DATA PROTECTION LAWS OF THE WORLD

Saudi Arabia

DLA PIPER

SAUDI ARABIA

Last modified 26 January 2017

LAW

Shari'a principles (that is, Islamic principles derived from the Holy *Quran* and the *Sunnah*, the latter being the witnesses' sayings of the Prophet Mohammed), which although not codified, are the primary source of law in the KSA. In addition to *Shari'a* principles, the law in the KSA consists of secular regulations passed by government, which is secondary if it conflicts with *Shari'a* principles.

At this time, there is no specific data protection legislation in place in the KSA (although we understand that a new freedom of information and protection of private data law is under review by the Shura Council). *Shari'a* principles generally protect the privacy and personal data of individuals.

That said, there are certain secular regulations passed by government, which although not dedicated as a whole to data privacy/protection, contain specific provisions governing the right to privacy and data protection in certain contexts. Examples of such regulations include:

- the Basic Law of Governance (no: A/90 dated 27th Sha'ban 1412 H (corresponding to 1 March 1992)), which provides that telegraphic, postal, telephone and other means of communications shall be safeguarded. They cannot be confiscated, delayed, read or breached

- the Anti-Cyber Crime Law (8 Rabi 1, 1428 (corresponding to 26 March 2007)) (as amended), which generally prohibits, amongst other things, the interception of data transmitted through an information network, the invasion of privacy through the misuse of camera-equipped mobile phones and the like, illegally accessing bank or credit data of another, unlawful access to computers for the purpose of deleting, destroying, altering or redistributing private data, or the production, preparation, transmission or storage of material impinging on public order, religious values, public morals, and privacy, through an information network or computers;

- the Telecoms Act (approved pursuant to the Royal Decree No. (M/12) dated 12/03/1422H (corresponding to 3 June 2001), which states that the privacy and confidentiality of telephone calls and information transmitted or received through public telecommunications networks shall be maintained, and disclosure, listening or recording the same is generally prohibited

- the Regulations for the Protection of Confidential Commercial Information (issued by Minister of Commerce and Industry Decision No. (3218) dated 25/03/1426H (corresponding to 4 May 2005), and as amended), which governs the protection of data considered to be "commercial secrets" under these regulations.

There may also be specific regulations applicable to certain industries, for example, in banking, the Saudi Arabian Monetary Agency imposes a general duty of confidentiality on banks, and requires banks to provide a safe and confidential environment to ensure confidentiality and privacy of customer data. Similarly, in the healthcare sector, confidentiality requirements will apply in terms of protecting medical data of patients.

In the absence of specific regulations which apply, the courts will apply Shari'a principles, which in essence provide that an individual has a right to be compensated for losses/harm suffered as a result of the disclosure of his/her personal information and/or breach of privacy by another party. A KSA court may also, in its absolute discretion, impose other penalties on a case by case basis (for example, imprisonment and/or fines).

DEFINITIONS

Definition of personal data

In the absence of specific data protection legislation, there is no definition of "personal data".

Definition of sensitive personal data

In the absence of specific data protection legislation, there is no definition of "sensitive personal data".

NATIONAL DATA PROTECTION AUTHORITY

There is no national data protection authority in the KSA. In respect of telecommunications services, the Communications and Information Technology Commission ('CITC') is responsible for overseeing the relevant telecoms laws and policies. The Saudi Arabian Monetary Agency is responsible for, amongst other things, overseeing commercial banks in the KSA.

REGISTRATION

In the absence of a national data protection authority, there are no data protection registration requirements in the KSA.

DATA PROTECTION OFFICERS

There is no requirement in the KSA for organisations to appoint a data protection officer.

COLLECTION & PROCESSING

There is no concept of "data controller" or "data processor" in the KSA. To ensure compliance with *Shari'a*, it is advisable to obtain data subjects' consent before processing their data.

TRANSFER

There are generally no specific data protection regulations regarding transfer of data outside of the KSA, although in certain sectors, the approval of a regulatory authority may be required. We do generally recommend that consent is sought from data subjects for any processing or transfer of personal data outside of the KSA.

SECURITY

There are no specific security measures that must adopted and implemented by commercial organisations, although as a matter of best practice and to avoid unauthorised processing, disclosure, loss or theft of personal data (and therefore potential liability under *Shari'a*), it is recommended that appropriate measures (technical and organisational) are put in place to protect the personal data held.

BREACH NOTIFICATION

There are no data protection regulations imposing a mandatory requirement to report data security breaches.

ENFORCEMENT

At this time, there is no clear designated authority responsible for the enforcement of data protection and privacy equivalent to, say, the Information Commissioner in the United Kingdom. That said, specific authorities are tasked with enforcing breaches of other legislation that is in place (for examples of such legislation, please see the section above entitled 'LAW'). For example, under

the Anti-Cyber Crime Law (as amended), the Bureau of Investigation and Public Prosecution is tasked with carrying out investigations, with the CITC providing any technical support required, and the matter potentially being referred to the courts.

ELECTRONIC MARKETING

Electronic marketing is regulated by Spam Regulations issued by the CITC, which require, amongst other things, opt-in consent from the date subject to receive electronic messages.

ONLINE PRIVACY

There is no specific legislation in the KSA that expressly regulates the use of cookies. We generally recommend that the use of cookies should be carefully and fully disclosed in a website privacy policy (which should be compliant with KSA law).

KEY CONTACTS

Mohamed Moussallati
Legal Consultant
T +966 11 201 8900
mohamed.moussallati@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organisation's level of data protection maturity.

Disclaimer

DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at www.dlapiper.com.

This publication is intended as a general overview and discussion of the subjects dealt with, and does not create a lawyer-client relationship. It is not intended to be, and should not be used as, a substitute for taking legal advice in any specific situation. DLA Piper will accept no responsibility for any actions taken or not taken on the basis of this publication.

This may qualify as 'Lawyer Advertising' requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.