Assessment of Qatar Financial Centre (“QFC”)

as an

International Organisation recognised by the

Office of the Commissioner of Data Protection (“Commissioner”) of the Dubai International Financial Centre Authority (“DIFC” or “DIFCA”)

as ensuring an

Adequate Level of Data Protection

سلطة مركز دبي المالي العالمي، حكومة دبي
الطابق ١٤، البوابة، صندوق بريد ٧٤٧٧٧، دبي، الإمارات العربية المتحدة
Dubai International Financial Centre Authority, Government of Dubai
Level 14, The Gate, PO Box 74777, Dubai, United Arab Emirates
Tel +971 4 362 2222, Fax +971 4 362 2333
difc.ae

Table of Contents

Introduction

Articles 26 and 27 of the Data Protection Law, DIFC Law No. 5 of 2020 and Section 5 of the DIFC Data Protection Regulations 2020 (the "DIFC DP Law 2020"[1]) address transfers of Personal Data to Third Countries or International Organizations. Article 26(2) specifically states:

> *For the purposes of Article 26(1), the Commissioner may determine from time to time that a Third Country, a territory or one (1) or more specified sectors within a Third Country, or an International Organisation ensures an adequate level of data protection*.

Such adequacy recognition is based on an assessment of key data protection concepts and obligations found in a jurisdiction's data protection laws to ensure equivalence with the local data protection law. As such, the DIFC Office of the Commissioner of Data Protection assesses the QFC laws and regulations according to the following criteria[2]:

1. Basic data protection concepts and definitions
2. Grounds for lawful and fair processing for legitimate purposes
3. Existence of Data Protection Principles
    a. purpose limitation
    b. data quality and proportionality
    c. data retention
    d. security and confidentiality
    e. transparency
4. Data Subjects' Rights
    a. right of access, rectification, erasure and objection
5. International / Onward Data Transfer Restrictions
6. Security of Processing and Breach Reporting
7. Accountability
    a. Special categories of data (aka sensitive personal data)
    b. Direct marketing
    c. Automated decision making and profiling
8. Additional content principles for specific types of processing

[1] *All definitions and capitalized terms herein, including the definition of the DIFC Data Protection Commissioner, are as set out in DIFC DP Law 2020, Schedule 1, Article 3.*

[2] *Please see EU adequacy referential for guidance: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108*

9. Existence of international commitments and conventions binding on QFC or its membership of any multilateral or regional organisations

Summary of QFC's Applicable Laws and Regulations

Observation 1: Basic data protection concepts and definitions

Concepts:

The QFC Data Protection Regulations 2021 (the "Regulations") sets out in Article 8 the general requirements that Data Controllers must adhere to when processing Personal Data, these are:

- That the data is processed fairly, lawfully and transparently;
- That it is processed for specified, explicit and legitimate purposes in accordance with the Data Subject's rights and not further processed in a way incompatible with those purposes or rights;
- That it is adequate, relevant and limited to what is necessary in relation to the purposes for which it is collected or further processed;
- That it is accurate and, where necessary, kept up to date; and
- That it is kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data was collected or for which they are further processed.
- That it must be Processed in a way that ensures that the data are appropriately secure, using appropriate technical and organisational measures. In particular, the data must be protected against unauthorised or unlawful Processing and against accidental loss, destruction or damage.

Data Controllers must ensure that every reasonable step is taken to ensure Personal Data, which is inaccurate or incomplete with regard to the purpose for which it was collected, is erased or rectified.

Finally, Data Controllers must establish and maintain systems and controls that enable it to satisfy itself that it complies with the requirements of this Article. This is the accountability principle.

Definitions

Article 39 provides a comprehensive list of key terms used in the Regulations; of significant importance are:

Data Subject: a natural person who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

Personal Data: any information relating to a Data Subject.

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, organising, 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.

Data Controller: an individual or entity that determines the purposes and means of the Processing of Personal Data.

Data Processor: an individual or entity that undertakes the Processing of Personal Data on behalf of a Data Controller

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

Breach notification requirements:

Article 31 sets out breach notification requirements, including notifying the Data Protection Office as well as asking Data Controllers to consider notifying a Data Subject, where necessary, in clear plain language.

In addition, Section 4, Part 2 of the QFCA Rules deals with 'Notices to the QFCA'. Specifically, section 4.4 deals with significant events and states:

> *A Licensed Firm must advise the QFCA immediately if it becomes aware of any matters that have occurred or may occur in the foreseeable future that could materially impact on the Licensed Firm's ability to provide adequate services to its Client and/or to continue in business and/or have a significant adverse impact on the reputation of the Licensed Firm or of the QFC.*

Chapter 4.1.3 of the QFCRA General Rules deals with 'Notice of certain significant events'. In particular, section 4.1.3 which states:

> *If an authorised firm becomes aware, or has reasonable grounds to believe, that a matter to which this rule applies has or may have happened, or may be about to happen, the firm must tell the Regulatory Authority about the matter immediately, but within 1 business day.*

Firms have used this mechanism to report data breaches as well.

The Regulations include a 72-hour reporting obligation. The Data Protection Office has the power to order such notification if it deems it necessary.

Enforcement powers

The Data Protection Office's powers are set out in Articles 33 of the Regulations, enumerating 1) corrective, 2) authorisation and advisory, and 3) enforcement powers .

In addition, the QFCRA undertakes regular enforcement activity, including investigations and imposing fines on regulated entities. The QFCRA is also subject to the Regulations, and as such, must in its objectives and carrying out any powers, and specifically enforcement powers, adhere to data protection principles.

Observation 2: Grounds for lawful and fair processing for legitimate purposes

Grounds for lawful processing are included in Article 10 of the Regulations.

These are summed up as:

- Consent;
- Necessary for the performance of a contract or in order to take steps to enter a contract;
- Compliance with any legal obligation;
- To protect the vital interests of the Data Subject;
- In the performance of a task carried out in the interests of the QFC or in the exercise of QFCA, QFCRA, Tribunal or Appeals Body functions or powers vested in the Data Controller or in a Third Party to whom the Personal Data is disclosed; or
- It is necessary for the purposes of the legitimate interests pursued by the Data Controller or another Person to whom the data are disclosed (unless those interests are overridden by the rights and legitimate interests of the Data Subject that require the data to be protected, in particular if the Data Subject is a Child).

Further to this, where a Data Controller wants to process Sensitive Personal Data, they must also meet one of the special conditions included in Article 12. These are summed up as:

- Explicit written consent (also addressed specifically in Article 11);
- Necessary to meet obligations and rights of the Data Controller in the field of employment law;
- Necessary to protect the vital interests of the Data Subject;
- Where the processing is carried out by a foundation, association or any other non-profit-seeking body in the course of its legitimate activities with appropriate guarantees that the Processing relates solely to the 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 Subjects;
- Where the processing relates to Personal Data which is manifestly made public by the Data Subject or is necessary for the establishment, exercise or defence of legal claims;
- Where the processing is necessary for compliance with any legal obligation to which the Data Controller is subject;
- Where the processing is necessary to uphold the legitimate interests of the Data Controller recognised in the international financial markets, provided that such is pursued in accordance with international financial standards and except where such interests are overridden by compelling legitimate interests of the Data Subject relating to the data subject's particular situation;
- Where the processing is necessary to comply with auditing, accounting or anti money laundering obligations that apply to a Data Controller; or
- Where the processing is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care 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.

Observation 3: Existence of Data Protection Principles

The Regulations include the general requirements set out in Observation 1 with respect to Article 8.

Articles 14 and 15 deal with transparency and require Data Controllers to provide information to Data Subjects when their Personal Data are first collected or collected indirectly, respectively.

Article 29 details the requirements in the areas of confidentiality and security of processing.

Observation 4: Data Subjects Rights (DSR)

Part 3, Articles 16 to 22 of the Regulations deal with Data Subject Rights.

Article 16 to 20 details the rights to access, rectification, erasure and the blocking of Personal Data.

The DSR include right to object to processing and the right to be informed about personal data disclosure to third parties or used on their behalf for direct marketing. This notification must also include an opportunity for the Data Subject to object to such disclosure.

The Regulations were updated in 2021 to enhance Data Subject rights by providing more clarity on the existing rights and introducing new rights, including portability and automated individual decision-making, including profiling.

Observation 5: International Data Transfers

Article 23 and 24 of the Regulations deal with data transfers to recipients outside the QFC.

Transfers of Personal Data outside the QFC are permitted once the jurisdiction to which the Personal Data are being transferred has been assessed by the Data Controller as providing an adequate level of protection for that Personal Data. Where a firm's assessment of the recipient jurisdiction is deemed to not offer an adequate level of protection, the firm may proceed with the transfer only where one of the exceptions in Article 10 of the Regulations are met.

Adequacy assessment of recipient jurisdictions

Prior to a Data Controller transferring Personal Data to a recipient in a jurisdiction outside the QFC for the first time they must first undertake an assessment of that jurisdiction. The assessment is to ensure that the levels of protection for the Personal Data is ensured by laws and regulations in that jurisdiction and which are applicable to the recipient.

It is critical that Data Controllers not only assess if there are suitable data protection laws and regulations in place but assess if they are applied in practice, to the recipient, and that they provide meaningful and effective remedies for Data Subjects to enforce their rights.

The adequacy assessment must be undertaken by the Data Controller and must take into consideration:

- the nature of the data being transferred;
- the purpose and duration of the processing;
- if the data does not emanate from the QFC, the country of origin and country of final destination of the personal data; and
- any relevant laws to which the recipient is subject.

In addition to the items mentioned above, Data Controllers may take into account the following:

- the law in force in the jurisdiction in question regarding data protection;
- international obligations to which the recipient is subject;
- any relevant codes of conduct or other rules which are enforceable in that jurisdiction;
- any security measures taken in respect of the data in that jurisdiction; and
- whether (or the extent to which) the jurisdiction in question is the subject of any finding or presumption of adequacy by another data protection regulator or other relevant body (such as the European Commission).

The list is not exhaustive as Data Controllers must be satisfied that the recipient jurisdiction adequately protects Personal Data.

Changes in circumstance for the recipient jurisdiction

Data Controllers must review their assessment of adequacy for recipient jurisdictions on a regular basis as there could be changes in the legal protections for Data Subjects and Personal Data. Specifically, where a Data Controllers is using a presumption of adequacy by another data protection regulator, such as the

European Union, in their assessment any subsequent change to such adequacy assessments should serve as a trigger event to review the firm's assessment of the adequacy of the recipient jurisdiction.

Transfers to jurisdictions not deemed adequate

Where a Data Controllers' assessment of the recipient jurisdiction is deemed not to offer an adequate level of protection, the transfer can go ahead if one of the conditions in Article 10(1) (B) to (J) are met, these include:

- the Data Subject has given their consent to the transfer;
- the transfer is necessary for the implementation or performance of a contract between the Data Subject and the Data Controller; or
- the transfer is necessary for compliance with any legal obligation to which the Data Controller is subject.

Permit to transfer

A Data Controller can apply to the Data Protection Office for a permit to undertake a transfer to a non-adequate jurisdiction.

There is a simple and straightforward process for QFC firms to apply for a permit via the e-Portal.

The Regulations permit the Data Protection Commission to publish a list of adequate jurisdictions. Where the recipient is located within one of these jurisdictions' transfers are permitted without any further requirements (without prejudice to other provision in relation to Data Controllers or Data Processors)

Observation 6: Security of Processing and Breach Reporting:

Confidentiality and Security provisions are included in Article 29 of the Regulations. Breach reporting is included in Observation 1.

Enforcement follows the current monitoring and enforcement priorities. Significant events or claims lodged by a Data Subject may trigger an enforcement action.

When updated in 2021, the Regulations provided further granularity on the security provisions and introduces a requirement to have data protection policies. Further, the concepts of privacy by default and design and data protection impact assessments were introduced to ensure data privacy risks are identified and mitigated, as far as possible, prior to the commencement of processing.

Observation 7: Accountability, principles and legitimate processing (including direct marketing or other compliance obligations required by other laws and regulations)

Observations 1 and 2 provide details on the principles and the legitimate basis for processing as included in the Regulations.

Accountability is largely covered in Part 5 of the Regulations, but at the outset, it is included in Article 9, which states:

A Data Controller must be able to demonstrate that it complies with the principles in Article 8.

Privacy by Design and Default requirements are outlined in Article 26 The processing of Personal Data for direct marketing must comply with the general requirements and Data Subjects may object to direct marketing.

Enforcement follows the current monitoring and enforcement priorities. Significant events or claim lodged by a Data Subject may trigger an enforcement action.

Observation 8: Additional content principles for specific types of processing (including sharing for the purposes of law enforcement)

The Regulations do not specifically mention processing for law enforcement at this time. Any processing, including the transfer of Personal Data, must comply with the lawful basis, as discussed in Observation 2.

Observation 9: Existence of international commitments and conventions binding on QFC or its membership of any multilateral or regional organisations

The QFC is not a member and is not bound by any international commitments or conventions or multilateral or regional organisations.

QFC has been a Member of the Global Privacy Enforcement Network (GPEN) since 2022 and was also granted Membership status in the Global Privacy Assembly in 2024.

Conclusion

The Qatar Financial Centre Authority has provided the above feedback and references to its laws and regulations to support recognition of adequacy the Regulations by the DIFC Authority Commissioner's Office. All elements that substantiate such recognition are generally present. Enforcement and supervision, data subjects' rights, the establishment of an independent Commissioner under the Authority, and other key updates were enacted included in the 2021 update to the initial Regulations promulgated in 2005. All such updates will align with the DIFC DP Law 2020 and other laws such as the GDPR and the UK DPA 2018 / UK GDPR.

QFC Data Protection Office has recently added DIFC Authority to its list of adequate jurisdictions as well.

Specifically, regarding regulated entities, QFCRA is committed to preventing financial crime through its AML/CFT framework, and strengthened cyber security capabilities within the financial sector to mitigate cybercrime.[3]

QFCRA authorized firms are subject to substantially the same financial crime prevention and macro-prudential supervision objectives and requirements as those supervised by the DFSA (collectively, "Regulated Firms"). A list of authorized firms is available from the QFCRA's public register, and a list of DNFBP's is available from the QFCA's public register and may be updated from time to time. Please see Appendix 1 for further guidance about these firms.

It is for these reasons that the DIFC Office of the Commissioner of Data Protection grants adequacy recognition to QFCRA as an International Organisation that ensures adequate data protection in accordance with Article 26 of the DP Law 2020. The QFC's current laws and regulations align to a substantial extent with the DIFC DP Law 2020 such that data transfers to QFC entities will receive the same or substantially equivalent protection.

The Commissioner has the right to repeal, amend or suspend this adequacy decision by notification to QFCA at any time. This decision shall be reviewed annually.

Jacques Visser, Commissioner of Data Protection

Dated: January 5, 2026

[3] Please see Strategic Goal 3: https://www.qfcra.com/five-strategic-goals/

Appendix 1: Enforcement Action

Data Protection Enforcement

The Qatar Financial Centre (QFC) Data Protection Office (DPO) issues significant fines for data protection breaches, recently levying a $150,000 penalty on a QFC firm in late 2024 for failing to report a data breach within the mandated 72-hour window and for inadequate data security.

Enforcement action options include:

- Warnings or admonishments or recommendations to Data Controllers issued
- Contraventions of the Regulations brought to the attention of the Tribunal (Qatar International Court and Dispute Resolution Centre)
- Directions issued to Data Controllers
- Investigations conducted

Recent enforcement actions:

Data Breach violations 2024

Appendix 2: Commitment to substantially comply with Article 28 of the DIFC DP Law 2020

Article 28 of the DIFC DP Law 2020 states the following:

Data sharing

(1) Subject to any other obligations under this Law and, in particular, a Controller's or Processor's obligations under Part 2 regarding accountability, transparency and compliance with general data protection principles or Part 4 regarding transfers out of the DIFC, where a Controller or Processor receives a request from any public authority over the person or any part of its Group ("a Requesting Authority") for the disclosure and transfer of any Personal Data, it should:

(a) exercise reasonable caution and diligence to determine the validity and proportionality of the request, including to ensure that any disclosure of Personal Data in such circumstances is made solely for the purpose of meeting the objectives identified in the request from the Requesting Authority;

(b) assess the impact of the proposed transfer in light of the potential risks to the rights of any affected Data Subject and, where appropriate, implement measures to minimise such risks, including by redacting or minimising the Personal Data transferred to the extent possible or utilising appropriate technical or other measures to safeguard the transfer; and

(c) where reasonably practicable, obtain appropriate written and binding assurances from the Requesting Authority that it will respect the rights of Data Subjects and comply with the general data protection principles set out in Part 2 in relation to the Processing of Personal Data by the Requesting Authority.

(2) A Controller or, as applicable, its Processor(s) or any Sub-processor(s), having provided (where possible under Applicable Law) reasonable notice to the Controller, may disclose or transfer Personal Data to the Requesting Authority where it has taken reasonable steps to satisfy itself that:

(a) a request by a Requesting Authority referred to in Article 28(1) is valid and proportionate; and

(b) the Requesting Authority will respect the rights of Data Subjects in the Processing of any Personal Data transferred to it by the Controller pursuant to a request under Article 28(1).

(3) A Controller or Processor may consult with the Commissioner in relation to any matter under this Article 28.

The QFCA's Data Protection Office will endeavour to monitor compliance with Article 28 of the DIFC DP Law 2020, to the extent practicable under applicable laws and regulations. QFCA, QFCRA and DIFCA may elect to document this by way of a Memorandum of Understanding or similar arrangement within a reasonable period after the date of this Decision, to be regularly reviewed by the QFCA, QFCRA and DIFCA.