



DATA PROTECTION RULES

VER 1 – OCT 2005



CONTENTS

1. INTRODUCTION	3
1.1 Application	3
1.2 Interpretation	3
2. PERMIT FOR PROCESSING SENSITIVE PERSONAL DATA	4
2.1 Application for a permit.....	4
3. PERMIT FOR TRANSFER OUT OF THE QFC OF PERSONAL DATA	6
3.1 Assessing adequate levels of protection.....	6
3.2 Application for permit.....	7
4. RECORDS AND NOTIFICATIONS	9
4.1 Records	9
4.2 Notifications.....	10
5. CLAIMS	12
5.1 Process of lodging a claim	12

1. INTRODUCTION

1.1 APPLICATION

- 1.1.1 The *Data Protection Rules* apply to every *Person* to whom the *Data Protection Regulations 2005* apply and to the same extent in relation to every such *Person* as the *Data Protection Regulations*, except to the extent that a provision of these *Rules* provides for a narrower application.

1.2 INTERPRETATION

- 1.2.1 (1) 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.
- (2) This does not affect any other legal requirements which may apply in relation to the form or manner of executing a document or agreement.
- 1.2.1 In these *Rules*:
- (A) defined terms are identified by the capitalisation of the initial letter of the word or phrase and are in italics; and
- (B) defined terms have the same meaning as they have in the *Data Protection Regulations*.

2. PERMIT FOR PROCESSING SENSITIVE PERSONAL DATA

2.1 APPLICATION FOR A PERMIT

2.1.1 A *Data Controller* which seeks a permit from the *QFC Authority* to *Process Sensitive Personal Data* pursuant to Article 8(2) of the *Data Protection Regulations* must apply in writing to the *QFC Authority* setting out:

- (A) the name of the *Data Controller*;
- (B) the address of the *Data Controller*;
- (C) the name, address, telephone number and e-mail address of the *Person* within the *Data Controller* responsible for making the application for the permit;
- (D) 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;
- (E) the purpose of the *Processing of the Sensitive Personal Data*;
- (F) the identity of the *Data Subjects* to whom the relevant *Sensitive Personal Data* relates, or in the event of classes of *Data Subjects* being affected, a description of the class of *Data Subjects*;
- (G) the identity of any *Person* to whom the *Data Controller* intends disclosing the *Sensitive Personal Data*;
- (H) to which jurisdictions, if known, such *Sensitive Personal Data* must be transferred outside of the *QFC*; and
- (I) a description of the safeguards put into place by the *Data Controller*, to ensure the security of the *Sensitive Personal Data*.

2.1.2 The *Data Controller* must provide the *QFC Authority* with such further information as may be required by the *QFC Authority* in order to determine whether to grant a permit in accordance with Article 8(2) of the *Data Protection Regulations*.

Rejection of an application for a permit

2.1.3 (1) The *QFC Authority* may refuse to grant an application for a permit to *Process Sensitive Personal Data*.

- (2) Upon refusing to grant a permit, the *QFC Authority* will without undue delay inform the *Data Controller* in writing of such refusal and provide the reasons for such refusal.

Granting a permit to process sensitive personal data

- 2.1.4 (1) The *QFC Authority* may grant an application for a permit to process *Sensitive Personal Data* with or without such conditions as it considers necessary.
- (2) Upon deciding to grant a permit, the *QFC Authority* will without undue delay inform the *Data Controller* of such decision and any conditions.

3. PERMIT FOR TRANSFER OUT OF THE QFC OF PERSONAL DATA

3.1 ASSESSING ADEQUATE LEVELS OF PROTECTION

Guidance

- (1) Article 9 of the *Data Protection Regulations* states:

Transfers to jurisdictions with adequate levels of protection

- (1) Subject to Article 10, a Data Controller may only transfer Personal Data to a Recipient located in a jurisdiction outside the QFC if an adequate level of protection for that Personal Data is ensured by laws and regulations that are applicable to the Recipient.
- (2) The adequacy of the level of protection ensured by laws and regulations to which the Recipient is subject as referred to in Article 9(1) shall be assessed in the light of all the circumstances surrounding a Personal Data transfer operation or set of Personal Data transfer operations, including, but not limited to:
- (A) the nature of the data;
 - (B) the purpose and duration of the proposed Processing operation or operations;
 - (C) if the data does not emanate from the QFC, the country of origin and country of final destination of the personal data; and
 - (D) any relevant laws to which the recipient is subject.
- (2) The *Regulatory Authority* expects *Data Controllers* to adopt a consistent approach when assessing the adequacy of levels of protection for *Personal Data* in other jurisdictions.
- (3) *Data Controllers* should consider not just the extent to which data protection standards have been adopted but also at whether there is a means for ensuring that standards are applied in practice and whether there is an effective mechanism for individuals to enforce their rights or obtain redress if the standards are not met.
- (4) In addition to the circumstances provided in Article 9(2) of the *Data Protection Regulations*, the *Data Controller* should also consider:
- (a) the law in force in the jurisdiction in question regarding data protection;

- (b) international obligations to which the recipient is subject;
- (c) any relevant codes of conduct or other rules which are enforceable in that jurisdiction;
- (d) any security measures taken in respect of the data in that jurisdiction; and
- (e) 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).

3.2 APPLICATION FOR PERMIT

3.2.1 A *Data Controller* who seeks a permit from the *QFC Authority* pursuant to Article 10(1)(A) of the *Data Protection Regulations* for transferring *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 *QFC Authority* setting out:

- (A) the name of the *Data Controller*;
- (B) the address of the *Data Controller*;
- (C) the name, address, telephone number, fax number and e-mail address of the *Person* within the *Data Controller* responsible for making the application for the permit;
- (D) 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;
- (E) the purpose of the proposed transfer of *Personal Data*;
- (F) the identity of the *Data Subjects* to whom the relevant *Personal Data* relates, or in the event of classes of *Data Subjects* being affected, a description of the class of *Data Subjects*;
- (G) the identity of the proposed *Recipient* of the *Personal Data*;
- (H) 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
- (I) a description of the safeguards put into place by the *Data Controller*, to ensure the security of the *Personal Data* should the relevant transfer take place.

3.2.2 The *Data Controller* must provide the *QFC Authority* with such further information as is required the *QFC Authority* in writing in

order to determine whether to grant a permit in accordance with Article 10(1)(A) of the *Data Protection Regulations*.

Rejection of an application for a permit

3.2.3 (1) The *QFC Authority* may refuse to grant an application for a permit to transfer *Personal Data*.

(2) Upon refusing to grant a permit, the *QFC Authority* will without undue delay inform the *Data Controller* in writing of such refusal and provide the reasons for such refusal.

Granting a permit to transfer personal data

3.2.4 (1) The *QFC Authority* may grant an application for a permit to transfer *Personal Data* with or without conditions it considers necessary.

(2) Upon deciding to grant a permit, the *QFC Authority* will without undue delay inform the *Data Controller* of such decision and any conditions.

4. RECORDS AND NOTIFICATIONS

4.1 RECORDS

For the purposes of Article 17(2)(A) of the *Data Protection Regulations*, a *Data Controller* must record the following information in relation to its *Personal Data Processing* operations:

- (A) description of the *Personal Data Processing* being carried out;
- (B) an explanation of the purpose for the *Personal Data Processing*;
- (C) the *Data Subjects* or class of *Data Subjects* whose *Personal Data* is being processed;
- (D) a description of the class of *Personal Data* being processed; and
- (E) a list of the jurisdictions to which *Personal Data* may be transferred by the *Data Controller*, along with an indication as to whether the particular jurisdiction has been assessed as having adequate levels of protection for the purposes of Articles 9 and 10 of the *Data Protection Regulations*.

Guidance

- (1) With respect to Rule 4.1.1(B) the purposes for which *Personal Data* may be processed will vary but will usually include one or more of the following:
 - (a) accounting and auditing;
 - (b) administration of justice;
 - (c) administration of membership records;
 - (d) advertising, marketing and public relations for the *Data Controller* itself;
 - (e) advertising, marketing and public relations for others;
 - (f) benefits, grants and loans administration;
 - (g) consultancy and advisory services;
 - (h) credit referencing;
 - (i) debt administration and factoring;
 - (j) education;
 - (k) information and data bank administration;
 - (l) insurance administration;

- (m) legal services;
 - (n) licensing and registration;
 - (o) pensions administration;
 - (p) property management;
 - (q) provision of financial services;
 - (r) research; and
 - (s) staff administration.
2. With respect to Rule 4.1.1(C), where *Personal Data* of multiple *Data Subjects* is being processed, *Data Controllers* may instead of listing individual *Data Subjects*, record the class of *Data Subject* involved. In such a case, *Data Controllers* may use the following, or other similar, classes:
- (a) staff, including agents, temporary and casual workers;
 - (b) clients and customers;
 - (c) suppliers;
 - (d) members;
 - (e) complainants, correspondents and enquirers;
 - (f) relatives and associates of the *Data Subject*; and
 - (g) advisors, consultants and other professional experts.

4.2 NOTIFICATIONS

4.2.1 For the purposes of Article 17(2)(B) of the *Data Protection Regulations*, a *Data Controller* must notify the *QFC Authority* of any of the following *Personal Data Processing* operations undertaken other than in accordance with a permit issued by the *QFC Authority*:

- (A) any *Personal Data Processing* operation or set of operations involving the *Processing of Sensitive Personal Data*; and
- (B) any *Personal Data Processing* operation or set of operations involving the transfer of *Personal Data* to a *Recipient* outside of the *QFC* which is not subject to laws and regulations which ensure an adequate level of protection.

4.2.2 When a *Data Controller* gives a notification to the *QFC Authority* in accordance with Rule 4.2.1, the notification must contain the following information:

- (A) the name of the *Data Controller*;
- (B) the address of the *Data Controller*;
- (C) the name, address, telephone number, fax number and e-mail address of the *Person* within the *Data Controller* responsible for making the application for the permit;
- (D) the reason for which notification is being provided;
- (E) a general description of the *Personal Data Processing* being carried out;
- (F) an explanation of the purpose of the *Personal Data Processing*;
- (G) the *Data Subjects* or class of *Data Subjects* whose *Personal Data* is being processed;
- (H) a description of the class of *Personal Data* being processed; and
- (I) a statement of which jurisdictions to which *Personal Data* will be transferred by the *Data Controller*, along with an indication as to whether the particular jurisdiction has been assessed as having adequate level of protection for the purposes of Articles 9 and 10 of the *Data Protection Regulations*.

4.2.3 The notification required by Rule 4.2.1 must be provided to the *QFC Authority*:

- (A) immediately upon commencing of the *Personal Data Processing* referred to in Rule 4.2.1;
- (B) on an annual basis where the *Personal Data Processing* is to continue in the subsequent year; and
- (C) immediately upon any *Personal Data Processing* being processed in a manner different to that described in the initial notification.

4.2.4 The annual notification in Rule 4.2.3(B) must be submitted to the *QFC Authority* within four months of the *Data Controller's* financial year end.

5. CLAIMS

5.1 PROCESS OF LODGING A CLAIM

5.1.1 For the purposes of Article 23(1) of the *Data Protection Regulations*, a *Person* may file a claim with the *QFC Authority* by providing the following information in writing:

- (A) full name and address of the *Person* making the claim;
- (B) the full name and address of the *Data Controller* whom the *Person* believes has contravened the *Data Protection Regulations*;
- (C) a detailed statement of facts which the *Person* believes gives rise to contravention of the *Data Protection Regulations*;
- (D) the relief sought by the *Person* making the claim; and
- (E) a declaration from the *Person* that they have provided the *QFC Authority* with accurate information and that they understand that any information provided will be processed by the *QFC Authority* in accordance with Article 8 of the *Data Protection Regulations*.

Guidance

A claim filed with the *QFC Authority* under Rule 5.1.1 should also include:

- (a) full contact details of the *Person* making the claim including the preferred method of contact;
- (b) the relationship the *Person* has with the *Data Controller* (for example employee, customer or account holder);
- (c) copies of any relevant documents which describe the events that gave rise to the claim; and
- (d) copies of relevant correspondence between the *Person* and the *Data Controller*, including details of any correspondence between the *Person* and the *Data Controller* trying to resolve the problem.

5.1.2 Upon receiving a claim lodged under Article 23(1) of the *Data Protection Regulations*, the *QFC Authority* may make such enquiries in respect of the claim that will, in the view of the *QFC Authority*, lead to the most timely, fair and effective resolution of the claim.

5.1.3 At the conclusion of the mediation process, should the *QFC Authority* determine to issue a direction requiring a *Data*

Controller to do any act or thing in accordance with Article 23(3) of the *Data Protection Regulations*, the *QFC Authority* will do so by issuing a notice in writing setting out:

- (A) the act or thing that the *Data Controller* is required to do;
and
- (B) the time within which, or before which, the *Data Controller* is required to do that act or thing.