QFC DATA PROTECTION RULES

VERSION 2 – DECEMBER 2021

مـــركـــز قـــطـر لـلـــمـال
QATAR FINANCIAL CENTRE

CONTENTS

1. INTRODUCTION

If a provision in the Data Protection Rules refers to a communication, notice, agreement or other document 'in writing' then, unless the contrary intention appears, it means in legible form and capable of being reproduced on paper, irrespective of the medium used. Expressions related to writing must be interpreted accordingly.

In these Rules:

(A) the Regulations means the Data Protection Regulations 2021;

(B) defined terms are identified by the capitalisation of the initial letter of the word; and

(C) defined terms have the same meaning as they have in the Data Protection Regulations.

2. PERMIT FOR PROCESSING SENSITIVE PERSONAL DATA

APPLICATION FOR A PERMIT

For the purposes of Article 12 of the Regulations, a Data Controller seeking a permit from the Data Protection Office to Process Sensitive Personal Data must apply in writing to the Data Protection Office setting out:

(A) the identity and contact details of the Data Controller;

(B) the name, address, telephone number and e-mail address of the Person within the Data Controller responsible for making the application for the permit;

(C) a description of the Processing of Sensitive Personal Data for which the permit is being sought, including a description of the nature of the Sensitive Personal Data involved;

(D) the purpose of the proposed Processing of the Sensitive Personal Data;

(E) the classes of Data Subjects being affected;

(F) the identity of any Person to whom the Data Controller intends disclosing the Sensitive Personal Data;

(G) to which jurisdictions, if known, such Sensitive Personal Data may be transferred outside of the QFC; and

(H) a description of the safeguards put into place by the Data Controller, to ensure the security of the Sensitive Personal Data.

The Data Controller must provide the Data Protection Office with such further information as it requires to determine whether to grant a permit.

Rejection of an application for a permit

The Data Protection Office may refuse to grant a permit to Process Sensitive Personal Data.

Upon refusing to grant a permit, the Data Protection Office will inform the Data Controller in writing of such refusal and provide the reasons for such refusal.

Granting a permit to Process Sensitive Personal Data

The Data Protection Office may grant a permit to Process Sensitive Personal Data without conditions or with such conditions as it considers necessary.

Upon deciding to grant a permit, the Data Protection Office will inform the Data Controller of the decision and any conditions applicable to the permit.

3. INFORMATION TO BE PROVIDED TO DATA SUBJECTS

For the purposes of Articles 14 and 15 of the Regulations, a Data Controller must provide a Data Subject with the following information:

(A) the identity and contact details of the Data Controller;

(B) the purposes of the intended Processing and the lawful basis for that Processing, as set out in Article 10 of the Regulations;

(C) whether the Data Subject is obliged to provide the Personal Data and the possible consequences of failing to do so;

(D) the categories of Personal Data concerned;

(E) if the data are to be, or may be, disclosed to one or more other individuals or entities, their names or a description of their categories;

(F) if the Data Controller intends to transfer the data to another jurisdiction, a statement of that fact, setting out a description of the applicable safeguards and, if applicable, how and where to obtain a copy of the safeguards;

(G) if the Processing is based on the legitimate interests of the Data Controller or another Person to whom the data are disclosed or to comply with an obligation imposed on the Data Controller by law, a clear statement of those interests or obligations;

(H) the period for which the data will be retained, or how to determine that period;

(I) a statement of the Data Subject's right to request from the Data Controller:

  (i) access to the data;

  (ii) rectification of the data;

  (iii) erasure of the data;

  (iv) restriction of the Processing of the data;

  (v) objection to the Processing of the data; and

  (vi) data portability.

(J) whether automated decision-making will be used, and if so:

  (i) meaningful information about the logic applied; and

  (ii) the significance, and the likely consequences, of the decision-making for the Data Subject.

(K) if the Processing is based on consent, that the Data Subject has the right to withdraw that consent at any time, but that withdrawing the consent does not affect the lawfulness of Processing based on consent before the withdrawal; and

(L) that under Article 34 of the Regulations, the Data Subject has the right to lodge a complaint with the Data Protection Office if the Data Subject considers that the Processing of Personal Data relating to them infringes the Regulations.

4. REQUESTS MADE UNDER PART 3 OF THE REGULATIONS – DATA SUBJECT RIGHTS

For the purposes of Article 16 of the Regulations, a Data Subject has the right to obtain, from a Data Controller, a statement that includes the following information:

(A) the lawful basis, as set out in Article 10 of the Regulations, and purposes of the Processing;

(B) the categories of Personal Data concerned;

(C) the Recipients, or categories of Recipient, to which the Personal Data have been or will be disclosed (in particular, Recipients outside the QFC);

(D) the period for which the Data Controller intends to retain the Personal Data, or the criteria used to determine that period;

(E) a statement of the Data Subject's rights to request from the Data Controller:

(i) rectification of the data;

(ii) erasure of the data;

(iii) restriction of the Processing of the data;

(iv) objection to the Processing of the data; and

(v) data portability.

(F) a statement of the Data Subject's right under Article 34 of the Regulations to lodge a complaint with the Data Protection Office if they consider that the Processing of Personal Data relating to them infringes the Regulations;

(G) if the Personal Data were collected otherwise than from the Data Subject, any available information about their source;

(H) whether automated decision-making will be used, and if so:

(i) meaningful information about the logic applied; and

(ii) the significance, and the likely consequences, of the decision-making for the Data Subject.

The Data Controller must communicate any action carried out in accordance with Article 17 or Article 18 of the Regulations to each Recipient to whom the Personal Data have been disclosed, unless doing so would be impossible or would involve disproportionate effort. The Data Controller must inform the Data Subject about those Recipients if the Data Subject requests it.

5. TRANSFERS OF PERSONAL DATA OUT OF THE QFC

APPLICATION FOR PERMIT

For the purposes of Article 24 of the Regulations, a Data Controller who seeks a permit from the Data Protection Office to transfer Personal Data to a Recipient which is not subject to laws and regulations which ensure an adequate level of protection must apply in writing to the Data Protection Office setting out:

(A) the identity and contact details of the Data Controller;

(B) the name and contact details of the Person within the Data Controller responsible for making the application for the permit;

(C) a description of the proposed transfer of Personal Data for which the permit is being sought, including a description of the nature of the Personal Data involved;

(D) the purpose of the proposed transfer of Personal Data;

(E) the classes of Data Subjects being affected;

(F) the identity of the proposed Recipient of the Personal Data;

(G) the jurisdiction of the proposed Recipient and a description of the laws and regulations which apply to the proposed Recipient in respect of Personal Data protection; and

(H) a description of the safeguards to be put into place by the Data Controller, to ensure the security of the Personal Data should the relevant transfer take place.

The Data Controller must provide the Data Protection Office with any further information that the Data Protection Office requires to determine whether to grant a permit.

Rejection of an application for a permit

The Data Protection Office may refuse to grant a permit to transfer Personal Data.

Upon refusing to grant a permit, the Data Protection Office will inform the Data Controller in writing of the refusal and provide the reasons for the refusal.

Granting a permit to transfer Personal Data

The Data Protection Office may grant a permit to transfer Personal Data without conditions or with such conditions as it considers necessary.

Upon deciding to grant a permit, the Data Protection Office will inform the Data Controller of the decision and any conditions applicable to the permit.

6. DATA PROTECTION IMPACT ASSESSMENTS

For the purposes of Article 27 of the Data Protection Regulations, a data protection impact assessment must contain at least:

(A) a systematic description of the envisaged Processing operations and the purposes of the Processing, including:

(i) identification and consideration of the lawful basis for the Processing as set out in Article 10 of the Regulations;

(ii) if the Processing is necessary for the purposes of the legitimate interests of the Data Controller or another Person in accordance with Article 10(1)(F) of the Regulations, the reasoning according to which the Data Controller believes that the rights or legitimate interests of the Data Subject do not override its interests or those of the other Person; and

(iii) if Processing is based on consent:

(a) confirmation that consent will be or has been validly obtained;

(b) the impact of the withdrawal of consent to that Processing; and

(c) how the Data Controller will ensure that it can comply with any exercise by the Data Subject of their right to withdraw consent;

(B) an assessment as to how the Processing operations are adequate, relevant and limited to what is necessary in relation to the purposes for which the Personal Data are Processed;

(C) an assessment of the risks to the rights and legitimate interests of Data Subjects; and

(D) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data and to demonstrate compliance with the Regulations, taking into account the rights and legitimate interests of Data Subjects and other persons concerned.

7. CONTRACTS BETWEEN DATA CONTROLLERS AND DATA PROCESSORS

For the purposes of Article 28 of the Regulations, a contract between a Data Controller and a Data Processor must set out, at a minimum:

(A) the subject matter and duration of the Processing;

(B) the nature and purpose of the Processing;

(C) the type of Personal Data and categories of Data Subjects; and

(D) the obligations and rights of the Data Controller.

The contract must also set out that the Data Processor:

(E) must not Process the Personal Data, or transfer it outside the QFC, unless instructed in writing by the Data Controller, or required by law to do so;

(F) must ensure that persons authorised to Process the data have undertaken to maintain its confidentiality or are under an appropriate statutory obligation of confidentiality;

(G) must take all the measures required by Article 29 of the Regulations;

(H) must comply with the conditions referred to in Article 28(2) and (6) of the Regulations for engaging another Data Processor;

(I) taking into account the nature of the Processing, must assist the Data Controller to fulfil the Data Controller's obligation to respond to requests by Data Subjects to exercise their rights, by implementing appropriate technical and organisational measures;

(J) must assist the Data Controller to comply with the Data Controller's obligations under Articles 27, 29 and 31 of the Regulations, taking into account the nature of the Processing and the information available to the Data Processor;

(K) after completing the services relating to Processing, must delete all the Personal Data or return it to the Data Controller (at the Data Controller's choice), and must delete any copy unless an applicable law requires it to be retained;

(L) must make available to the Data Controller all information necessary to show that the Data Processor has complied with the obligations laid down in the Regulations; and

(M) must allow for, and assist with, audits and inspections by the Data Controller or an auditor appointed by the Data Controller.

8. RECORDS OF PROCESSING

For the purposes of Article 30 of the Regulations, a Data Controller and Data Processor must record the following information in relation to a Data Processing operation:

(A) the identity and contact details of the Data Controller;

(B) the purposes of the Processing;

(C) the lawful basis, as set out in Article 10 of the Regulations, for the Processing;

(D) descriptions of the categories of Data Subjects and the categories of Personal Data;

(E) the categories of Recipients to whom the Personal Data have been or will be disclosed;

(F) if applicable, transfers of Personal Data to a jurisdiction outside the QFC or to another Person, including the details of the jurisdiction or the other Person and, in the case of a transfer referred to in Article 24 of the Regulations, the documentation of suitable safeguards;

(G) the envisaged time limits for retention of the different categories of Personal Data;

(H) a general description of the technical and organisational measures referred to in Article 29(1) of the Regulations.

9. NOTIFICATION OF PERSONAL DATA BREACHES

For the purposes of Article 31 of the Regulations, the notification of a Personal Data Breach must at least:

(A) describe the nature of the Personal Data Breach including:

(i) the categories of Data Subjects affected;

(ii) the approximate number of Data Subjects affected;

(iii) the categories and approximate number of Personal Data records affected;

(B) give the name and contact details of a person from whom more information can be obtained;

(C) describe the likely consequences of the Personal Data Breach;

(D) describe the measures that the Data Controller has taken or proposes to take to address the consequences of the Personal Data Breach, including, if appropriate, measures to mitigate its possible adverse effects;

(E) if the notification is not made within 72 hours after becoming aware of the Personal Data Breach, give reasons for the delay.

10. LODGING A COMPLAINT WITH THE DATA PROTECTION OFFICE

For the purposes of Article 34 of the Regulations, a Data Subject (the complainant) who makes a complaint to the Data Protection Office must give the following information in the complaint:

(A) the complainant's full name and address;

(B) the full name and address of the Data Controller whom the complainant believes has contravened the Regulations;

(C) a detailed statement of facts that the complainant believes gives rise to the relevant contravention of the Regulations;

(D) a statement of the relief that the complainant seeks;

(E) a declaration by the complainant that they have provided the Data Protection Office with accurate information and that they understand that any information provided will be Processed by the Data Protection Office in accordance with Article 34 of the Regulations.