Bloomberg BNA

WORLD DATA PROTECTION REPORT >>>

News and analysis of data protection developments around the world.
For the latest updates, visit www.bna.com

International Information for International Business

VOLUME 17, NUMBER 2 >>> FEBRUARY 2017

Saudi Arabia

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

By Courtney M. Bowman and Jonathan Reardon

The past few years have seen a downward trend in oil prices, prompting some of the world's largest oil producers to attempt to diversify their economies in order to cushion 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. 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—as well as 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 hurdle is streamlining the complex legal regime that currently governs the provision of technology services in the Kingdom. Companies seeking to offer cloud computing or other infor-

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.

mation technology services currently have to interpret a complex set of laws and regulations touching on privacy, cross-border data transfers and sector-specific restrictions, making market entry or growth a relatively complicated proposition.

Various government ministries are attempting to address these issues in order to make the Kingdom a more attractive target for technological investment and growth, and their efforts are exemplified by the recent publication of a set of draft regulations on cloud computing. The draft regulations indicate that certain concepts seen in many other countries' privacy laws—such as specific requirements related to the protection of more "sensitive" data and data breach notification—may soon exist in the Kingdom on a broader scale than they do currently. However, draft regulations suggest that at least some of these concepts may be given a unique Saudi "twist" in their implementation. This article summarizes these recent regulatory developments in the Saudi cloud computing space in order to shed some light for those companies seeking to enter or expand their business in the market.

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 experienced a considerable growth in interest in cloud computing services. However, the law applying to cloud computing service providers is anything but straightforward, as multiple laws and regulations—including the Telecommunications Act, the Telecommunications Bylaw, the Electronic Transactions Law and the Anti-Cyber Crime Law, and various Council of Ministers resolutions and decisions—currently apply to the provision of such services. At present, any would-be cloud services provider could easily be put off by the myriad laws that could apply to its business.

The Saudi government appears to be taking steps to change that. Recognizing that the country needed a more streamlined cloud computing regulation if it is to emerge as a hub in the industry, the Communications and Information Technology Commission (CITC), the Saudi government ministry responsible for regulating communications and information technology within the Kingdom, formulated a draft regulation on cloud computing and published it for a public comment period between July and September of 2016. Significantly, the draft regulations incorporate data protection concepts often seen in other nations' privacy laws, although there are several important differences in the proposed Saudi regulations from those that are implemented elsewhere in the world.

The draft regulations include the requirement that cloud services providers with data centers "or other key cloud infrastructure" in Saudi Arabia, as well as cloud services providers processing or storing "sensitive user content," (referred to as "Level 3" data) obtain a Cloud Infrastructure and Services License (CISL) in order to operate in the country. The draft regulations also envision a second type of license, a Cloud Services License (CSL), for those providers that do not operate cloud infrastructure within Saudi Arabia or "manage data considered to be critical from an information security point of view" (presumably those providers that deal with data classified as either "Level 1" or "Level 2"). Cloud services providers that only have "a limited commercial presence" within the Kingdom as measured by "subscriber numbers and revenues" (possibly meaning fewer than 10,000 Saudi residents as cloud users and less than 1 million SAR in revenue) will not require a license to operate within the country.

It appears that the government puts a premium on governmental and private sector business' sensitive information over individuals' sensitive data.

In the draft regulations, the CITC claims that the licensing program will increase cloud users' confidence in cloud services, will ensure that providers are aware of the regulations that apply to them, and will establish points of contact between service providers and the CITC. At present, however, the scope of the licensing requirement remains unclear, as the draft regulation defines "Level 3" data in terms that are vague at best. For example, Level 3 data is said to include, *inter alia*, "Sensitive User Content of private sector companies or organizations," but what constitutes "Sensitive User Content" is not further defined.

Other classification levels are ambiguous as well: Level 1 data is defined to include "[n]on-sensitive User Content of individuals, not subject to any sector-specific restrictions on the outsourcing of data," while "Level 4" data is "[h]ighly sensitive or secret User Content belonging to concerned governmental agencies or institutions." Moreover, it appears that individuals' sensitive data may receive, as a maximum, a Level 2 classification, thereby appearing to put a premium on governmental and private sector business' sensitive information over individuals' sensitive data. In sum, these categories appear to be quite broad and, at present and without further regulatory guidance, could mean a wide range of providers may have to obtain a license in order to provide cloud services in the Kingdom if the regulations are enacted as currently drafted.

The proposed regulations also include other data protection obligations commonly seen around the world, including requirements to permit users the right to access, verify and delete data, and an obligation to report data security breaches to both users and the CITC "without undue delay" in certain circumstances. Additionally, the regulations require cloud providers to adopt internal policies relating to business continuity, disaster re-

   ISSN 1473-3579

covery, and risk management, and require licensed providers to comply with certification programs or standards that the CITC defines as mandatory. Though not as comprehensive as the cybersecurity provisions contained in the EU's new General Data Protection Regulation, the inclusion of this provision appears to be a nod to the cybersecurity concerns that plague cloud computing generally.

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 transferred out of the country in any format, for any reason, and for any length of time—a provision that likely will be difficult with which to comply in practice, given the increasing 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 currently drafted, suggest that the Saudi government is poised to adopt some privacy law concepts widely utilized throughout the rest of the world in order to regulate cloud computing services, albeit with a unique "twist" as far as the classification of sensitive data is concerned. Companies interested in providing cloud computing services to the Saudi market should watch for the possible finalization and adoption of these proposed regulations—along with any additional regulatory guidance on the scope of the regulations.