp; Technology</a> > <a href="#">Data protection &amp; privacy</a> , <a href="#">Data centres</a> <a href="#">Intellectual Property</a>
<b>Sector Focus</b>	<a href="#">Technology Media and Telecommunications</a>
<b>Contact</b>	<a href="#">Raza Rizvi</a> , <a href="#">Neil Westwood</a>

---

Saudi Arabia's Communications and Information Technology Commission (CITC) has published its long-awaited [Cloud Computing Regulatory Framework](#) (the Framework). A draft version of the Framework was the subject of a public consultation which concluded in September 2016.

The final Framework is not consistent with international trends in cloud computing regulation and has several areas of practical and conceptual complexity. The Framework includes a long list of definitions, such as "Cloud Computing" and "Cloud Service Provider", but also deals with some issues in broad terms, making it difficult to determine the scope of the Framework. Cloud solutions will, therefore, need to be carefully considered on a case-by-case basis.

The Framework applies to any cloud service provided to customers (whether natural or legal persons) resident in Saudi Arabia, regardless of the domicile of the cloud service provider. Certain provisions of the Framework also apply to cloud services which rely on data centres or other technology located in Saudi Arabia, regardless of the customer's place of residence.

Cloud service providers contracting directly with end customers, as well as their subcontractors and suppliers, are caught by the Framework. They must register with the CITC before they can operate critical infrastructure in Saudi Arabia which is used to provide cloud services, or before processing certain categories of sensitive customer data.

A key objective of the Framework is to grant cloud customers greater control over how cloud service providers handle their data. Such data processing requirements are typically covered in separate legislation to registration/licensing requirements. The Framework requires cloud service providers to apply specific default levels of information security to customer data, which vary depending on the nature of the customer. The customer then has the ability to direct the cloud service provider to apply a higher or lower level of security. This objective is also achieved by incorporating concepts common to personal data protection laws in other jurisdictions, such as limitations on the purpose of processing customer data, data localisation obligations, and obligations to inform customers and the CITC of data security incidents.

Other novel aspects of the Framework include:

- obligations to provide certain pre-contract information to cloud customers and to include certain minimum content in cloud service contracts
- an express acknowledgement that cloud service providers will not be held liable for unlawful or infringing content stored on their systems, combined with a process enabling the CITC to require providers to take down such content
- various restrictions on cloud service providers' ability to limit contractual liability vis-à-vis their customers, and
- a process whereby customer data stored in the cloud can be exempted from content filtering in Saudi Arabia, where the data are: (i) not accessible by users in Saudi Arabia; or (ii) only available to users of a private cloud or users who are under the control of single organisation.

The Framework will enter into force on 08 March 2018. We anticipate that an immediate impact of the Framework will be the re-papering of agreements, in particular those covering the provision of cloud services to individual, corporate or government customers based in the Saudi Arabia. Cloud service providers will also need to carefully manage the overlap between the Framework and sector-specific regulations, not to mention any sector-neutral personal data protection law which Saudi Arabia may introduce in line with regional trends.

Customers procuring cloud services must ensure that they are fully abreast of the rights and protections afforded to them under the Framework and that their vendors have understood the measures they are now expected to take. For our guidance note on procuring cloud services in the Middle East and Africa, please contact [Raza Rizvi](#) or [Neil Westwood](#).

This document (and any information accessed through links in this document) is provided for information purposes only and does not constitute legal advice. Professional legal advice should be obtained before taking or refraining from any action as a result of the contents of this document.

---

© Simmons & Simmons LLP 2018. All rights reserved. Registered in England & Wales Registered Number OC352713

---

ellexica Limited, CityPoint, One Ropemaker Street, London EC2Y 9SS T: +44 20 7628 2020