

# QFC DATA PROTECTION REGULATIONS

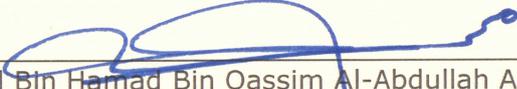
DECEMBER 2021



مركز قطر للمال  
QATAR FINANCIAL CENTRE

QATAR FINANCIAL CENTRE  
REGULATION NO. 6 of 2005  
QFC DATA PROTECTION REGULATIONS

The Minister of Commerce and Industry hereby enacts the following regulations pursuant to Article 9 of Law No. (7) of 2005.

  
Mohammed Bin Hamad Bin Qassim Al-Abdullah Al-Thani  
Minister of Commerce and Industry of the State of Qatar

Issued at: The Qatar Financial Centre, Doha

On: 21 DECEMBER 2021

Corresponding to: 17 JUMADA AL-AWWAL 1443

## CONTENTS

PART 1 – APPLICATION, COMMENCEMENT AND INTERPRETATION .....	6
ARTICLE 1 – CITATION.....	6
ARTICLE 2 – APPLICATION.....	6
ARTICLE 3 – COMMENCEMENT AND REPEAL.....	6
ARTICLE 4 – LANGUAGE .....	6
ARTICLE 5 – PURPOSE OF THESE REGULATIONS .....	6
ARTICLE 6 – GENERAL APPLICATION OF THESE REGULATIONS .....	7
ARTICLE 7 – SCOPE .....	7
PART 2 – GENERAL PROVISIONS FOR THE PROCESSING OF PERSONAL DATA.....	7
ARTICLE 8 – PRINCIPLES RELATING TO THE PROCESSING OF PERSONAL DATA .....	7
ARTICLE 9 – RESPONSIBILITY FOR COMPLIANCE WITH THE PRINCIPLES .....	8
ARTICLE 10 – LAWFULNESS OF PROCESSING .....	8
ARTICLE 11 – CONDITIONS FOR CONSENT .....	10
ARTICLE 12 – PROCESSING OF SENSITIVE PERSONAL DATA .....	11
ARTICLE 13 – TRANSPARENT INFORMATION, COMMUNICATION AND EXERCISE OF THE RIGHTS OF THE DATA SUBJECT .....	12
ARTICLE 14 – INFORMATION TO BE PROVIDED WHERE PERSONAL DATA ARE COLLECTED FROM THE DATA SUBJECT .....	13
ARTICLE 15 – INFORMATION TO BE PROVIDED WHERE PERSONAL DATA ARE NOT COLLECTED FROM THE DATA SUBJECT .....	13
PART 3 – DATA SUBJECTS’ RIGHTS .....	15
ARTICLE 16 – RIGHT TO ACCESS .....	15
ARTICLE 17 – RIGHT TO RECTIFICATION.....	15
ARTICLE 18 – RIGHT TO ERASURE.....	15
ARTICLE 19 – RIGHT TO OBJECT .....	16
ARTICLE 20 – RIGHT TO RESTRICTION OF PROCESSING.....	17
ARTICLE 21 – RIGHT TO DATA PORTABILITY.....	17
ARTICLE 22 – AUTOMATED INDIVIDUAL DECISION-MAKING, INCLUDING PROFILING .....	18
PART 4 – TRANSFERS OF DATA OUTSIDE THE QFC.....	20
ARTICLE 23 – TRANSFERS OUT OF THE QFC: ADEQUATE LEVEL OF PROTECTION .....	20
ARTICLE 24 – TRANSFERS OUT OF THE QFC IN THE ABSENCE OF AN ADEQUATE LEVEL OF PROTECTION.....	21
PART 5 – DATA CONTROLLER AND DATA PROCESSOR OBLIGATIONS.....	23
ARTICLE 25 – RESPONSIBILITY OF THE DATA CONTROLLER .....	23
ARTICLE 26 – DATA PROTECTION BY DESIGN AND BY DEFAULT.....	23
ARTICLE 27 – DATA PROTECTION IMPACT ASSESSMENT .....	23
ARTICLE 28 – DATA PROCESSORS.....	24
ARTICLE 29 – SECURITY OF PROCESSING .....	25
ARTICLE 30 – RECORD OF PROCESSING OPERATIONS .....	26
ARTICLE 31 – NOTIFICATION OF PERSONAL DATA BREACHES .....	26
PART 6 – THE DATA PROTECTION OFFICE .....	27
ARTICLE 32 – ESTABLISHMENT OF THE DATA PROTECTION OFFICE AND THE DATA PROTECTION COMMISSIONER .....	27

ARTICLE 33 – POWERS.....	27
PART 7 – REMEDIES .....	30
ARTICLE 34 – RIGHT TO LODGE A COMPLAINT WITH THE DATA PROTECTION OFFICE .....	30
ARTICLE 35 – RIGHT TO COMPENSATION AND LIABILITY .....	31
ARTICLE 36 – GENERAL CONDITIONS FOR IMPOSING PENALTIES .....	31
PART 8 – FINAL PROVISIONS .....	33
ARTICLE 37 – GENERAL EXEMPTIONS .....	33
ARTICLE 38 – INTERPRETATION .....	33
ARTICLE 39 – DEFINITIONS.....	34

## PART 1 – APPLICATION, COMMENCEMENT AND INTERPRETATION

### ARTICLE 1 – CITATION

These Regulations are the Data Protection Regulations 2021.

### ARTICLE 2 – APPLICATION

These Regulations are made by the Minister in accordance with Article 9 of the QFC Law and apply in the QFC. To the fullest extent permitted by the QFC Law, the laws, rules and regulations of the State of Qatar concerning the matters dealt with, by or under these Regulations do not apply in the QFC.

### ARTICLE 3 – COMMENCEMENT AND REPEAL

- (1) In this Article:  
**Commencement Date** means 180 days after the date of the signature of these Regulations by the Minister.
- (2) The QFCA may, by notice, extend the Commencement Date until such date as it considers appropriate.
- (3) These Regulations (other than Article 32) come into force on the Commencement Date.
- (4) Article 32 comes into force on the signature of these Regulations by the Minister.
- (5) The Data Protection Regulations 2005 and the Data Protection Rules 2005 are repealed on the Commencement Date.

### ARTICLE 4 – LANGUAGE

In accordance with a determination by the Minister in accordance with Article 9 of the QFC Law, these Regulations are written in English and the English text is the only authoritative text. A translation into another language is not authoritative.

### ARTICLE 5 – PURPOSE OF THESE REGULATIONS

These Regulations are intended:

- (A) to protect the rights and legitimate interests of individuals in relation to their Personal Data; and
- (B) to set out principles and rules about protecting and Processing Personal Data.

## ARTICLE 6 – GENERAL APPLICATION OF THESE REGULATIONS

- (1) These Regulations apply to the Processing of the Personal Data of living natural persons. Such Processing may be by:
  - (A) automated means; or
  - (B) non-automated means (in the case of Personal Data that forms part of a Filing System or is intended to form part of a Filing System).
- (2) Unless specifically provided in these Regulations or in any other legislation, these Regulations do not apply to the Personal Data of deceased persons.

## ARTICLE 7 – SCOPE

- (1) These Regulations apply to the Processing of Personal Data by a Data Controller or Data Processor incorporated or registered in the QFC.
- (2) These Regulations also apply to the Processing of Personal Data by a Data Controller or Data Processor that is not incorporated or registered in the QFC, if, as part of ongoing arrangements, that Data Controller or Data Processor Processes Personal Data through a Data Controller or Data Processor that is incorporated or registered in the QFC (but not if it does so only on an occasional basis). In this case, these Regulations apply only to the extent of that Processing activity.

## PART 2 – GENERAL PROVISIONS FOR THE PROCESSING OF PERSONAL DATA

### ARTICLE 8 – PRINCIPLES RELATING TO THE PROCESSING OF PERSONAL DATA

- (1) Principle 1: Lawfulness, fairness and transparency

Personal Data of a Data Subject must be Processed lawfully, fairly and transparently.

- (2) Principle 2: Specific purpose

Personal Data must be Processed only for specific, explicit and legitimate purposes and only in accordance with the relevant Data Subject's rights set out in these Regulations. A Data Processor must not further Process Personal Data in a way that is incompatible with those purposes or those rights.

- (3) Principle 3: Data minimisation

Personal Data that is Processed must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are Processed.

- (4) Principle 4: Accuracy

Personal Data may be Processed only if the data are accurate and up to date. Reasonable efforts (taking into account the purposes for which the data were Processed) must be made to ensure that Personal Data that are inaccurate are erased or corrected without undue delay.

(5) Principle 5: Storage limitation

Personal Data must be kept in a form that permits Data Subjects to be identified but only for as long as is necessary for the purposes for which the data were Processed.

(6) Principle 6: Integrity and confidentiality of Processing

Personal Data 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.

## ARTICLE 9 – RESPONSIBILITY FOR COMPLIANCE WITH THE PRINCIPLES

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

## ARTICLE 10 – LAWFULNESS OF PROCESSING

(1) The Processing of Personal Data is lawful only if, and only to the extent that, at least one of the following paragraphs applies:

- (A) the Data Subject concerned has given their consent to the Processing of their Personal Data for one or more specific purposes;
- (B) the Processing is necessary:
  - (i) to perform a contract to which the Data Subject is a party; or
  - (ii) in order to take steps at the Data Subject's request before entering into a contract;
- (C) the Processing is necessary to comply with an obligation imposed on the Data Controller by law;
- (D) the Processing is necessary to protect the vital interests of the Data Subject or another individual;
- (E) the Processing is necessary to perform a task carried out:
  - (i) in the public interest; or
  - (ii) by any of the following in the performance of its functions:
    - (a) the QFC Authority;

- (b) the QFC Regulatory Authority;
  - (c) the Civil and Commercial Court;
  - (d) the Regulatory Tribunal;
  - (e) a QFC Institution;
- (F) the Processing is necessary for the purposes of the legitimate interests of 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).

## ARTICLE 11 – CONDITIONS FOR CONSENT

- (1) If a Data Controller Processes Personal Data on the basis of consent, the Data Controller must be able to show that the consent complies with these Regulations.
- (2) Consent by a Data Subject must be:
  - (A) freely given;
  - (B) specific;
  - (C) informed; and
  - (D) an unambiguous indication by the Data Subject that they agree to the Processing of the relevant Personal Data.
- (3) If consent is given in a document that also concerns other matters, then the consent must:
  - (A) be clearly distinguishable from the other matters;
  - (B) be intelligible and easily accessible; and
  - (C) use clear, unambiguous, and plain language.
- (4) The withdrawal of a consent does not render unlawful any Processing based on the consent before it was withdrawn.
- (5) A Data Subject must be able to withdraw their consent as easily as it was given, at any time and in any form, and must be informed of this right before giving their consent.
- (6) When deciding whether a consent to the Processing of Personal Data was freely given, consideration must be given to whether the performance of a contract (including the provision of a service) was conditional on the consent being given to the Processing of Personal Data that is not necessary to the performance of that contract.

## ARTICLE 12 – PROCESSING OF SENSITIVE PERSONAL DATA

- (1) Subject to paragraph (2), the Processing of Sensitive Personal Data is prohibited unless one or more of the following paragraphs apply:
  - (A) the Data Subject has given their explicit written consent to the Processing for one or more specific purposes;
  - (B) the Processing is necessary to carry out the obligations, and exercise specific rights, of the Data Controller or Data Subject under employment law, including the assessment of the Data Subject's working capacity as an employee;
  - (C) the Processing is necessary to protect the vital interests of the Data Subject or another individual and the Data Subject is physically or legally incapable of giving their consent;
  - (D) the Processing is carried out by an insurance firm for the purposes of providing a policy for life or health insurance;
  - (E) the Processing is carried out by a not-for-profit entity in the course of its legitimate activities and with appropriate safeguards, but only if:
    - (i) the Processing relates solely to members or former members of the entity or to individuals who have regular contact with it in connection with its purposes; and
    - (ii) the data are not disclosed to any other person without the consent of the Data Subject;
  - (F) the Processing relates to Personal Data that the Data Subject has manifestly made public;
  - (G) the Processing is necessary to establish, pursue or defend a legal claim or when a court is acting in its judicial capacity;
  - (H) the Processing is necessary to comply with an obligation imposed on the Data Controller by law;
  - (I) the Processing is necessary to perform a task carried out by any of the following in the performance of its functions:
    - (i) the QFC Authority;
    - (ii) the QFC Regulatory Authority;
    - (iii) the Civil and Commercial Court;
    - (iv) the Regulatory Tribunal;
    - (v) a QFC Institution;

- (J) the Processing is necessary for substantial public interest reasons that:
    - (i) are proportionate to the aim or aims pursued;
    - (ii) respect the principles of data protection referred to in Article 8; and
    - (iii) provide for suitable and specific measures to safeguard the rights of the Data Subject;
  - (K) 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 that Personal Data is Processed by:
    - (i) a health professional, subject to national laws or regulations established by national competent bodies, with an obligation of professional secrecy; or
    - (ii) another person also subject to an equivalent obligation of professional secrecy.
- (2) Paragraph (1) does not apply if the Data Controller:
- (A) has obtained a permit from the Data Protection Office to Process the relevant Personal Data; and
  - (B) applies adequate safeguards in the Processing.
- (3) A Data Controller may appeal against a refusal by the Data Protection Office to issue a permit under paragraph (2)(A), to the Regulatory Tribunal, in accordance with Article 33(6).

## ARTICLE 13 – TRANSPARENT INFORMATION, COMMUNICATION AND EXERCISE OF THE RIGHTS OF THE DATA SUBJECT

- (1) When a Data Controller gives information in accordance with Article 14 or 15 or makes any communication under Articles 16 to 22, the Data Controller must do so in a concise, transparent, intelligible and easily accessible form, using clear and plain language.
- (2) The information must be given, or the communication made, in writing or by other appropriate means, including electronically.
- (3) If a Data Subject makes a request to a Data Controller under any of Articles 16 to 22, the Data Controller must inform the Data Subject about action taken on the request without undue delay, and at the latest within 30 days from receiving the request.
- (4) The Data Controller may extend the period mentioned in paragraph (3) for a further 60 days if it is necessary to do so because of the complexity and number of the relevant requests. The Data Controller must inform the Data Subject of any extension and the reasons for it within 30 days from receiving the initial request.

- (5) Where the Data Controller has reasonable doubts concerning the identity of the Data Subject making a request referred to in Articles 16 to 22, the Data Controller may request the maker of the request to provide additional information necessary to confirm the identity of the Data Subject.
- (6) If a Data Controller does not take action on a request referred to in Articles 16 to 22, it must inform the Data Subject concerned without undue delay, and at the latest within 30 days from receiving the request, of the reasons for not taking action. The Data Controller must also inform the Data Subject that they may lodge a complaint with the Data Protection Office for a review of the Data Controller's failure to take action on the request.
- (7) Subject to paragraph (8), a Data Controller must not impose a charge to give information, or make a communication, required by these Regulations. In particular, information provided under Article 14 or 15 and any communication made or action taken under Articles 16 to 22 must be free of charge.
- (8) If requests from a particular Data Subject are manifestly unfounded or excessive, in particular because of their repetitive character, the Data Controller may either:
  - (A) charge a reasonable fee (taking into account the administrative costs of providing the information or communication or taking the action requested); or
  - (B) refuse to act on the request.
- (9) The Data Controller bears the burden of demonstrating that a request is manifestly unfounded or excessive.

#### **ARTICLE 14 – INFORMATION TO BE PROVIDED WHERE PERSONAL DATA ARE COLLECTED FROM THE DATA SUBJECT**

- (1) At the time when Personal Data are first collected from a Data Subject, the Data Controller must give the Data Subject the information set out in the Data Protection Rules clearly and separately from any other information.
- (2) If the Data Controller intends to further Process the Personal Data for a purpose other than that for which the data were collected, then, before that further Processing, the Data Controller must also give the Data Subject information on that other purpose.

#### **ARTICLE 15 – INFORMATION TO BE PROVIDED WHERE PERSONAL DATA ARE NOT COLLECTED FROM THE DATA SUBJECT**

- (1) Where Personal Data have not been obtained from the Data Subject, the Data Controller must provide the Data Subject with the information set out in the Data Protection Rules clearly and separately from any other information.

- (2) The Data Controller must give the information referred to in paragraph (1) to the Data Subject:
  - (A) within a reasonable period, but no longer than 30 days after obtaining the Personal Data, taking into account the circumstances in which the data are Processed;
  - (B) if the Personal Data are to be used for communication with the Data Subject, no later than the time of the first communication with them; or
  - (C) if the Data Controller envisages that the Personal Data will be disclosed to another Recipient, no later than when the data are first disclosed.
- (3) If the Data Controller intends to further Process the Personal Data for a purpose other than that for which the data were collected, then, before that further Processing, the Data Controller must give the Data Subject information on that other purpose and any relevant further information referred to in paragraph (1).
- (4) Paragraph (1) does not apply:
  - (A) if the Data Subject already has the information;
  - (B) if doing so would be impossible or would involve disproportionate effort;
  - (C) to the extent that complying with the obligation in paragraph (1) would make impossible, or seriously impair, the achievement of the objectives of the Processing; or
  - (D) if obtaining or disclosing the relevant Personal Data is required by a law to which the Data Controller is subject, and that law provides appropriate measures to protect the Data Subject's legitimate interests.
- (5) In a case referred to in paragraph (4)(C), the Data Controller must take appropriate measures to protect the Data Subject's rights and legitimate interests. The measures must include making the information referred to in paragraph (1) publicly available.

## PART 3 – DATA SUBJECTS’ RIGHTS

### ARTICLE 16 – RIGHT TO ACCESS

- (1) A Data Subject has the right to obtain from a Data Controller confirmation about whether Personal Data about the Data Subject are being Processed. If the Data Subject’s Personal Data are being Processed, the Data Subject has the right to be given access to it and to be given the information set out in the Data Protection Rules.
- (2) If Personal Data of a Data Subject are transferred to another jurisdiction, the Data Subject has the right to be informed of the appropriate safeguards that apply to the transfer.
- (3) The Data Controller must give the Data Subject a copy of the Personal Data that is being Processed when requested by the Data Subject to do so.
- (4) The Data Subject may ask for an additional copy or copies of the data but the Data Controller may charge a reasonable fee (based on administrative costs) for the copy or copies. If the Data Subject makes a request by electronic means, the Data Controller must provide the additional copy or copies in a commonly used electronic form unless the Data Subject requests otherwise.
- (5) The right to obtain a copy referred in paragraph (3) must not adversely affect the rights and legitimate interests of others.

### ARTICLE 17 – RIGHT TO RECTIFICATION

- (1) A Data Subject has the right to have a Data Controller rectify inaccurate Personal Data about the Data Subject without undue delay.
- (2) A Data Subject has the right to have a Data Controller complete Personal Data that is incomplete (taking into account the purposes of the relevant Processing), including by incorporating a supplementary statement made by the Data Subject.

### ARTICLE 18 – RIGHT TO ERASURE

- (1) A Data Subject has the right, in the circumstances set out in paragraph (2), to have a Data Controller erase Personal Data about the Data Subject that the Data Controller holds. In those circumstances, if a Data Subject makes a request, the Data Controller must erase the Personal Data without undue delay.
- (2) The circumstances are the following:
  - (A) the Personal Data are no longer necessary for the purposes for which they were collected or otherwise Processed;
  - (B) the Data Subject withdraws consent to the Processing and there is no other legal ground for the Processing;

- (C) the Data Subject objects, in accordance with Article 19(1);
  - (D) the Personal Data have been unlawfully Processed; or
  - (E) the Personal Data must be erased to comply with a legal obligation to which the Data Controller is subject.
- (3) If the Data Controller has made the Personal Data public and is obliged under paragraph (1) to erase it, the Data Controller must take reasonable steps to inform any other Data Controller that is Processing the Personal Data that the Data Subject has asked for erasure of:
- (A) any links to the Personal Data;
  - (B) copies of the Personal Data; or
  - (C) replication of the Personal Data.
- (4) In fulfilling their obligations under paragraph (3), the Data Controller may take into account the available technology and the cost of implementation.
- (5) Paragraphs (1), (2) and (3) do not apply to the extent that Processing is necessary:
- (A) to comply with a legal obligation of the Data Controller;
  - (B) in the exercise of official authority vested in the Data Controller;
  - (C) for reasons of public interest; or
  - (D) to establish, pursue or defend a legal claim.

## ARTICLE 19 – RIGHT TO OBJECT

- (1) A Data Subject has the right to object, on grounds relating to their particular situation, at any time to the Processing of Personal Data which is in accordance with Article 10(1)(E)(i) and (F).
- (2) If a Data Subject objects under paragraph (1), a Data Controller must not continue to Process the relevant Personal Data unless:
- (A) the Data Controller demonstrates that there are compelling legitimate grounds for the Processing that override the interests, rights and legitimate interests of the Data Subject; or
  - (B) the Processing is necessary to establish, pursue or defend a legal claim.
- (3) A Data Subject has the right to object at any time to the Processing of their Personal Data for direct marketing purposes. If a Data Subject objects to the Processing of their Personal Data for direct marketing purposes, the Personal Data must no longer be Processed for those purposes.

- (4) A Data Controller must inform a Data Subject about their rights under paragraphs (1) to (3) and must do so clearly and separately from any other information. The Data Controller must do so no later than the time of the Data Controller's first communication with the Data Subject.

## ARTICLE 20 – RIGHT TO RESTRICTION OF PROCESSING

- (1) A Data Subject has the right to require a Data Controller to restrict Processing if one of the following applies:
- (A) the Data Subject contests the accuracy of the Personal Data in which case the restriction will only apply for as long as it takes the Data Controller to verify the accuracy of the Personal Data;
  - (B) the Processing is unlawful and the Data Subject opposes the erasure of the Personal Data and requests the restriction of their use instead;
  - (C) the Data Controller no longer needs the Personal Data for the purposes of the Processing, but the Personal Data are required by the Data Subject for the establishment, exercise or defence of a legal claim;
  - (D) the Data Subject has objected to Processing in accordance with Article 19(1) pending the verification whether the legitimate grounds of the Data Controller override those of the Data Subject.
- (2) Where Processing has been restricted under paragraph (1), with the exception of storage, the Personal Data can only be Processed:
- (A) with the Data Subject's consent;
  - (B) for the establishment, exercise or defence of a legal claim;
  - (C) for the protection of the rights of another natural or legal person, or
  - (D) for reasons of public interest.
- (3) If Processing has been restricted under paragraph (1), a Data Controller must inform the Data Subject before the restriction of Processing is lifted.

## ARTICLE 21 – RIGHT TO DATA PORTABILITY

- (1) The Data Subject has the right to receive Personal Data about them, which they have provided to a Data Controller, in a structured, commonly used and machine-readable format if:
- (A) the Processing is based:
    - (i) on consent in accordance with Article 10(1)(A) or Article 12(1)(A); or
    - (ii) on a contract in accordance with Article 10(1)(B); and
  - (B) the Processing is carried out by automated means.

- (2) In exercising the right to data portability under paragraph (1), the Data Subject has the right to have the Personal Data transmitted directly from one Data Controller to another, if technically feasible.
- (3) The exercise of the right referred to in paragraph (1):
  - (A) is without prejudice to the right to erasure in accordance with Article 18; and
  - (B) does not apply to Processing:
    - (i) that is necessary for the performance of a task carried out in the public interest; or
    - (ii) in the exercise of official authority vested in the Data Controller.
- (4) The exercise of the right referred to in paragraph (1) must not adversely affect the rights and legitimate interests of others.

## ARTICLE 22 – AUTOMATED INDIVIDUAL DECISION-MAKING, INCLUDING PROFILING

- (1) A Data Subject has the right not to be subjected to a decision that is based solely on automated Processing, including Profiling, if the decision would have a legal effect on them or would otherwise significantly affect them.
- (2) Paragraph (1) does not apply if:
  - (A) the relevant decision is necessary to enter into or perform a contract between the Data Subject and a Data Controller;
  - (B) the decision is made pursuant to laws or regulations applicable to the Data Controller; or
  - (C) the Data Subject has given their explicit written consent to the decision being based solely on automated Processing.
- (3) In a case referred to in paragraph (2)(A) or (C), the Data Controller must implement suitable measures to safeguard the Data Subject's rights and legitimate interests. The measures must include rights for the Data Subject:
  - (A) to obtain a human intervention by the Data Controller;
  - (B) to express their point of view; and
  - (C) to contest the decision.
- (4) A decision referred to in paragraph (2) must not be based on Sensitive Personal Data unless:
  - (A) the Data Subject concerned has given their explicit written consent to the Processing for one or more specified purposes; or

- (B) the Processing is necessary for substantial public interest reasons, on the basis of applicable laws and regulations, that are proportionate to the aim or aims pursued, respect the principles of data protection and provide for suitable and specific measures to safeguard the rights of the Data Subject.

## PART 4 – TRANSFERS OF DATA OUTSIDE THE QFC

### ARTICLE 23 – TRANSFERS OUT OF THE QFC: ADEQUATE LEVEL OF PROTECTION

- (1) Any Processing of Personal Data which involves the transfer of Personal Data to a Recipient located in a jurisdiction outside the QFC may take place if the Data Protection Office has decided that the jurisdiction has an adequate level of protection.
- (2) For the purposes of the decision required by paragraph (1), the Data Protection Office may take into account factors including:
  - (A) the rule of law, the general respect for individual's rights and the ability of individuals to enforce their rights via administrative or judicial redress;
  - (B) the access of public authorities to Personal Data;
  - (C) the existence of effective data protection law, including rules on the onward transfer of Personal Data to another jurisdiction;
  - (D) the existence and functioning of one or more independent supervisory authorities with adequate enforcement powers; and
  - (E) international commitments and conventions binding on the jurisdiction and its membership of any multilateral or regional organisations.
- (3) The Data Protection Office may make its decision based on adequacy decisions made by other competent data protection authorities where those decisions have taken into account the same factors.
- (4) The Data Protection Office must publish details of its decisions under paragraph (2).
- (5) A jurisdiction may lose adequacy status from time to time. In such circumstances, the Data Protection Office will issue an amended list of jurisdictions.
- (6) Processing of Personal Data that involves the transfer of the Personal Data to a Recipient located in a jurisdiction outside the QFC that the Data Protection Office has decided has an adequate level of protection does not require any specific authorisation or notification to the Data Protection Office.

## ARTICLE 24 – TRANSFERS OUT OF THE QFC IN THE ABSENCE OF AN ADEQUATE LEVEL OF PROTECTION

- (1) A transfer of Personal Data to a Recipient located in a jurisdiction outside the QFC, if that jurisdiction has not been decided to have an adequate level of protection in accordance with Article 23, may take place only if:
  - (A) the Data Controller or Data Processor in question has provided appropriate safeguards including enforceable rights and effective legal remedies for Data Subjects;
  - (B) one of the specific derogations in paragraph (3) applies; or
  - (C) the limited circumstances in paragraph (4) apply.
- (2) The appropriate safeguards referred to in paragraph (1)(A) may be provided by:
  - (A) a legally binding and enforceable arrangement between public authorities or bodies; or
  - (B) a legally binding and enforceable agreement between the parties that includes standard data protection clauses adopted by the Data Protection Office.
- (3) The derogations referred to in paragraph (1)(B) are the following:
  - (A) the Data Subject concerned has been informed of the risks and has given their explicit consent to the transfer of their Personal Data for one or more specific purposes;
  - (B) the 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 at the Data Subject's request;
  - (C) the 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;
  - (D) the transfer is necessary to comply with a legal obligation of the Data Controller or Data Processor;
  - (E) the transfer is necessary to protect the vital interests of the Data Subject or another individual;
  - (F) the transfer is necessary to perform a task carried out:
    - (i) in the public interest; or
    - (ii) by any of the following in the performance of its functions:
      - (a) the QFC Authority;

- (b) the QFC Regulatory Authority;
    - (c) the Civil and Commercial Court;
    - (d) the Regulatory Tribunal;
    - (e) a QFC Institution;
  - (G) the transfer is necessary for the establishment, exercise or defence of a legal claim.
- (4) Where a transfer could not be based on Article 23, or on an appropriate safeguard under paragraph (2) or a derogation under paragraph (3), a transfer to a Recipient located in a jurisdiction outside the QFC where that jurisdiction has not been determined to have an adequate level of protection may take place only if:
- (A) the transfer:
    - (i) is not repeating or not part of a repetitive course of transfers;
    - (ii) concerns only a limited number of Data Subjects;
    - (iii) does not contain any Sensitive Personal Data;
    - (iv) is for the purposes of the legitimate interests of the Data Controller or another entity to which the data is 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); and
    - (v) the Data Controller has completed a documented assessment of the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of Personal Data; or
  - (B) a permit for the transfer has been obtained from the Data Protection Office and the Data Controller applies adequate safeguards with respect to the protection of the Personal Data.
- (5) A Data Controller may appeal against a refusal by the Data Protection Office to issue a permit under paragraph (4)(B) to the Regulatory Tribunal in accordance with Article 33(6).

## PART 5 – DATA CONTROLLER AND DATA PROCESSOR OBLIGATIONS

### ARTICLE 25 – RESPONSIBILITY OF THE DATA CONTROLLER

The Data Controller must implement appropriate and effective technical and organisational measures to ensure, and to be able to demonstrate, that Processing is performed in accordance with these Regulations. Those measures must be reviewed and updated where necessary.

### ARTICLE 26 – DATA PROTECTION BY DESIGN AND BY DEFAULT

- (1) A Data Controller must, both at the time of the determination of the means for Processing and at the time of the Processing itself, implement appropriate technical and organisational measures to:
  - (A) integrate the necessary safeguards into the Processing to meet the requirements of these Regulations;
  - (B) implement the data protection principles in Article 8; and
  - (C) protect Personal Data against:
    - (i) accidental or unlawful destruction, accidental loss, alteration, unauthorised disclosure or access; and
    - (ii) all other unlawful forms of Processing.
- (2) A Data Controller must implement appropriate technical and organisational measures to ensure that, by default, only Personal Data that are necessary for each specific purpose are Processed. The measures must ensure that, by default, Personal Data:
  - (A) are not made accessible (without the Data Subject's intervention) to an indefinite number of Recipients; and
  - (B) are made accessible only to individuals who, for their role, function or task, need to Process those Personal Data.

### ARTICLE 27 – DATA PROTECTION IMPACT ASSESSMENT

- (1) If a type of Processing is likely to result in a high risk to the rights and legitimate interests of Data Subjects, a Data Controller must, before Processing, carry out an assessment of the impact that the envisaged Processing will have on the protection of Personal Data.
- (2) A data protection impact assessment is required in particular if:
  - (A) there is automated Processing, including Profiling, which leads to decisions that have a legal effect or would otherwise significantly affect the Data Subject;
  - (B) Processing of Sensitive Personal Data is on a large scale; or

there is systematic monitoring of a publicly accessible area on a large scale. At a minimum, the assessment must contain the information set out in the Data Protection Rules.

- (3) The Data Protection Office may establish and make public a non-exhaustive list of the Processing operations which require a data protection impact assessment.
- (4) A single assessment may address a set of similar Processing operations that present similar risks.
- (5) The Data Controller must carry out a review to assess whether the Processing was performed in accordance with the relevant data protection impact assessment. In particular, the Data Controller must do so when there is a change of the risk represented by Processing operations.

## ARTICLE 28 – DATA PROCESSORS

- (1) If Personal Data is to be Processed on behalf of a Data Controller, the Data Controller must engage only a Data Processor that provides sufficient guarantees:
  - (A) to implement technical and organisational measures to comply with these Regulations; and
  - (B) to ensure that Data Subjects' rights are protected.
- (2) The Data Processor must not engage another Data Processor without the Data Controller's prior written authorisation.
- (3) The Data Controller and the Data Processor must enter into a written contract that sets out, at a minimum, the information contained in the Data Protection Rules. The Data Protection Office may require firms to include certain standard contractual clauses in those contracts.
- (4) A Data Processor, and any other person, must not Process Personal Data except:
  - (A) on written instructions from the Data Controller;
  - (B) if they are required to do so by applicable laws or regulations; or
  - (C) if directed to do so by the Data Protection Office.
- (5) If a Data Processor is obliged by laws or regulations to Process Personal Data otherwise than on written instructions from the Data Controller, the Data Processor must inform the Data Controller of that obligation before Processing the data.
- (6) The Data Processor must immediately inform the Data Controller if, in their opinion, an instruction contravenes these Regulations or any other applicable legal requirement.

- (7) If the Data Processor engages another Data Processor to carry out Processing on behalf of the Data Controller, the obligations between the Data Controller and the Data Processor referred to in paragraph (3) to (5) must be imposed on that other Data Processor by a written contract.
- (8) If that other Data Processor fails to fulfil those obligations, the initial Data Processor remains liable to the Data Controller for the performance of those obligations.
- (9) If a Data Processor determines the purposes and means of Processing Personal Data, the Data Processor is taken to be a Data Controller in relation to that Processing.

## ARTICLE 29 – SECURITY OF PROCESSING

- (1) A Data Controller and a Data Processor must implement technical and organisational measures to ensure an appropriate level of security in the Processing of Personal Data, including but not limited to:
  - (A) the De-identification or encryption (or both) of the Personal Data;
  - (B) the ability to ensure the continuing confidentiality, integrity, availability and resilience of Processing systems and services;
  - (C) the ability to restore the availability of and access to the Personal Data in a timely manner in the event of a physical or technical incident;
  - (D) a process for regularly testing, assessing and evaluating the effectiveness of the measures.
- (2) In deciding what measures are appropriate, the Data Controller and the Data Processor may take into account:
  - (A) the available technology;
  - (B) the costs of implementation;
  - (C) the nature, scope, context and purposes of the Processing; and
  - (D) the likelihood and severity of risks to the rights and legitimate interests of individuals.
- (3) In assessing the appropriate level of security, the Data Controller and the Data Processor may take into account the risks that are presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, the Personal Data.
- (4) The measures outlined in paragraphs (1) and (2) must include the implementation of appropriate data protection policies.

## ARTICLE 30 – RECORD OF PROCESSING OPERATIONS

- (1) A Data Controller must make and retain a written record of all Processing of Personal Data under its responsibility. The record must contain all of the information outlined in the Data Protection Rules.
- (2) Each Data Processor engaged in a specific Processing activity must maintain a record containing the information specified in the Data Protection Rules with respect to the Processing activity carried out on behalf of a Data Controller.
- (3) The records referred to in paragraphs (1) and (2) must be in writing, including in electronic form.
- (4) The Data Controller or the Data Processor must make the record available to the Data Protection Office on request.

## ARTICLE 31 – NOTIFICATION OF PERSONAL DATA BREACHES

- (1) In case of a Personal Data Breach, the Data Controller must notify the Personal Data Breach to the Data Protection Office without undue delay and, where feasible, not later than 72 hours after having become aware of it.
- (2) The obligation in paragraph (1) does not apply where the Data Controller has determined that the Personal Data Breach is unlikely to result in a risk to the rights and legitimate interests of Data Subjects.
- (3) The notification required by paragraph (1) must at least contain the information set out in the Data Protection Rules.
- (4) If it is not possible to provide all the information at the same time, the information may be provided in phases without undue further delay.
- (5) The Data Controller must document any Personal Data Breaches, including the facts relating to the Personal Data Breach, its effects and the remedial action taken to enable the Data Protection Office to verify compliance with this Article.
- (6) The Data Controller must consider notifying any Personal Data Breaches to affected Data Subjects, taking into account the risk to their rights and legitimate interests. If a notification is given it must use clear and plain language and must contain at least:
  - (A) the nature of the Personal Data Breach;
  - (B) the likely consequences of the Personal Data Breach; and
  - (C) a description of the measures taken or proposed to be taken by the Data Controller to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.
- (7) A Data Processor must notify the Data Controller concerned without undue delay after becoming aware of a Personal Data Breach.

## PART 6 – THE DATA PROTECTION OFFICE

### ARTICLE 32 – ESTABLISHMENT OF THE DATA PROTECTION OFFICE AND THE DATA PROTECTION COMMISSIONER

- (1) A Data Protection Office is established by the QFC Authority in accordance with Article 6 of the QFC Law.
- (2) The Data Protection Office administers these Regulations and all aspects of data protection within the QFC.
- (3) The Data Protection Office is to be managed by the Data Protection Commissioner who will determine its procedures and management.
- (4) The Data Protection Office shall be subject to the supervision of the QFC Authority which shall have the power and function to:
  - (A) ensure that the Data Protection Office exercises its statutory powers and performs its statutory functions;
  - (B) ensure that the Data Protection Office uses its resources in accordance with its objectives; and
  - (C) give the Data Protection Office written directions as to the furtherance of any of its objectives or the performance of its functions.
- (5) The QFC Authority may make rules to enable it, the Data Protection Commissioner and the Data Protection Office to implement, carry out or enforce their duties, functions and powers including the powers to ensure rights and legitimate interests are protected in the Processing of Personal Data.
- (6) In exercising its powers and performing its functions the Data Protection Office will be independent of any other person or body whose interests could conflict with the functions of the office.

### ARTICLE 33 – POWERS

- (1) The Data Protection Office has the following investigative powers:
  - (A) to order a Data Controller or a Data Processor to provide any information that the Data Protection Office requires for the performance of its duties;
  - (B) to carry out investigations, including data protection audits, on its own initiative or based on information received from third parties;
  - (C) to notify a Data Controller or Data Processor of an alleged infringement of these Regulations;
  - (D) to obtain access to any premises of a Data Controller or Data Processor, including to any data Processing equipment and means.

- (2) The Data Protection Office has the following corrective powers:
- (A) to warn a Data Controller or Data Processor that intended Processing operations are likely to infringe these Regulations;
  - (B) to issue reprimands or orders to rectify any infringements to a Data Controller or a Data Processor;
  - (C) to order a Data Controller or Data Processor to comply with the Data Subject's requests to exercise the Data Subject's rights under these Regulations;
  - (D) to order a Data Controller or Data Processor to carry out Processing operations in a specified manner and within a specified period;
  - (E) to order a Data Controller to notify a Data Subject of a Personal Data Breach;
  - (F) to impose a temporary or permanent limitation, including a ban, on the Processing of Personal Data;
  - (G) to order a Data Controller to rectify or erase Personal Data and to notify these actions to Recipients to whom the Personal Data have been disclosed;
  - (H) to impose a penalty in accordance with Article 36, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;
  - (I) to order the suspension of data transfers to a Recipient outside the QFC or to an international organisation;
  - (J) to order a Data Controller to undertake a data protection impact assessment.
- (3) The Data Protection Office has the following authorisation and advisory powers, subject to the approval of the QFCA:
- (A) to issue, on its own initiative or on request, opinions, interpretations, guidance, and training on any issue related to these Regulations;
  - (B) to publish a list of adequate jurisdictions for data transfers in accordance with Article 23;
  - (C) to grant permits for the Processing of Sensitive Personal Data, and for transfers of Personal Data.
- (4) If the Data Protection Office considers that a Data Controller or Data Processor has failed to comply with a determination, decision or order of the Data

Protection Office, the Data Protection Office may apply to the Civil and Commercial Court for one or more of the following orders:

- (A) an order directing the Data Controller or Data Processor to comply with the determination, decision or order or any provision of these Regulations;
  - (B) an order directing the Data Controller or Data Processor to pay any costs incurred by the Data Protection Office or other person relating to the issue of the direction by the Data Protection Office, and any subsequent action.
- (5) The Data Protection Office may rely on Part 5 Compliance and Enforcement Rules of the QFCA Rules (the "CER Rules") to enforce these Regulations.
- (6) Any determination, decision or order made by the Data Protection Office, under these Regulations or the Data Protection Rules may be appealed to the Regulatory Tribunal in accordance with QFC Law.

## PART 7 – REMEDIES

### ARTICLE 34 – RIGHT TO LODGE A COMPLAINT WITH THE DATA PROTECTION OFFICE

- (1) Every Data Subject, body, organisation or association has the right to lodge a complaint with the Data Protection Office in relation to an alleged infringement of these Regulations.
- (2) A complaint must be in writing and must contain any information required for the purpose in the Data Protection Rules.
- (3) The Data Protection Office must investigate the complaint and must keep the complainant informed on the progress and the outcome of the complaint, including the possibility of a judicial remedy in accordance with the QFC Law.
- (4) If the Data Protection Office is satisfied that these Regulations have been infringed, it may make a determination to that effect. The making of such a determination does not affect the Data Protection Office's exercise of any of its other powers.
- (5) If the Data Protection Office is satisfied that a complaint alleging an infringement of these Regulations is not substantiated, it may dismiss the complaint.
- (6) The Data Protection Office may refuse to accept, review or investigate a complaint or may suspend or postpone any such activity if:
  - (A) the Data Protection Office determines that these Regulations do not apply to the complaint;
  - (B) there is not enough evidence to prove the complaint;
  - (C) the Data Protection Office, the Civil and Commercial Court, or the Regulatory Tribunal has previously made a decision relating to the subject matter of the complaint;
  - (D) the complainant has not taken the steps required by the Data Protection Office to facilitate the handling, resolution or investigation of the complaint;
  - (E) the dispute that caused the complaint is resolved; or
  - (F) the complaint is frivolous, vexatious, trivial or is not made in good faith.
- (7) The Data Protection Office must facilitate the submission of complaints referred to in paragraph (1) by any means of communication.
- (8) Where the complaint or the request is manifestly unfounded or excessive, in particular because of its repetitive character, the Data Protection Office may charge a reasonable fee based on administrative costs. The Data Protection

Office bears the burden of demonstrating that a complaint or request is manifestly unfounded or excessive.

- (9) This Article does not exclude any other administrative or judicial remedy for an alleged infringement of these Regulations.

## ARTICLE 35 – RIGHT TO COMPENSATION AND LIABILITY

- (1) Any person who has suffered material or non-material damage due to an infringement of these Regulations has the right to receive compensation from the Data Controller or Data Processor responsible for the damage suffered.
- (2) A Data Controller involved in Processing is liable for any damage caused by Processing which infringes these Regulations. A Data Processor is liable for the damage caused by Processing only where it has not complied with obligations under these Regulations specifically directed to Data Processors or where it has not acted in accordance with the lawful instructions of a Data Controller.
- (3) A Data Controller or Data Processor is exempt from liability under paragraph (2) if it can establish that it is not in any way responsible for the event giving rise to the damage.
- (4) Where more than one Data Controller or Data Processor, or both a Data Controller and a Data Processor, are involved in the same Processing and where they are, under paragraphs (2) and (3), responsible for any damage caused by Processing, each Data Controller or Data Processor is jointly and severally liable for the entire damage.
- (5) Where a Data Controller or Data Processor has, in accordance with paragraph (4), paid full compensation for the damage suffered, that Data Controller or Data Processor is entitled to claim back from the other Data Controllers or Data Processors involved in the same Processing that part of the compensation corresponding to their part of responsibility for the damage, but subject to paragraph (2).

## ARTICLE 36 – GENERAL CONDITIONS FOR IMPOSING PENALTIES

- (1) The Data Protection Office must ensure that penalties for infringements of these Regulations or non-compliance with an order of the Data Protection Office are, in each individual case, effective, proportionate and dissuasive.
- (2) Depending on the circumstances of each individual case, penalties may be imposed in addition to, or instead of, measures referred to in Article 33(2)(A), (B), (C), (D), (E), (F), (G), (I), and (J). When deciding whether to impose a penalty and when deciding on the amount of the penalty in each individual case, due regard must be given to the following:
  - (A) the nature, gravity and duration of the infringement, considering:
    - (i) the nature, scope or purpose of the Processing concerned;

- (ii) the number of Data Subjects affected; and
    - (iii) the level of damage suffered by them;
  - (B) the intentional or negligent character of the infringement;
  - (C) any action taken by the Data Controller or Data Processor to mitigate the damage suffered by Data Subjects;
  - (D) the degree of responsibility of the Data Controller or Data Processor taking into account technical and organisational measures implemented by them;
  - (E) any relevant previous infringements by the Data Controller or Data Processor;
  - (F) the degree of cooperation by the Data Controller or Data Processor with the Data Protection Office, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;
  - (G) the categories of Personal Data affected by the infringement;
  - (H) the way the infringement became known to the Data Protection Office, and in particular whether, and if so to what extent, the Data Controller or Data Processor notified the Data Protection Office of the infringement;
  - (I) if the Data Protection Office has previously made orders against the Data Controller or Data Processor concerned with regard to the same subject matter, the extent of compliance with those measures;
  - (J) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.
- (3) Infringements of any provision of these Regulations or non-compliance with an order by the Data Protection Office will be subject to a maximum penalty of \$1,500,000.00 USD.

## PART 8 – FINAL PROVISIONS

### ARTICLE 37 – GENERAL EXEMPTIONS

- (1) These Regulations do not apply to natural persons in the course of their purely personal or household activities.
- (2) Articles 14, 15, 16, 17, 18, 19, 20, 21, 22, 23 and 24 do not apply to:
  - (A) the QFC Authority, the QFC Regulatory Authority, or a QFC Institution, in their capacity as a Data Controller, only to the extent that compliance with those Articles would be likely to prejudice the proper discharge of their powers and functions;
  - (B) the Civil and Commercial Court and the Regulatory Tribunal; or
  - (C) an individual acting in a judicial or quasi-judicial capacity:
    - (i) for the purposes of assessing a person’s suitability for judicial office; or
    - (ii) where the application of those provisions would be likely to prejudice their judicial independence or judicial proceedings.

### ARTICLE 38 – INTERPRETATION

- (1) In these Regulations, a reference to:
  - (A) a provision of any law or regulation includes a reference to that provision as amended or re-enacted from time to time;
  - (B) an obligation to publish a particular document, or cause a particular document to be published includes publishing or causing it to be published in printed or electronic form, unless expressly provided otherwise;
  - (C) a calendar year means a year of the Gregorian calendar;
  - (D) a month means a month of the Gregorian calendar;
  - (E) a day means a day of the Gregorian calendar;
  - (F) the masculine gender includes the feminine and the neuter;
  - (G) writing includes any form of representing or reproducing words in legible form; and
  - (H) references to a “Person” include any natural or legal person, Body Corporate or body unincorporate, including a branch, company, partnership, unincorporated association, government or state.
- (2) The heading of an Article in these Regulations is for ease of reference only and does not affect the interpretation of the Article.

- (3) A reference in these Regulations to a Part or Article by number only, without further identification, is a reference to a Part or Article of that number in these Regulations.
- (4) A reference in a provision of these Regulations to a paragraph, sub-paragraph or Article by number or letter only, and without further identification, is a reference to the paragraph, sub-paragraph or Article of that number or letter contained in the provision in which that reference occurs.

## ARTICLE 39 – DEFINITIONS

The following words and phrases have the meanings shown against each of them:

<b>Body Corporate</b>	has the meaning set out in the Companies Regulations 2005.
<b>Child</b>	an individual who is under the age of 18 years.
<b>Civil and Commercial Court</b>	the Civil and Commercial Court of the QFC established under Article 8 of the QFC Law.
<b>Data Controller</b>	an individual or entity that determines the purposes and means of the Processing of Personal Data.
<b>Data Processor</b>	an individual or entity that undertakes the Processing of Personal Data on behalf of a Data Controller.
<b>Data Protection Commissioner</b>	the individual appointed in accordance with Article 32 who determines the procedures and management of the Data Protection Office.
<b>Data Protection Office</b>	the QFC Institution established by Article 32.
<b>Data Subject</b>	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.

<b>De-identification</b>	the Processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific Data Subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the Personal Data are not attributed to an identified or identifiable natural person.
<b>Filing System</b>	any structured set of Personal Data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.
<b>Minister</b>	the Minister as defined in the QFC Law.
<b>Permitted Activity</b>	The activities listed in Schedule 3 or designated by the Council of Ministers under Article 10(1) of the QFC Law.
<b>Personal Data</b>	any information relating to a Data Subject.
<b>Personal Data Breach</b>	any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.
<b>Processing</b>	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.
<b>QFC</b>	The Qatar Financial Centre.
<b>QFC Authority or QFCA</b>	the Qatar Financial Centre Authority established under Article 3 of the QFC Law.
<b>QFC Institution</b>	an institution established pursuant to Article 6 of the QFC Law.
<b>QFC Law</b>	Law No. (7) of 2005 of the State of Qatar.

<b>Recipient</b>	any person, or a legal person, public authority, agency or other body, whether a third party or not, to whom Personal Data, including Sensitive Personal Data, are disclosed.
<b>Regulations</b>	Regulations enacted by the Minister in accordance with Article 9 of the QFC Law.
<b>Regulatory Authority</b>	the Regulatory Authority of the QFC established under Article 8 of the QFC Law.
<b>Rules</b>	Rules made by the QFC Authority in accordance with the QFC Law, these Regulations or any other Regulation under which the QFC Authority has power to make rules, including, where the context permits, standards, principles and codes of practice.
<b>Sensitive Personal Data</b>	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.
<b>State</b>	the State of Qatar.
<b>Regulatory Tribunal</b>	the Qatar Financial Centre Regulatory Tribunal, established under Article 8 of the QFC Law.