

Middle East & Africa Technology, IP and Sourcing Focus

Data Protection in the Kingdom of Saudi Arabia: A Primer

Noor Al-Fawzan and Omar Elsayed

Although some surveys of privacy law suggest otherwise, privacy requirements do in fact exist in the Kingdom of Saudi Arabia (KSA) and are very relevant to companies operating there or seeking to provide services to customers in KSA.

Background

The paramount body of law in KSA is the *Sharī'ah*. The *Sharī'ah* is comprised of a collection of fundamental principles derived from a number of different sources, which include the Holy *Qu'ran* and the *Sunnah*, which are the witnessed sayings and actions of the Prophet Mohammed.

Prohibited acts under *Sharī'ah* are punishable by specific penalties set out in the Holy *Qu'ran* or the *Sunnah*. However, where the Holy *Qu'ran* and the *Sunnah* are silent in that regard, a judge may use his discretion to determine the appropriate penalty. Such penalties may include imprisonment, monetary compensation and/or deprivation of certain rights. In determining the severity of a penalty, a judge will take into consideration the damage suffered by a victim and whether such damage is actual or consequential. In general, however, only actual proven damages are awarded by Saudi Arabian adjudicatory bodies.

Previous decisions of the Saudi Arabian adjudicatory bodies generally do not establish a binding precedent for the decision of later cases and the principle of *stare decisis* is not accepted in KSA. In addition, enacted legislation and the decisions of the various Saudi Arabian adjudicatory bodies are not generally or consistently indexed and collected in a central place or made publicly available.

Data Protection under *Sharī'ah* Principles

Sharī'ah principles protect each individual's right to privacy and prohibit any invasions thereon. Under *Sharī'ah* principles, disclosure of secrets is prohibited except *inter alia* where the owner of the relevant secret agrees to such disclosure or if the public interest requires so. The Holy *Qu'ran* and the *Sunnah* do not stipulate a penalty for disclosure of secrets; however, as explained above, such disclosure may be punishable by a penalty that a judge, in his discretion, deems appropriate and equitable. Such penalty may include a fine, imprisonment or deprivation of certain rights such as suspension of a practicing license.

Data Protection under Saudi Arabian Law

In general, there is no specific data protection law in KSA. Therefore, in the absence of specific provisions on data protection, Saudi Arabian courts and adjudicatory bodies will interpret data privacy violations under general *Sharī'ah* principles, which are, as explained above, often expressed in general terms and afford courts and adjudicatory bodies considerable discretion. We understand, however, that a new personal data protection law is under review by the *Shura* Council.

Cyber Data Protection

The KSA Anti-Cyber Crime Law punishes any person that illegally:

- Accesses the computer of another for the purpose of deleting, destroying, altering, or redistributing its information by a fine not exceeding 3,000,000 Saudi Riyals (approximately US\$ 800,000) and/or imprisonment for a period not exceeding four years

- Accesses the bank or credit information of another or information pertaining to its owned securities by a fine not exceeding 2,000,000 Saudi Riyals (approximately US\$ 533,333) and/or imprisonment for a period not exceeding three years
- Interrupts data that is transmitted through a computer or an information network by a fine not exceeding 500,000 Saudi Riyals (approximately US\$ 133,333) and/or imprisonment for a period not exceeding one year

Employee Data Protection

KSA laws do not stipulate any procedures which employers must follow for the transfer of employee data outside of KSA. However, given general *Sharī'ah* principles and the proposed personal data protection law, multinational employers in KSA would probably benefit from including provisions in their employment contracts whereby the employees consent to the use or disclosure of their data to third parties to the extent such disclosures are anticipated or possible.

Patient Data Protection

The KSA Healthcare Practice Code requires that a health practitioner safeguards the secrets of patients which he comes across while carrying out his profession except *inter alia* where written approval of the relevant patient is obtained. Violators of such confidentiality requirements can be subject to a fine not exceeding 20,000 Saudi Riyals (approximately US\$ 5,333) and other disciplinary penalties such as the suspension of practicing license. Such penalties may be increased based on the severity of the relevant breach or its reoccurrence.

Telecom Data Protection

The KSA Telecommunications Law restricts the disclosure of information that is intercepted during its transmission. Violators of such restrictions can be subject to a fine not exceeding 5,000,000 Saudi Riyals (approximately US\$ 1,333,333). In addition, the Telecommunications Law restricts providers of telecom and internet services from disclosing information regarding their subscribers to third parties or from allowing individuals to monitor the communications of their subscribers.

Registration and Export of Personal Data

There are no specific requirements in respect of collection, registration or export of personal data under KSA legislation. It is, however, advisable to obtain the consent of the data subject prior to any export of their personal data to avoid breach of the general *Sharī'ah* principles.

An Arabic version of this article will appear on Latham & Watkins Arabic-language blog www.al-mirsal.com.

Disclaimer: *Middle East & Africa Technology, IP and Sourcing Focus* is made available by Latham & Watkins for educational purposes only as well as to give you general information and a general understanding of the law, not to provide specific legal advice. Your receipt of this communication alone creates no attorney client relationship between you and Latham & Watkins. *Middle East & Africa Technology, IP and Sourcing Focus* should not be used as a substitute for competent legal advice from a licensed professional attorney in your jurisdiction.

CONTACT

Justin Cornish
+971.4.704.6461
justin.cornish@lw.com

Alice Marsden
+971.2.813.4831
alice.marsden@lw.com

Brian Meenagh
+971.2.813.4844
brian.meenagh@lw.com

www.lw.com