Forecast for Data Centres in the Region – Cloudy with a Chance of Regulation

Andrew Fawcett - Partner - Digital & Data
a.fawcett@tamimi.com - Abu Dhabi

Cloud computing is a particular innovation that is growing rapidly worldwide with more and more businesses, government entities, and consumers adopting cloud services.

As you are probably aware, cloud computing is a type of computing that relies on sharing computing resources through remote access and universal data storage, rather than having local servers or personal devices to handle applications.

If GCC countries are serious about positioning their major centres as strategic business hubs, they need more high specification data centres to store the increasing volume of data and to attract leading international cloud providers.

Customer Experience

From a consumer perspective, there are three main reasons why having more local data centres and internet exchange points are important to the overall customer experience for cloud services:

- local exchange of data or hosting reduces latency as data passes via a more direct local route;
- use of more direct route reduces packet loss, consequently increasing data transfer speeds; and
- local Internet Service Providers ('ISP') can reduce their upstream data transit download charges payable to offshore wholesale internet access suppliers.

Regional Snapshot

According to datacentermap.com there are currently 104 co-location data centres across 14 Middle East countries.

By comparison there are:

- 359 across 14 countries in Asia;
- 1088 across 23 countries in Europe; and
- 1,798 in North America.

There are 8 listed in the UAE. Malta and Lithuania also have 8. Cyprus has 12.

Cloud Readiness

Based on a scorecard system developed by BSA – The Software Alliance (www.bsa.org) to measure 'cloud readiness' of a country, there are some aspects in the current legal and regulatory regimes of GCC countries that may need to be addressed for the GCC to be assessed as a more favourable environment for cloud computing.

By way of example only, in the UAE context (which broadly represents a median for the regional regimes) the following are likely to be seen as potential issues:

- There is no express data breach notification law. Data breach notification laws are laws that require an entity that has been subject to a data breach to notify their customers and other parties about the breach, and take other steps to remediate injuries caused by the breach.

- ISPs are subject to mandatory filtering and censoring. For example, The UAE's Telecommunications Regulatory Authority ('TRA') has established the 'Internet Access Management' regulatory policy that regulates access to the content available on the Internet in the UAE. The policy includes a list of categories of prohibited content that contradicts with UAE's Islamic identity, culture, tradition, laws, and regulations. ISPs are obliged to block access to the websites and pages that contain content that fall within these prohibited categories.
- There are no safe-harbour provisions which protect ISPs. *Federal Law No. (7) of 2002 Pertaining to Copyrights and Neighbouring Rights* ("Copyright Law") contains no "safe harbour" provisions designed to immunise intermediaries from liability for copyright damages. The Copyright Law contains no provision dealing expressly with secondary liability at all.

There is also an aspect of the UAE legal system that could potentially be misconstrued as a regulatory hurdle. The UAE uses the inquisitorial system, which is a legal system where the court or a part of the court is actively involved in investigating the facts of the case, as opposed to an adversarial system where the role of the court is primarily that of an impartial referee between the prosecution and the defence. Under the inquisitorial system, which is tied to common Civil Law, the truth is uncovered through questioning those most familiar with the dispute by a judicial authority. It's up to an 'independent' prosecutor or investigating magistrate to distinguish between reliable and unreliable evidence. Accordingly, under *Federal Law No. 35 Concerning the Penal Procedures Law*, the Public Prosecution (not the police) , in proceeding with an investigation, can order a person in possession of something which the Public Prosecution deems should be seized or perused, to submit it (see Article 78). This could include data held by data hosting providers.

Those more used to an adversarial system, where judges focus on the issues of law and procedure and act as a referee in the contest between the defence and the prosecutor, are often uncomfortable with the investigative powers of the public prosecution. However, the inquisitorial system is not unique to the Middle East. If the cloud related aspects of a business are in France, Germany, or Japan the public prosecutions will have similar powers.

Proposed Cloud Regulation in KSA

To address objectives that include encouraging investment in a local cloud industry Saudi Arabia's Communications and Information Technology Commission ('CITC') has recently undertaken public consultation on the proposed regulation of cloud computing.

The CITC is proposing a Cloud Infrastructure and Services License ('CISL') for Cloud Service Providers ('CSPs') with data centres, or other key cloud infrastructure, in the Kingdom and those processing or storing sensitive user content.

The proposed regulations seek to address many of the gaps outlined above. For example:

- The draft regulations provide that a CSP will not incur liability based only on the fact that unlawful content or user content stored or processed by the CSP's cloud system infringes a third party's intellectual property rights. Nor will the CSP have an obligation to actively monitor their cloud system for content that infringes a third party's intellectual property rights. However, a CSP must remove or render inaccessible content on their cloud system that infringes a third party's intellectual property rights if they are ordered to do so by the CITC or any other authorised entity in the Kingdom.
- Further, CSPs must inform cloud users and the CITC, without undue delay, of security breaches or information leakages, depending on the affect or likely affect of such breaches or leakages.

There are some aspects of the proposed regulation that do require careful consideration. It is proposed that no 'Level 3' user content can be transferred outside Saudi Arabia. While the higher Level 4 classifies concerns highly sensitive or secret content belonging to concerned governmental agencies or institutions (and it is understandable that there may be a reason to localise such content), the 'Level 3' classification in the proposed regulations is much broader and includes 'sensitive' user content of private sector

companies or organisations. What is ‘sensitive’ is not defined.

However, overall, the CITC’s proposed cloud-specific regulations should be welcomed as a positive move to benefit users of cloud services and for the development of the cloud industry in Saudi Arabia, and will hopefully act as a prompt for appropriate cloud-specific regulation in other GCC jurisdictions.