CORPORATE COUNSEL
An ALM Website
corpcounsel.com | November 4, 2016

Privacy Law in Saudi Arabia: A Primer for Businesses

From the Experts

Courtney M. Bowman and Jonathan Reardon

Despite the volume of business that U.S. companies conduct in Saudi Arabia, the state of privacy law in the kingdom remains something of a mystery to many outsiders. This uncertainty leaves entities unsure of how to proceed, and has the potential to leave market entrants vulnerable to unanticipated legal exposure. This article attempts to shed light on the Saudi privacy regime by providing a general overview of Saudi privacy law, as well as guidance on practical approaches to compliance.

Riyadh, Saudi Arabia

Sources of Law

Saudi Arabia does not have an omnibus data protection law like many countries in the EU and an increasing number of countries in other regions around the world. As in many countries without such a law, much of Saudi privacy law is derived from two sources: the country's constitution (officially the Basic Law of Governance) and various sector-specific laws, some of which are described in more detail below. However, what distinguishes Saudi privacy law is its additional reliance on Sharia in some instances, which makes it important for companies doing business in the kingdom to have at least a basic understanding of how Sharia operates in practice.

Sharia is derived from both the Quran, the holy book of Islam, and the Sunna, which reflects the practices of the Prophet Muhammad. Although Sharia frequently is referred to as "Islamic law," it is not strictly a legal system; instead, it essentially offers a comprehensive code for living one's life in compliance with Islamic dictates. However, there is no single, agreed-upon interpretation of Sharia; instead, there are multiple schools of thought, and their predominance varies among (and even within) different Islamic countries around the world. These countries have incorporated Sharia into their respective legal systems to different extents. In Saudi Arabia, the more conservative Hanbali school of thought tends to dominate.

Not surprisingly, given that Islam originated in what is now Saudi Arabia and the religion permeates many aspects of life there, Sharia plays a particularly central role in the kingdom's legal system. Generally, in the absence of an applicable legislation, Saudi judges apply Sharia in adjudicating claims. However, judicial decisions generally are not reported, and

judges are not bound by precedent. These factors make judicial outcomes more difficult to predict than in other jurisdictions.

Regardless, companies doing business in Saudi Arabia should be aware that certain Sharia principles create a tort for damages resulting from the wrongful disclosure of a person's private information. That means that even if there is not a specific privacy law applying to the sector in which a particular company operates, there remains the chance that the company could face liability for any disclosures that are deemed wrongful.

In terms of legislation, there is no statutory definition of "personal data," but it is generally thought to include identifying information such as name, address, email address, age, date of birth, gender, occupation and the like. Likewise, there is no statutory definition of "sensitive" personal information, but there are specific requirements relating to certain types of information in the health care, banking, and governmental fields, among others, that are traditionally thought of as being "sensitive." For example, health care practitioners may not disclose patient data without patient consent.

The privacy laws that do exist are focused on specific sectors or particular types of offenses. For example:

• **The Anti-Cybercrime Law** imposes civil and criminal sanctions on certain breaches of personal data, including the illegal access of data or computers to modify, delete, damage, leak or redistribute private data; the interception or reception of data transmitted through an information network without authorization; and the illegal access of bank or credit data, or data related to ownership of securities, with the intention of obtaining data, information, funds or services offered.

• **The Telecommunications Act** prohibits internet service providers and telecommunications companies from intercepting telephone calls or data carried on public networks and intentionally disclosing the information or contents of any message intercepted in the course of its transmission.

• **Saudi health care regulations** require health care practitioners (a term that is broadly defined) to protect the confidentiality of patient information unless the patient has consented to the disclosure of that information in writing.

There also are sector-specific laws regulating the transfer of certain types of data abroad. For example:

• Those wishing to transfer **banking information** overseas need the permission of the Saudi Arabia Monetary Agency in order to complete the transfer.

• The approval of the **Saudi Food and Drugs Authority** is required to transfer certain health-related information outside Saudi Arabia.

More generally, Article 40 of the Basic Law of Governance guarantees the privacy of postal, telephonic and other communications.

Practical Considerations and Best Practices

In general, companies operating in the Saudi market should consider obtaining a data subject's explicit consent to any collection, processing or disclosure of that individual's personal data. Explicit consent, as defined by the EU's Article 29 Working Party (WP29) in its Opinion 15/2011 of July 13, 2011, "encompasses all situations where individuals are presented with a proposal to agree or disagree to a particular use or disclosure of their personal information and they respond actively to the question, orally or in writing." According to the WP29, an example of explicit consent would include an individual providing an electronic signature indicating that he or she consents to the processing of his or her personal information.

On the other hand, a medical clinic's informing a patient that his or her medical file will be transferred to a researcher unless the patient objects will not have obtained that patient's consent, even if the patient never objects. Although it may seem onerous in some situations, obtaining explicit consent lowers the risk that a company that collects, processes and/or discloses Saudis' personal data will be found liable for the wrongful disclosure or misuse of that data under the Basic Law of Governance and Sharia principles. It is not clear whether implied consent is sufficient to avoid liability in these instances; explicit consent therefore is considered ideal.

In sum, entities doing business in Saudi Arabia must be mindful of the kingdom's unique judicial atmosphere and manage their risk exposure accordingly. Although this can seem like an intimidating task—judicial decisions are not precedential (or even published), and the lack of a single governmental body charged with privacy enforcement means that there is little regulatory guidance on point—it is not an impossible one. The first step toward establishing compliance with the kingdom's privacy regime, as it is in any market in which a company wishes to conduct business, is to become familiar with and maintain an awareness of the general state of the privacy law in that country.

Courtney M. Bowman *is a litigation associate in the Los Angeles office of Proskauer Rose who specializes in international privacy issues.* ***Jonathan Reardon*** *is the head of the Al Khobar, Saudi Arabia, office of the law firm Al Tamimi & Co.*

Reprinted with permission from the November 4, 2016 edition of CORPORATE COUNSEL © 2016 ALM Media Properties, LLC. This article appears online only. All rights reserved. Further duplication without permission is prohibited. For information, contact 877-257-3382 or reprints@alm.com. # 016-11-16-02