Saudi Arabia

Kingdom in the Cloud: Saudi Arabia’s Draft Cloud Computing Regulations

The past few years have seen a downward trend in oil prices, prompting many of the world's largest oil producers to attempt to diversify their economies in order to counter the economic blow. Saudi Arabia, which has been heavily dependent on oil profits, is among those countries seeking to reduce its reliance on oil revenues and increase its foothold in other sectors, including the technology space. This is not only motivated by the desire to diversify the Saudi economy but also as a matter of necessity in order to maintain its role as a global economic player.

Initiatives in the public sphere include an increased provision of e-services and interconnectivity between government agencies, while the government has been making an effort to encourage the growth of cloud computing—along with investment in other information technology initiatives—in both the public and private sectors.

These goals are ambitious, and the country faces at least two formidable hurdles it must overcome if it wishes to become a real player in the technology world. The first is data security, as an increased reliance on cloud computing and e-government brings with it enhanced security concerns, especially in light of the recent high-profile cyberattack targeting Saudi government ministries. The second is streamlining the complex legal regime that currently governs the provision of technology services in the Kingdom, which can prove challenging given the potential for legal and regulatory issues in both the public and private sectors.

By Courtney M. Bowman and Jonathan Reardon

Courtney M. Bowman is a litigation associate at Proskauer Rose LLP in Los Angeles and is a member of the firm’s Privacy & Cybersecurity Practice Group. She specializes in international privacy issues.

Jonathan Reardon is head of the Al Khobar Office, Saudi Arabia, at Al Tamimi & Company where he advises a wide range of international companies on corporate, commercial and regulatory matters in Saudi Arabia including extensively on data privacy issues.
The draft regulations include the requirement that cloud services providers with data centers "as a key cloud infrastructure," in Saudi Arabia, as well as cloud services providers processing or storing "sensitive user content," adhere to a Level 3 Data Processing and Services License (CISL), in order to operate in the country. The draft regulations also require companies processing "sensitive user content," to notify the CITC "with respect to any data breach that affects users or the company," and establish "sensitive user content" categories, which potentially include personal information and governmental and private sector business sensitive information over individuals' sensitive data.

At present, any would-be cloud services provider could easily be put off by the myriad laws that could apply to its business. A Closer Look at Saudi Arabia's Draft Cloud Computing Regulations

Like many other countries around the world, Saudi Arabia has implemented a cloud computing regulatory framework in order to address the challenges presented by cloud computing services. However, the law applying to cloud computing services providers is complex and challenging, as multiple laws and regulations—including the Telecommunications Act, the Information Technology Act, the Electronic Transactions Law, the Telecommunications (Anti-Cyber Crime) Bylaw, and the Electronic Transactions Law—are currently in place. The regulations that apply to these issues in order to make the Kingdom a more attractive destination for cloud computing services providers could be subject to significant changes in the future, as the draft regulations propose a comprehensive set of measures to address the challenges faced by cloud computing services providers.

In the draft regulations, the CITC claims that the licensing requirements for cloud computing services providers will ensure that providers are aware of the regulations that apply to them, and will establish a "level of confidence" for cloud users in the Kingdom. The draft regulations require cloud providers to adopt international standards for data security and data breach notification, and will establish "sensitive user content" categories, which potentially include personal information and governmental and private sector business sensitive information over individuals' sensitive data.

The proposed regulations also include other data protection requirements that could be subject to significant changes in the future, as the draft regulations propose a comprehensive set of measures to address the challenges faced by cloud computing services providers.
covery, and risk management, and require licensed pro-
viders to comply with certification programs or other
decisions that the CITC obtains in accordance. Though not
as comprehensive as the cybersecurity provisions con-
tained in the EU’s new General Data Protection Regula-
tion, the inclusion of this provision appears to be a rea-
sonable first step in the Saudi government’s efforts to regu-
late cloud computing services.

Further, and in keeping with another global trend, the
regulations appear to serve as data localization function-
as well: they provide that Level 3 data may not be trans-
ferred out of the country in any format, for any reason,
and for any length of time, for any reason that likely will
be difficult to comply with in practice, given the in-
creasing prevalence of cross-border data transfers.

Although the comment period on the draft regulations
has ended, a revised set of regulations has not yet been
published. Regardless, the proposed regulations, as cur-
rently drafted, suggest that the Saudi government is
likely to adopt some privacy law concepts similar to
those found throughout the rest of the world in order to regu-
late cloud computing services, albeit with a unique
‘twist’ as far as the classification of sensitive data is con-
cerned. Companies interested in providing cloud com-
puting services in the Saudi market should watch for the
possible finalization and adoption of these proposed
regulations—along with any additional regulatory guid-
ance on the scope of the regulations.