DATA PROTECTION LAWS OF THE WORLD

Qatar - Financial Centre

QATAR - FINANCIAL CENTRE

Last modified 17 January 2024

LAW

Note: Please also see Qatar.

The Qatar Financial Centre ("**QFC**"), a business center located on-shore in Qatar with its own regulations that are separate and distinct from those of the State of Qatar, implemented QFC Regulation No. 6 of 2005 on QFC Data Protection Regulations ("**DPL**").

Additionally, under the powers granted to the QFC Authority under Article 32(6) of the DPL, the QFC Authority has issued the Data Protection Rules 2005 (DPR).

The QFC updated the DPL and DPR on 6 December 2023. This note reflects the position under the DPL and DPR as amended. As a general comment, the changes provide increased clarity around the DPL and DRP as well as creating certain new obligations and bring the QFC more closely in line with the position under the GDPR and other similar laws, which should assist international businesses in taking a relatively uniform approach to their data compliance activities.

The DPL and DPR apply to the processing of personal data of living natural persons. Such processing may be by automated means or non-automated means. The DPL and DPR apply to data controllers and processors incorporated or registered in the QFC and to those that are not if, as part of ongoing arrangements, the data controller or processor process personal data through a data controller or processor that is incorporated or registered in the QFC unless it does so on an occasional basis.

DEFINITIONS

Definition of data controller

An individual or entity that determines the purposes and means of the processing of personal data.

Definition of data processor

An individual or entity that undertakes the processing of personal data on behalf of a data controller or another data processor.

Definition of data subject

A natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the data subject.

Definition of personal data

Any information relating to a data subject.

Definition of personal data breach

Any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosed of, or access to, personal data transmitted, stored or otherwise processed.

Definition of processing

Any operation or set of operations that is performed (whether or not by automatic means) on personal data or on sets of personal data, and includes collecting, recording, organizing, structuring, storing, adapting or altering, retrieving, consultation, using, disclosing by transmission, disseminating or otherwise making available, aligning or combining, restricting, erasing and destroying the personal data.

Definition of sensitive personal data

Personal data revealing or relating to race or ethnicity, political affiliation or opinions, religious or philosophical beliefs, trade-union or organizational membership, criminal records, health or sex life, and genetic and biometric data used to identify an individual.

NATIONAL DATA PROTECTION AUTHORITY

The Data Protection Office at the QFC Authority is the administrator of the DPL and DPR in the QFC ("**DPO**").

REGISTRATION

Unless certain exceptions apply, data controllers must obtain a permit from the DPO prior to processing sensitive personal data or transferring personal data outside of the QFC to a recipient who is not subject to laws or regulations that ensure an adequate level of protection for that personal data.

DATA PROTECTION OFFICERS

There is no requirement under the DPL or the DPR for organizations to appoint a data protection officer. Though note the general obligation of a data controller to implement appropriate technical and organizational measures to protect personal data, as further detailed below (see Security). It is however recommended that organizations that operates on a large scale or carries out regular and systematic monitoring of individuals appoint an individual responsible for overseeing the data controller’s compliance with data protection requirements.

COLLECTION & PROCESSING

Conditions for Consent

Data controllers must be able to show that the data subject's consent complies with the DPL where they are using consent as a basis for their processing activities.

Consent by a data subject must be:

- Freely given;
- Specific;
- Informed; and
- Unambiguous.

Where consent is given in a document that also concerns other matters then the consent must be:

- Clearly distinguishable;
- Intelligible and easily accessible; and

- Use clear, unambiguous and plain language.

Processing personal data

Data controllers may process personal data when any of the following conditions are met:

- The data subject has given his / her consent to the processing of that personal data;
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- Processing is necessary for compliance with an obligation to which the data controller is subject to by law;
- Processing is necessary in order to protect the vital interests of the data subject or another individual;
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of the QFC Authority, the QFC Regulatory Authority, QFC Civil and Commercial Court, the QFC Regulatory Tribunal or a QFC Institution;
- Processing is necessary for the purposes of the legitimate interests of the data controller or another person to whom the personal data is disclosed, except where such interests are overridden by legitimate interests of the data subject which require the data to be protected.

Processing sensitive personal data

Data controllers may process sensitive personal data when any of the following conditions are met:

- The data subject has given his / her explicit written consent to the processing;
- Processing is necessary for the purposes of carrying out the obligations and the exercise of specific rights of the data controller or the data processor in the field of employment law;
- Processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his / her consent;
- Processing is carried out by an insurance firm for the purposes of providing a life or health insurance policy;
- Processing is carried out by a non-for-profit body in the course of its legitimate activities with appropriate guarantees that the processing relates solely to the members or former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed to a third party without the consent of the data;
- Processing relates to personal data which is manifestly made public by the data subject;
- Processing is necessary to establish, pursue or defend a legal claim or when a court is acting in its judicial capacity;
- Processing is necessary for compliance with an obligation to which the data controller is subject to by law;
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of the QFC Authority, the QFC Regulatory Authority, QFC Civil and Commercial Court, the QFC Regulatory Tribunal or a QFC Institution;
- Processing is necessary for substantial public interest reasons that are proportionate to the aim or aims pursued, respect the principles relating to the processing of personal data and provide suitable and specific measures to safeguard the rights of the data subject;
- Processing is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of healthcare services, and where that personal data is processed by a health professional subject under national laws or regulations established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

TRANSFER

Data controllers may transfer personal data out of the QFC if the personal data is being transferred to a Recipient in a jurisdiction that the DPO has decided has laws and regulations that ensure an adequate level of protection for that personal data. The DPO has produced a list of jurisdictions which it deems to have such adequate levels of protection and may also take the following factors into consideration when assessing the adequacy of the level of protection ensured by laws and regulations to which the Recipient is subject to:

- The rule of law, the general respect for individual's rights and the ability of individuals to enforce their rights by administrative or judicial means;
- The access of public authorities to personal data;
- The existence of effective data protection regulations including on onward transfer of personal data to another jurisdiction;
- The existence and functioning of one or more independent supervisory authorities with adequate enforcement powers;
- International commitments and conventions binding on the jurisdiction and its membership of any multilateral or regional organizations;
- Decisions taken by other data protection authorities where their decisions take into consideration the same factors as those the DPO does.

In the absence of an adequate level of protection, data controllers may transfer personal data out of the QFC if any of the following are true:

- The data controller or data processor have appropriate adequate safeguards including enforceable rights and remedies for the data subjects which may be provided by a legally binding and enforceable arrangement between public authorities or a legally binding and enforceable agreement between parties which contain data protection clauses adopted by the DPO;
- The data subject has been informed of the risks of such transfer and has given his / her explicit consent to the proposed transfer;
- Transfer is necessary for the performance of a contract between the data subject and the data controller, or the implementation of pre-contractual measures taken in response to the data subject’s request;
- Transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the data controller and a third party;
- Transfer is legally required for the purposes of the data controller's or data processor's compliance with a legal obligation;
- Transfer is necessary in order to protect the vital interests of the data subject;
- Transfer is necessary to perform a task carried out in the public interest or by any of the following authorities in the performs of their functions, the QFC Authority, the QFC Regulatory Authority, the QFC Civil and Commercial Court, the QFC Regulatory Tribunal or a QFC Institution;
- Transfer is necessary for the establishment, exercise or defense of a legal claim.

If none of the above are applicable, a data controller may transfer personal data out of the QFC only if:

- DPO has granted a permit for the transfer or the set of transfers and the data controller applies adequate safeguards with respect to the protection of this personal;
- The transfer is based on binding corporate rules that fulfil the requirements of the DPR and approved by the DPO or another internationally acceptable transfer mechanism approved by the DPO; or
- The transfer:
    - Is not repeating or not part of a repetitive course of transfers;
    - Concerns only a limited number of data subjects;
    - Does not contain sensitive personal data;
    - Is for the purposes of the legitimate interests of the data controller or third party to which the data is disclosed unless sch legitimate interests are overridden by those of the data subject; and
    - The data controller has completed a documented assessment of the circumstances surrounding the data transfer and has provided adequate safeguards with regard to the protection of the personal data.

SECURITY

Data controllers and processors must implement appropriate technical and organizational measures to ensure an appropriate level of security in the processing of personal data. These measures include, but are not limited to:

- The de-identification and / or encryption of the personal data;
- Ability to ensure continuing confidentiality, integrity, availability and resilience of processing systems and advances;
- Ability to restore availability of and access to the personal data in a timely manner if a physical or technical incident has occurred;

- A process for routinely testing, assessing and evaluation the effectiveness of the measures.

The measures implemented ought to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected and in particular, to protect such personal data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, the personal data. In assessing what measures are appropriate, data controllers and processors can consider:

- Availability of technology;
- Costs of implementation;
- The processing activities; and
- The likelihood and severity of the risks to the rights and legitimate interests of individuals.

BREACH NOTIFICATION

There is a requirement under the DPL to inform the DPO of a Personal Data Breach. The notification must be made without undue delay and where possible, no later than 72 hours from the time the data controller is made aware of the breach.

The data controller must also consider notifying the data subjects affected of the breach and if the data controller determines that it will notify the data subjects then, it must notify them without undue delay after becoming aware of the breach and its notification:

- Must use clear and plain language;
- Must contain an explanation of the nature of the personal data breach;
- Must describe the consequences (or those that are likely) of the data breach; and
- Must contain a description of the measures taken or proposed to be taken by the data controller to address the breach and the measures to mitigate the effects of the breach.

The requirement to notify the DPO of a personal data breach does not apply if the breach is unlikely to result in a risk to the rights and legitimate interests of the data subjects.

ENFORCEMENT

In the QFC, the DPO oversees the enforcement of the DPL.

The DPO has, *inter alia*, the following powers:

- To order a data controller or processor to provide information that the DPO requires for the purposes of its performance of its duties;
- To carry out investigations and audits;
- To issue reprimands or orders to rectify infringements of the DPL and DPR;
- To order a data controller or processor to comply with the data subject's requests to exercise its rights under the DPL;
- To order a data controller or processor to carry out processing operations in a specified manner; and
- To impose penalties and such other corrective measures.

ELECTRONIC MARKETING

Immediately upon collecting personal data, the DPL requires data controllers to provide data subjects who they have collected personal data from, with, among other things, any further information to the extent necessary. This includes information on whether the personal data will be used for direct marketing purposes.

If the personal data has not been obtained from the data subject, the data controller or their representative must at the time of undertaking the recording of personal data or within a reasonable period no longer than 30 days after obtaining the personal data (taking into account the circumstances in which data are processed) – or if it is envisaged that the personal data will be disclosed to a third party, no later than when the personal data is first recorded or disclosed – provide the data subject with, among other things, information regarding whether the personal data will be used for direct marketing purposes.

A data subject has the right to object at any time to the processing of their personal data for direct marketing purposes. In which case, the personal data must no longer be processed for such purposes.

ONLINE PRIVACY

The DPL or DPR do not contain specific provisions relating to online privacy, however, the broad provisions detailed above are likely to apply. In addition, as Qatar criminal law applies in the QFC, the privacy principles laid out therein may apply (see Qatar).

KEY CONTACTS

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

Elias Al-Far
Associate
T +974 4420 6125
elias.al-far@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.