Qatar’s Data Protection Guidelines: A Novel Approach

Zeina Al Nabih - Senior Associate - Corporate / Mergers and Acquisitions / Commercial - Doha

Frank Lucente - Partner - Corporate / Mergers and Acquisitions / Commercial / Competition / Family Business / Private Equity

f.lucente@tamimi.com - Doha

Nuša Gorenjak

N.Gorenjak@tamimi.com - Qatar

The Compliance and Data Protection (“CDP”) department within the Ministry of Transport and Communications (“MOTC”) regulates data protection matters in Qatar and oversees the operation of Law No. 13 of 2016 (the “Data Protection Law”).

The Data Protection Law imposes certain obligations on the data controllers, such as obtaining a permit to process sensitive personal data or notifying the individuals and the Competent Authority at the MOTC concerning any personal data breach. However, Data Protection Law does not provide further information on how such obligations should be exercised or how they may be defined in greater depth.

It was expected that Executive Regulations to the Data Protection Law would be issued to deal with the foregoing points. Instead, in November 2020, the CDP has taken a novel approach and issued guidelines to the Data Protection Law (“DP Guidelines”). In order to provide guidance to companies on what is required by the Data Protection Law when processing personal data as part of their business operations. In addition, the CDP issued separate guidelines for individuals whose personal data is being processed so as to clarify their rights under the Data Protection Law. The DP Guidelines address matters that were

expected to be addressed by the Executive Regulations to the Data Protection Law.

DP Guidelines

The Data Protection Law applies to any processing of personal data whether processed electronically or through a combination of electronic and non-electronic means. However, it does not apply to personal data processed by individuals for their personal or family matters or to personal data being processed for the purpose of collecting official statistical data as regulated by the relevant laws.

The DP Guidelines attempt to address such matters as:-

(1) data privacy by design and default;

(2) data privacy impact assessment ("DPIA");

(3) direct marketing;

(4) exemptions pursuant to the Data Protection Law;

(5) individuals' complaints;

(6) individuals' rights;

(7) personal data breach notifications;

(8) personal data management systems;

(9) principles of data privacy;

(10) privacy notices;

(11) recording processing activities;

(12) sensitive nature data processing; and

(13) social media.

Along with the DP Guidelines, the CDP has also issued the forms that companies are required to use to submit a DPIA, to make notifications concerning any data breach and for requesting a permit to process sensitive personal data.

Additional requirements pursuant to the DP Guidelines

The DP Guidelines imposed additional obligations that were not specifically addressed by the Data Protection Law. Some of such additional obligations are set out below:

Contract between a data controller and a data processor

The DP Guidelines state that the data controller and the data processor should have a written contract in place. Such obligation is based upon Article 11(8) of the Data Protection Law that provides: "*The Controller shall: Verify Processors' compliance with the instructions given thereto, adoption of appropriate precautions to protect Personal Data, and follow through on the same constantly*."

Furthermore, the DP Guidelines provide further information on what such a written contract should include. In particular it is expected that contracts should address the following matters:

- the subject and duration of processing;
- the nature and purpose of processing;
- types of personal data being processed duties and rights of data controllers;
- duty of confidentiality;
- use of appropriate security measures;
- use of sub-processors;
- individuals' rights;
- assistance that data processors should provide to data controllers;
- rights regarding audits and inspections; and
- what will occur at the end of a contract.

Personal data breach

The DP Guidelines seek to introduce a 72-hour deadline within which data controllers should notify the CDP and individuals of a personal data breach. It should be noted that such a deadline was not mentioned in the Data Protection Law.

Furthermore, the Data Protection Law provides that data controllers are only obliged to notify the CDP and data subjects in cases where a data breach may cause serious damage to data subject. The DP Guidelines have provided a few examples of circumstances whereby processing activities "may cause serious damage". These include:

- processing of sensitive nature personal data;
- using new innovative technology or using existing technology in a new manner;
- carrying out automated decision making;
- collecting personal data through third parties;
- tracking individuals or behavioral monitoring;
- cross-border transfers;
- processing employees' personal data
- direct marketing;
- carrying out a processing activity that is new to the industry.

Data Privacy Impact Assessments (DPIA)

The Data Protection Law provides in Article 11(1) that: "*The Controller shall take the following procedures: . . . reviewing privacy protection measures before proceeding with new processing operations*." Furthermore, Article 13 states: "*Each of the Controller and the Processor shall take precautions necessary*

to protect Personal Data . . . Such precautions shall be commensurate with the nature and importance of the Personal Data intended to be protected."

Based on the above provisions, the DP Guidelines state that data controllers should carry put the DPIA before any new processing activity or before making significant changes to an existing activity. Moreover, the DPIA should be conducted *before* carrying out a processing activity that "*may cause serious damage*" to the individuals.

Sensitive personal data

Article 16 of the Data Protection Law provides that "*Personal Data of a special nature may only be processed after obtaining the permission from the Competent Department, as per the measures and controls determined by a decision issued by the Minister . . .*"

The Data Protection Law did not provide any further details on how such a permit could be obtained. The same was expected to be regulated by the Executive Regulations to the said law. However, the DP Guidelines now address such matters and they provide that if a data controllers intend to process sensitive personal data, the data processor should:

1. identify both a permitted reason for such processing and an additional condition for processing;
2. complete a DPIA; and
3. make a request for a permit from the CDP.

As seen from the above, the DP Guidelines introduced new additional conditions for processing sensitive personal data. According to the DP Guidelines, data controllers should complete a DPIA, request a permit from the CDP and identify both permissible grounds and "additional conditions" for processing. The same must be documented in maintained records or processing activities.

The "additional conditions" mentioned in the preceding paragraph include:

- explicit consent;
- parental consent;
- data having already been made public by data subjects;
- data being related to an employment relationship
- data necessary in the context of social security;
- data being necessary for the vital interests of data subjects;
- data being necessary for legal claims;
- data required in the context of preventive or occupational medicine;
- processing in the context of a charity or non-profit administration;
- processing in the context of public health;
- processing in the context of public interest; or
- processing necessary for protection of national or public security.

In addition, the DP Guidelines define a process on how a permit it to be obtained. As such, data controllers should fill out the "Special Nature Processing Request Form" that must be submitted to the CDP. Along with the said form, data controllers will need to submit the relevant DPIA and any other additional information that the CDP may request. Currently, such documents are submitted by email. However, an online portal that would facilitate such submissions is expected to be launched soon.

Do companies need to be complaint with the DP Guidelines?

It appears the DP Guidelines have been structured as an attempt to mirror the comprehensiveness of the General Data Protection Regulations ("GDPR") in force in the European Union, even though the same are not reflected in the provisions of the Data Protection Law. From a strict legal viewpoint, it is arguable the DP Guidelines have no force in law, should be considered as recommendations only and, as such, may not necessarily require strict adherence. However, it will be interesting in the near future to see how the DP Guidelines will be sought to be enforced by the authorities and what the attitude of a Qatar court will be should a question of non-compliance or enforcement come before such a court.

For further information, please contact Zeina Al Nabih , Nuša Gorenjak or Frank Lucente.