QATAR DATA PROTECTION GUIDELINES – UPDATE

Date: 26 April 2021

Qatar Data Protection Alert

By: Amjad Hussain, Khaled Al-Assaf, Roberto Lusardi

STATUS OF THE GUIDELINES

After a substantial period following the passing of Law No. 13 of 2016 on the Protection of Personal Data Privacy (the Data Protection Law), the Ministry of Transport and Communications (MoTC) in January 2021 issued a set of guidelines on Personal Data Privacy Protection Law (the Guidelines). This is a positive development as it provides greater clarity on the implementation of the Data Protection Law. Pursuant to the Guidelines, the Compliance and Data Protection department (CDP) at the MoTC is indicated as the competent department for implementing the Data Protection Law and for clarifying and developing related controls and procedures.

The Guidelines, although not having the equivalence of binding legislation, provide a set of guidelines, controls, and checklists to support compliance with the Data Protection Law and for implementing decisions relating to data privacy. They should prove useful in clarifying many issues and requirements relating to data privacy that were not detailed under the Data Protection Law, both for entities acting as data controllers or processors and for individuals in terms of their privacy rights.

APPLICATION OF THE GUIDELINES/CDP ROLE

For purposes of this publication we will concentrate on how the Guidelines apply to organizations that act as data controller or processor, referred to within the Guidelines as “regulated entities.” The Guidelines are not intended to apply equally across the board to all organizations. This is evident from statements within the Guidelines themselves, which provide that “Every organisation is different and there is no one-size fits-all answer. The [Data Protection Law] is not prescriptive,” and “These guidelines have been created to help regulated entities navigate their responsibilities under the [Data Protection Law] …. CDP, however, cannot decide exactly which precautions regulated entities need to take, and how they should implement them…”

From the above it is clear the Guidelines are intended to and assist organizations with understanding how the provisions of the Data Protection Law apply to them specifically. It is necessary to differentiate between small businesses, which do not process large amounts of personal data and which may not be able to afford complying with all of the Guidelines, and larger organizations, which process large amounts of personal data including the transfer of such data outside of Qatar. As a general provision, the Guidelines impose different levels of compliance in relation to processing of personal data. There is no obligation for all organizations to comply with every aspect of the Guidelines but rather a recommendation for organizations to carry out an initial assessment and, if not applicable, record the reasons why certain of the Guidelines were not implemented.

MAIN AREAS OF COMPLIANCE

Although the Guidelines are extensive, some of the main areas for organizations (from small to large businesses) to be aware of relate to: i) the conclusion of a contract with data processors; ii) the creation of a Personal Data Management System (PDMS); iii) the undertaking of a Personal Data Impact Assessment (PDIA); iv) restrictions on direct marketing; and v) the creation of a Record of Processing Activities (ROPA). These are highlighted further below to give a basic understanding of what organizations are expected to do to ensure compliance.

Contract

Data controllers should conclude a contract with data processors to verify their processors' compliance with the Data Protection Law and their instructions and that they have appropriate precautions in place. Such contracts would generally cover matters relating to the nature, purpose, and duration of the processing, instructions for processing, appropriate security measures, audits/reviews, and individuals' rights. The extent of the contract will depend on things like the type, amount, and manner of the processing. Such a contract is the best way of recording the rights and obligations of data controllers and processors for purposes of compliance with the Data Protection Law. Compliance must be monitored on a regular basis as part of the applicable PDMS.

PDMS

The creation of a PDMS by data controllers ordinarily comprises a ROPA and PDIA (as applicable) and may include the following: i) accountability for compliance with the Data Protection Law; ii) a record of operational processes identifying the use of personal data and mapping data flows; iii) performance of assessments to identify the impact on the rights of data subjects; iv) implementation of technical and organizational measures to protect the rights of data subjects; v) establishment of processes for breach notification, data subject requests, and consent management; and vi) measuring, evaluating, and monitoring performance and conformance with the Data Protection Law. Controllers must document their decisions (if required by the CDP) in respect of identifying and reviewing their processors. Pursuant to the Guidelines, the manner in which data controllers go about ensuring compliance and implementing appropriate measures will depend on their circumstances, their resources, and what personal data they process and how they process it. The Guidelines include a checklist for organizations to use in respect of PDMS requirements.

DPIA

A DPIA does not seem to be required for all data controllers and, again, this will depend on the resources they have available and the nature of the data they process. Controllers should, however, still record where they believe a DPIA is not required. A DPIA forms part of a PDMS and is an assessment to identify the risk of processing personal data to individuals and mitigate the risk of processing to an acceptable level. The Guidelines state, “Controllers should perform a DPIA prior to processing personal data in a new way or prior to making a significant change to a current processing activity.” Ultimately it is up to individual data controllers to identify the level of risk involved with the processing and whether or not the processing may cause serious harm to individuals. In the event of any uncertainty, the data controllers should opt to conduct a DPIA to ensure compliance and demonstrate best practice.

Direct Marketing

Pursuant to the Guidelines, direct marketing is now more restricted and regulated. Data controllers should not send any direct marketing to individuals unless they have received their explicit consent. This applies to marketing

by electronic means or otherwise. The consent does not necessarily have to be in writing but must be: i) explicit and unambiguous; ii) provided on an 'opt-in' basis (opt-out basis or pre-ticked boxes are no longer allowed); and iii) easy to withdraw. Controllers are required to keep a record of how and when such consent was provided. Marketing communications should further identify the data controller and provide the controller's contact details in order for individuals to easily withdraw consent and stop receiving such communications. Marketing communications should state they have been sent for purposes of direct marketing. Controllers are also discouraged from buying email lists of contact information of individuals to send marketing communications to. Although data controllers may use third parties to send marketing communications on their behalf, the controllers are responsible for ensuring such third parties comply with the Data Protection Law.

ROPA

ROPA forms the backbone of the PDMS and covers compliance with requirements such as: i) tracking consent; ii) publishing of a privacy notice; iii) manage privacy assessments; iv) planning any required training; v) managing data breaches and notifications; vi) verifying data processor compliance; vii) managing cross-border data flows; and viii) managing sensitive personal data processing. ROPA is further required to include a record of all marketing activities. The Guidelines state that “The CDP recommends that all controllers put a RoPA in place to keep track of their processing activities to some extent. It is ultimately for the controller to decide on whether to put a RoPA in place to support compliance with obligations under the [Data Protection Law]. If a controller does not maintain a RoPA and a complaint is made about their obligations a controller could be liable to fines under Article 23 and/or 24 of the [Data Protection Law].” In the event that an organization does not believe that it is required to keep a ROPA, it should at least keep a record of why it is not required.

CONCLUSION

Organizations in Qatar have now been provided with a lot more detail in respect of what is expected of them in terms of compliance with the Data Protection Law, specifically in relation to procedural and implementation requirements. The Guidelines, while still new and untested, appear to allow for some flexibility in respect of requirements based on the amount and type of personal data processing activities. However what is clear for all organizations in Qatar is that consideration needs to be given to such processing activities and appropriate systems put into place or, to the extent that no systems are deemed necessary, that such decisions (and the reasons therefor) are clearly recorded.

KEY CONTACTS

AMJAD HUSSAIN
PARTNER

DOHA
+974.4.424.6119
AMJAD.HUSSAIN@KLGATES.COM

