Data Protection and Privacy Law in Qatar

Muhammad Mitha - Senior Counsel - Banking and Finance
m.mitha@tamimi.com - Doha

December 2016 – January 2017

This law aims to establish a certain degree of protection for, and prescribes the guidelines for the processing of, personal data within Qatar.

This article aims to highlight the salient features of the Data Protection Law and analyse its likely effect from the perspective of banks and financial institutions licensed to operate in Qatar.

Salient Features:

The scope of the Data Protection Law extends to personal data which is processed electronically or obtained, collected and extracted for electronic processing or processed through a combination of traditional and electronic processing methods. However, the Data Protection Law does not extend protection to private processing of personal data or data collected for the purposes of attaining official statistics.

The Data Protection Law grants certain rights to individuals which include the right to give or withdraw consent to any processing of their personal data. An individual also has the right to review any of their personal data being stored,and to request any modifications or corrections where the information is inaccurate.

To protect these rights, the Data Protection Law places a heavy burden on the data controllers (i.e. individuals or companies who determine the data processing method and purpose) and processors to ensure that the personal data is handled with care and is duly protected from any leakage or loss or unauthorized disclosure of data. It directs the controllers to have in place adequate measures and procedures to ensure the safe custody of personal data. Some of the directions given to the controllers are as follows:

- Review the data privacy procedures;
- Determine the processors responsible for personal data privacy protection;
- Train and raise awareness amongst processors;
- Develop sound internal systems for receiving and considering complaints and for the effective management of personal data;
- Use proper technology;
- Carry out comprehensive audit to determine the level of compliance; and
- Verify the processor’s compliance with the instructions given.

Added protection is afforded to personal data of a private nature, namely; information relating to race, religious beliefs, children, health, relationships and criminal records which may only be processed after obtaining permission of the relevant department of the Ministry of Transport and Communications. Children are also protected under Data Protection Law from owners and operators of websites for children who are obligated to make adequate disclosures on their websites and obtain permission from the child’s parents before their information can be processed.

A prohibition has been imposed on direct marketing through electronic communication to individuals without obtaining their prior consent.

Notwithstanding the above, there are exemptions given under the Data Protection Law which allow the competent authority or the controllers to process personal data without compliance with certain provisions. These exceptions are as follows:

- Protection of national and public security;
- Protection of international relations of the State;
- Protection of economic or financial interests of the State;
- Prevention, collection of data on or investigation of a crime;
- Execution of a task related to public interest in accordance with the law;
- Execution of an obligation under the law or an order from the court of competent jurisdiction;
- Protection of vital individual interests;
- For purposes of scientific research carried out for the public interest; and
- Collection of the information needed for investigating a criminal offense, upon an official request from the investigation authorities.

The Data Protection Law prescribes high financial penalties for non-compliance or legislative breaches. The penalties will range from QAR 1,000,000 to QAR 5,000,000. However, it is notable that the penalties are financial only and imprisonment is not a prescribed sanction under this law.

Impact on the Qatari Financial Sector:

Banks in the Qatar are regulated by the Qatar Central Bank ("QCB") save for banks who operate within the Qatar Financial Center ("QFC"). QFC banks are excluded from the scope of this article as the QFC promulgated its own Data Protection Rules and Data Protection Regulations back in 2005 which apply to all companies operating in the QFC including banks.

The QCB has issued instructions to the banks to establish mechanisms and procedures which will safeguard the personal information and data of their customers. These banks are required to follow stringent guidelines to ensure that their computer systems/networks are well protected and proper encryption methods and information monitoring are in place.

The enactment of Data Protection Law may cause some practical difficulties for the banks either due to lack of clarity or the subjective nature of the law. To identify a couple of examples – under the Instructions to the Banks issued by the QCB, banks are directed to retain customers' information for at least 15 years. However, the Data Protection Law grants a right to the individual to demand deletion of their personal information once the purpose for which the information was collected has been fulfilled, which may result in non-compliance with the aforementioned retention period. Another example relates to the 'Know Your Client' (KYC) process that the banks are required to undertake. During this process certain personal data of a private nature (as defined in the Data Protection Law) may be gathered by the bank. However, according to the Data Protection Law, such information may only be processed after obtaining permission of the relevant department of the Ministry of Transport and Communications. It is not clear whether the banks would need a blanket approval from the Ministry of Transport and Communications in this regard or would such permission differ from case to case. This may be a cumbersome process for the banks.

Moreover, the banks in Qatar are currently allowed to outsource certain non-core functions to service providers for the purposes of cost reduction, service improvement, or saving time for main services provided that they ensure that adequate controls and guidelines for risk mitigation are in place. However, it seems that the Data Protection Law places an additional obligation on the banks, as opposed to the processors, to ensure that the data obtained meets the lawful purposes and is processed in accordance with the law.

Furthermore, banks may have to revisit their marketing and promotional activities whereby currently their customers are being directly approached through electronic communication to market their products and services. Activities such as email updates or SMS marketing may not be possible under the Data Protection Law. However, the practical risks remain unclear at present as the relevant section in the Data Protection

Law remain open to interpretation due to its broad connotation.

Recommendations for the Banks:

As mentioned above, the Data Protection Law comes into effect only 6 months (which may be extended by a decision by the Cabinet) from the date of its publication in the official gazette. In order for the banks to be compliant with the law on its effective date, banks operating in Qatar should consider taking some precautionary steps some of which we have highlighted below:.

- raise awareness internally and amongst its service providers;
- review internal documents, agreements, policies, disclaimers, consents etc. from the perspective of complying with the Data Protection Law and also identify matters which need to be addressed;
- conduct internal training for the relevant departments such as IT, Legal, Marketing, technical support etc. to address any questions or concerns that the customers may have in relation to the Data Protection Law and their rights thereunder;
- conduct training for service providers responsible for processing the data, revisit internal risk assessments and mitigation plans;
- broadly identify potential issues, consult internally and take steps to rectify those issues or where the risk is still unclear, put in place appropriate holding measures; and
- revisit all security measures implemented by the bank and the service providers and assess whether any further steps can be taken or investments be made to protect customer data.