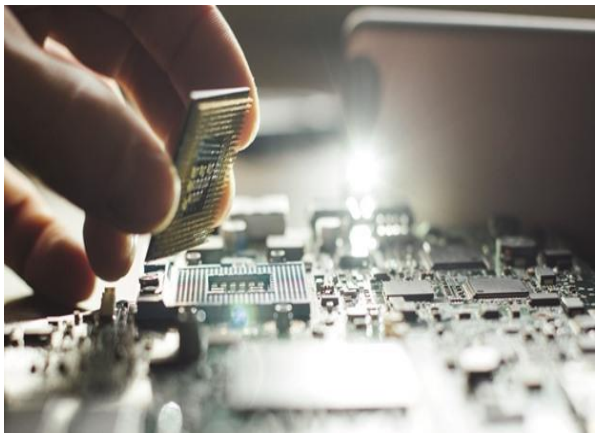
Data Protection Law in Qatar

By Emma Higham, Kellie Blyth/Doha



On November 3, 2016, the legislative framework for data protection in Qatar was overhauled by Law No. 13 of 2016 Concerning Personal Data Protection (the DPL)

The DPL incorporates concepts familiar from other international privacy frameworks and enshrines an individual's right to have their personal data protected.

It mandates that any party who processes such data adhere to the principles of transparency, fairness and respect for human dignity. It will require prompt action to ensure compliance, both for governance reasons and given that the law introduces material fines for breach.

The DPL will help build consumer trust in Qatar in the online environment and may encourage consumers to engage with innovative technologies in confidence that their data will be protected. It comes at a time when the rapid pace of technological change means that more personal data than ever before is being processed electronically, including due to the advance of big data and Internet of Things technologies.

This article is based on unofficial translations into English of the original Arabic text of the DPL. However, In the event of any inconsistency between the English translation and the original Arabic text, the original Arabic text will prevail.

Scope of application of the DPL

The DPL applies to: (i) personal data, being data relating to identifiable individuals; and (ii) any personal data that is processed electronically.

The DPL will apply in most instances where personal data is handled. Article 2 provides that the requirements shall apply where personal data (being data which identifies an individual or which can be used in combination with other data to identify an individual) is electronically processed, or obtained, gathered or extracted in preparation for electronic processing, or where a combination of electronic and traditional processing is used.

The regulator responsible for implementing and enforcing the DPL in Qatar is the Ministry of Transport and Communications (MoTC). The DPL does not specify any geographic limitations on its application. However, the MoTC's ability to bring enforcement action against organisations with no legal presence in Qatar will be limited.

Companies operating in Qatar have been given a six-month grace period (until May 3, 2017) to achieve compliance with the

DPL. We anticipate that this period may be extended to reflect the scale of the changes and cultural shift required. Failure to comply with requirements of the DPL may give rise to a fine of up to a maximum of QR5mn (equivalent to about $1,375,000). Specific penalties apply to breach of the different fundamental articles of the DPL.

Requirements of the DPL

Where the DPL applies, a company will be obliged to comply with certain restrictions and obligations relating to the collection, disclosure and safekeeping of personal data. The principal requirements can be split into the six categories which are set out below.

It is important to note that unlike many other jurisdictions, the DPL does not impose any specific restrictions or requirements that apply to international transfers of personal data (unless such transfer would inflict "gross harm" (discussed below) on the data subject).

Lawful grounds for processing

Personal data should not be processed without the approval of the data subject, unless the processing is necessary to achieve a legitimate purpose. The legitimate purpose referred to may be satisfied by reference to the purpose of the data controller or a third party to whom the personal data is sent. It remains to be seen how narrowly the term "necessary" will be interpreted in practice.

Fair processing notices (FPNs)

To achieve transparency, the data controller (the person who determines, individually or jointly, the purposes for which and the manner in which the personal data is to be processed) is required to issue a notification to the data subject (the person to whom personal data relates), which specifies the identity of the data controller, the purposes for which the data will be processed and a comprehend-sive description of the processing activities.

Compliant information handling practices

The DPL obliges the data controller to: (i) process personal data honestly and in accordance with the law; (ii) put in place appropriate measures to safeguard the data; (iii) comply with the privacy protection policies issued by the MoTC from time to time; (iv) review existing data protection measures before introducing new products / services relating to personal data; (v) ensure that the personal data collected is relevant and accurate; and (iv) not keep the data for longer than required.

Effective management of third parties and employees

A data controller is responsible for identifying all parties who process personal data on its behalf. As defined in the DPL, the term 'data processor' includes both third party organizations as well as the data controller's own employees. Both the data controller and data processors are required to take the necessary steps to protect personal data from loss, damage, alteration, disclosure or from being accessed or used accidentally or unlawfully. As an example, for data controllers this includes providing training to data processors and putting appropriate security measures and systems in place to ensure that the data is protected.

Efficient handling of subject access requests

Data subjects have a right to access and review their personal data at any time (including an option to obtain a copy of their data for a fee) as well as to receive information regarding how their personal data is being processed.

Data breach notification

Any data controller who suffers a data security breach which would cause 'gross harm' to the data subjects concerned must notify both the MoTC as regulator and the affected data subjects. In addition, the DPL requires that any data processor who suffers a breach of its security measures notify the data controller as soon as the data processor becomes aware of the breach.

"Gross harm" is not expressly defined in the DPL. However, the DPL does identify a category of data known as "special personal data" which warrants a greater degree of protection. "Special personal data" includes data relating to race, children, health, physical or psychological conditions, religious beliefs, sexual life or crimes. In our view "gross harm" would include (but may not be limited to) any breach concerning special personal data. The level of fines is undoubtedly designed to drive compliance and to deter irresponsible personal data handling practices. It also highlights how seriously the Qatari government is taking the protection of an individual's right to privacy.

The concepts and requirements of the Data Protection Law will be clarified in further ministerial decisions. However, early indications are that the Data Protection Law is likely to transform the regulatory landscape for privacy in Qatar.