QATAR

Qatar has implemented Law No. (13) of 2016 Concerning Personal Data Protection ("the Data Protection Law").

With its Data Protection Law—adopted in 2016—Qatar became the first Gulf Cooperation Council (GCC) member state to issue a generally applicable data protection law.

While the Data Protection Law took effect in 2017, executive regulations further implementing this law are expected to be passed in 2021.

The Data Protection Law applies to personal data when this data is any of the following:

- Processed electronically
- Obtained, collected or extracted in any other way in preparation for electronic processing
- Processed by combining electronic processing and traditional processing

The Data Protection Law provides that each individual shall have the right to privacy of their personal data. Such data may only be processed within a framework of transparency, honesty, respect for human dignity and in accordance with the provisions of the Data Protection Law.

DEFINITIONS

Definition of personal data

Personal data is defined under the Data Protection Law as data relating to a natural person whose identity is identified or is reasonably identifiable, whether through this data or by means of combining this data with any other data or details.

Definition of sensitive personal data

Sensitive personal data means personal data consisting of information as to a natural person’s:
DATA PROTECTION LAWS OF THE WORLD

- Ethnic origin
- Health
- Physical or mental health or condition
- Religious beliefs
- Relationships
- Criminal records

NATIONAL DATA PROTECTION AUTHORITY

Qatar Ministry of Transport and Communications (MoTC).

REGISTRATION

There is currently no requirement in Qatar for data controllers who process personal information to register with the regulator, the MoTC.

DATA PROTECTION OFFICERS

There is currently no obligation for organizations in Qatar to appoint a data protection officer. There is an obligation on the data controller to specify processors responsible for protecting personal data, train them appropriately on the protection of personal data and raise their awareness in relation to protecting personal data.

COLLECTION & PROCESSING

Generally, data subject consent is required to collect and process personal data, except to the extent processing is deemed necessary for a lawful purpose of the controller, or the third party to whom the personal data is sent.

Lawful purpose is defined in the Data Protection Law as "the purpose for which the personal data of the data subject is being processed in accordance with the law," which includes specific purposes set forth under Data Protection Law as described below.

Prior to processing personal data, the data controller must notify the data subject of the following information:

- The details of the data controller or another party who processes the data on behalf of the data controller
- The lawful purpose for which the data controller or any third party wants to process the personal data
- A comprehensive and accurate description of the processing activities and the degrees of disclosure of personal data for the lawful purpose
- Any other information deemed necessary and required for the satisfaction of personal data processing

The data controller is free to process data without the consent of the data subject or a lawful purpose in the following circumstances:

- The data processing is in the public interest
- The data processing is required to meet a legal obligation
- The data processing is required to protect the data subjects' vital interests
- The data processing is required for scientific research being conducted in the public interest
- The data processing is required to investigate a crime, if officially requested by the investigating authorities

Sensitive personal data may not be processed except after obtaining authorization from the MoTC. The procedure for obtaining this authorization has not yet been issued (this is likely to be in the form of a Ministerial resolution).

TRANSFER

Data controllers may collect, process and transfer personal data when the data subject consents, unless deemed necessary for realizing a 'lawful purpose' for the controller or for the third party to whom the personal data is sent. The data controller has to demonstrate, when disclosing and transferring personal data to the data processor, that the transfer is for a lawful purpose and
that the transfer of data is made pursuant to the provisions of the Data Protection Law.

Data controllers should not take measures or adopt procedures that may curb trans-border data flow, unless processing such data violates the provisions of the Data Protection Law or will cause gross damage to the data subject. The Data Protection Law defines ‘trans-border data flow’ as accessing, viewing, retrieving, using or storing personal data without the constraints of state borders.

**SECURITY**

Data controllers must take appropriate technical and organizational measures to securely manage personal data.

The data controller must carry out the following procedures:

- Review privacy protection procedures before implementing new processing operations
- Specify the processors responsible for protecting the personal data
- Train processors on the protection of personal data and raise their awareness relating to the same
- Set up internal systems to receive and investigate complaints, data access requests, data correction or deletion requests and provide the data subjects with information relating to the same
- Set up internal systems for the effective management of personal data, and report any violation of the same with the aim of safeguarding personal data
- Adopt suitable technical means to enable individuals to exercise their rights to access, review and correct their personal data directly
- Carry out comprehensive review and checking of the commitment to protect personal data
- Verify that the data processor abides by the instructions given to him/her or take suitable precautions to protect personal data, and continually monitor that situation

The data controller and processor must take necessary precautions to protect personal data against loss, damage, amendment, disclosure or access thereto or use thereof in an accidental or unlawful way. The Data Protection Law states the precautions taken must be proportionate to the nature and importance of the personal data to be protected. Organizations should adopt best practice methodologies in keeping with their business sector.

**BREACH NOTIFICATION**

There is an obligation on the data controller to notify the regulator, the MoTC and the data subject of any breaches of the measures to protect the data subject’s privacy if it is likely to cause damage to the data subject.

**ENFORCEMENT**

In Qatar, the MoTC is responsible for the enforcement of the Data Protection Law. Any data subject may submit a complaint to the MoTC in the case of a violation of the Data Protection Law. The MoTC will investigate the complaint and, if the complaint is found to be valid, the MoTC can oblige the data controller or processor to rectify the violation within a specified time period.

The MoTC can also impose fines of up to 5 million (US$1.4 million) for violations of the Data Protection Law.

**ELECTRONIC MARKETING**

Unsolicited direct marketing is prohibited under the Data Protection Law, which requires prior consent to send electronic marketing communications (including by wired or wireless communication).

All electronic marketing communications must include the identity of the sender and an indication that it is sent for the purpose of direct marketing. The message must include an address that can easily be reached and must enable the recipient to send a message requesting the sender to stop the electronic communication and enable the recipient to withdraw the consent at any time.

**ONLINE PRIVACY**

The Data Protection Law (or any other law) does not specifically regulate online privacy or the use of cookies and location data.
except in relation to children. Owners and operators of websites must observe the following requirements:

- Place a notification on the website regarding how children’s data is used and its disclosure policies
- Obtain express approval from the parents or guardian of the child before processing any personal data
- Provide the child’s parent or guardian—upon request and after verifying the identity of the child’s parent or guardian—a description of the personal data that is being processed, stating the purpose of the processing, and a copy of the child’s data that is being collected and processed
- Delete, erase, or suspend the processing of any personal data that was collected from the child or about the child, if the child’s parent or guardian requests this, and
- Refrain from making any child’s participation in a game or prize offer, or any other activity conditional on the child’s submission of personal data which goes beyond what is required for the purposes of participation in the game or prize offer

**KEY CONTACTS**

**Brenda Hill**
Legal Director
T +974 4420 6126
brenda.hill@dlapiper.com

**DATA PRIVACY TOOL**

You may also be interested in our Data Privacy Scorebox to assess your organization’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.

Copyright © 2021 DLA Piper. All rights reserved.