Unlike the European Union, there is no harmonised legal framework to specifically address privacy and data protection in the states of the Gulf Cooperation Council (GCC). The absence of specific legislation does not mean, however, that privacy is not protected but such protection will emanate from general legal provisions rather than from a particular piece of legislation.

This article provides for a whistle-stop tour of the various relevant legal provisions in each of the six GCC jurisdictions (Bahrain, Kuwait, Oman, Qatar, Saudi Arabia and the United Arab Emirates (UAE)) in terms of data protection.

In Bahrain, there are industry-specific laws and certain provisions in general laws that cover data protection and confidential information.

- According to the Telecommunications Law, the Telecommunications Regulatory Authority (TRA) has an obligation not to divulge any confidential information.
- The TRA Regulation on Bulk Messaging provides limited protection from the advertising activity of bulk messaging (by SMS and/or MMS).
- The E-transactions Law provides protection and regulation regarding online safety such as protection of payment details and prevention of identity theft.
- The Consumer Protection Guidelines set out that licensed operators should take steps to protect consumers’ privacy regarding personal information and calling patterns. Consumers’ privacy should also be protected from unauthorised use of their personal records and information; and, illegal, unsolicited, unwanted or offensive communications.
- According to the Bahrain Penal Code, divulging a secret entrusted by a person concerned with such information without consent to disclose the same from such concerned person will be punished. The sanction will also be applicable to the use of such information by the recipient for his personal benefit or the benefit of another.

In Kuwait, the constitution mentions that: “Freedom of communication by post, telegraph and telephone and the secrecy thereof shall be guaranteed; accordingly, censorship of communications and disclosure of their contents shall not be permitted except in the circumstances and manner specified by law”.

- Based on this, any information that is transmitted by post, telegraph and telephone would be considered confidential and may only be disclosed to the public in accordance with Kuwait law.
- The Evidence Law mentions that “lawyers, doctors, agents or others who acquire information in the course of carrying out their professions may not reveal the same, even after the end of their services or their representative capacity, unless such information was relayed to them with the intention of committing a felony or a misdemeanor”. The “others” category may apply to businesses processing the personal information of their customers, therefore preventing them from revealing this information.
- According to the Central Bank of Kuwait Circular, banks fall into the “others” category. Bank officers and employees may not reveal information about their customers or any information received about customers of other banks in the course of their business. A bank would be responsible for the actions of its officers and employees who violate such duty of confidentiality.

Likewise, in Oman the constitutional law recognises the individual’s right to a private life and guarantees citizens’ confidentiality in all forms of communication.

- The electronic transactions law issued pursuant to Royal Decree No 69/2008 (as amended) (the Electronic Transactions Law) and the cyber crimes law, issued pursuant to Royal Decree No 12/2011 (as amended) (the Cyber Crimes Law) are the two main pieces of legislation in this area.
Other provisions relating to confidentiality and protection of personal data may be found in the Banking Law and circulars issued by the Central Bank of Oman as well as in the capital markets’ authority insurance regulations.

The Electronic Transactions Law deals with the protection of private data and, although it is aimed specifically at e-commerce, it does provide certain safeguards and criminal sanctions against the illegal use of personal information.

The Cyber Crimes Law covers violations of safety, confidentiality of data and systems. Some of the penalties for hacking crimes are increased if they involve the misuse of personal data.

The protection of privacy and personal data in Qatar is addressed in various provisions of some of Qatar’s laws. For example:

- According to the Qatari Constitution, an individual’s privacy must be respected. The Constitution also mentions that unless permitted under Qatari law, an individual shall not have his privacy, family affairs, residence, correspondence, honour or reputation interfered with.

- The Penal Code prohibits an individual to disclose secret or confidential information entrusted to him by virtue of his position or role within an organisation.

- The Telecommunications Act prohibits ISPs and telecom companies from disclosing any information relating to their subscribers and customers and from intercepting telephone calls or data carried on the public telecommunications network. It also prohibits companies from intentionally disclosing the information or contents of any message intercepted in the course of its transmission other than in the course of duty.

- The Anti-Cyber Crime Law imposes civil and criminal sanctions for:
  - the interception of data transmitted through an information network without legitimate authorisation
  - the illegal access of bank data, credit information or information regarding ownership of securities, and
  - unlawfully accessing computers to modify, delete, damage or redistribute personal information.

- Another law which protects personal information in the Kingdom of Saudi Arabia is the Healthcare Practice code requiring a health practitioner to safeguard their patients’ secrets discovered in the course of their profession.

Although no specific DP legislation exist in Saudi Arabia, a right to privacy is established in a number of different laws of the Kingdom, starting with the Saudi Constitution which mentions the right to privacy and sets out the overriding principle that all correspondence and communications between parties should be kept strictly confidential and should not be disclosed.

This principle is supported by provisions contained in the Saudi Telecommunications Act and the Anti-Cyber Crime Law.

- The Telecommunications Act prohibits ISPs and telecom companies from disclosing any information relating to their subscribers and customers and from intercepting telephone calls or data carried on the public telecommunications network. It also prohibits companies from intentionally disclosing the information or contents of any message intercepted in the course of its transmission other than in the course of duty.

- The Anti-Cyber Crime Law imposes civil and criminal sanctions for:
  - the interception of data transmitted through an information network without legitimate authorisation
  - the illegal access of bank data, credit information or information regarding ownership of securities, and
  - unlawfully accessing computers to modify, delete, damage or redistribute personal information.

- Another law which protects personal information in the Kingdom of Saudi Arabia is the Healthcare Practice code requiring a health practitioner to safeguard their patients’ secrets discovered in the course of their profession.

When no relevant legislation applies to protect privacy and personal information, Shariah will apply. Shariah (or Islamic law) is a compilation of principles mostly derived from the Holy Quran. Shariah principles protect the individual’s right to his own privacy and prohibit the disclosure of secrets (unless the owner of the secrets agrees to the disclosure or the public interest requires such disclosure). If Shariah does not provide for any penalty, the penalty will be left at the court’s discretion.

In the UAE, certain provisions in various federal laws can impact data processing activities, for example:

- The UAE Constitution of 1971 provides for freedom of communication “by post, telegraph or other means” and guarantees the right to secrecy of such communications.

- Federal Law No. 5 of 1985 (the Civil Code) provides that a person is liable for acts causing harm generally, which could include harm caused by unauthorised use or publication of the personal or private information of another.

- Federal Law No. 3 of 1987 (the Penal Code) is the primary source of criminal law in the UAE. It sets out offences relating to the publication of matters relating to a person’s private or family life, the unauthorised disclosure of secrets entrusted to a person by reason of their profession, craft, circumstance or art and the interception and/or disclosure of correspondence or a telephone conversation without the consent of the relevant individuals. The punishment for these offences can include fines and/or imprisonment.

- Federal Law No. 5 of 2012 (the Cyber Crimes Law) contains certain offences relating to particular types of personal data in an electronic or online context.

Both the Penal Code and the Cyber Crimes Law set out criminal offences and do not directly confer rights upon individuals in relation to the misuse of their data. However, Federal Law No. 35 of 1992, as amended (the Criminal Procedures Law) permits a person who sustains a direct personal injury from a crime to pursue their civil rights before the criminal courts during the
There are also provisions in certain sector specific laws and regulations that address privacy rights in particular areas, such as the Labour Law, the Credit Information Law and the Medical Liability Law.

Besides the absence of specific legal frameworks addressing the protection of personal data, the economic “freezones” areas of Dubai International Financial Centre (DIFC) and Dubai Healthcare City (DHCC) and the Qatar Financial Centre (QFC) each have their own data protection regime applicable to companies established in those zones.

The legal provisions in the DIFC and the QFC are based, if not entirely on the principles set out by the European Data Protection Directive, on European best practice and require personal data to be processed fairly, lawfully, securely and for a specified legitimate purpose.

Freezone data protection regimes will only be applicable to activities undertaken within the relevant free zones. This means that, if an entity is operating in one of the free zones in Dubai or Qatar, it will need to ensure compliance with the QFC Data Protection Regulations or the DIFC Data Protection Law or the Health Data Protection Regulation, depending on which set of rules applies to that entity.

This article was written by Alexia Zuber.

For more information please contact Alexia on +973 17 13 3213 or alexia.zuber@crsblaw.com