Data Protection Office
Qatar Financial Centre

Data Protection

Regulations & Rules 2021 Guidance

DPO_GUIDE_2022_V3

CONTENT

Introduction 4

Scope 4

Part 1 – Application, Commencement and Interpretation..... 6

Article 1 – Citation..... 6

Article 2 – Application 6

Article 3 – Commencement 6

Article 4 – Language 7

Article 5 – Purpose of these Regulations 7

Article 6 – General Application of These Regulations 8

Article 7 – Scope 9

Part 2 – General Provision for the Processing of Personal Data 10

Article 8 – Principles relating to the Processing of Personal Data 12

Article 9 – Responsibility for Compliance with the Principles 15

Article 10 – Lawfulness of Processing 16

Article 11 – Conditions for Consent 19

Article 12 – Processing of Sensitive Personal Data 23

Article 13 – Transparent information, communication and exercise of the rights of the Data Subject .. 29

Article 14 & 15– Information to be Provided where Personal Data are Collected from the Data Subject.32

Part 3 – Data Subject Rights 36

Article 16 – Right to Access 37

Article 17 – Right to Rectification 40

Article 18 – Right to Erasure 42

Article 19 – Right to Object 45

Article 20 – Right to Restriction of Processing 47

Article 21 – Right to Data Portability 49

Article 22 – Automated Individual Decision-Making, Including Profiling 50

Part 4 – Transfers of Personal Data Outside the QFC 54

Article 23 – Transfers Out of the QFC: Adequate Level of Protection 56

Article 24 – Transfers out of the QFC: Absence of an An Adequate Level of Protection 57

Part 5 – Data Controller and Data Processor Obligations 63

Article 25 – Responsibility of the Data Controller 63

Article 26 – Data Protection by Design and by Default 63
Article 27 – Data Protection Impact Assessment 66
Article 28 – Data Processors 72
Article 29 – Security of Processing 76
Article 30 – Record of Processing Operations 80
Article 31 – Notification of Personal Data Breaches 84
Part 6 – The Data Protection Office 90
Article 32 – Establishment of the Data Protection Office and the Data Protection Commissioner 90
Article 32A – The Data Protection Commissioner 91
Article 33 – Powers 92
Part 7 – Remedies 95
Article 34 – Right to Lodge a Complaint with the Data Protection Office 95
Article 35 – Right to Compensation and Liability 96
Article 36 – General Conditions for Imposing Penalties 99
Part 8 – Final Provisions 101
Article 37 – General Exemptions 100
Article 38 – Interpretation 103
Article 39 – Definitions 103

Introduction

This document provides guidance on all aspects of the QFC Data Protection Regulations and Rules 2021 (the "Regulations" and the "Rules"). While every effort has been made to include all elements and examples relevant to Qatar Financial Centre ("QFC") licenced firms, this document will not cover everything. Firms are encouraged to read and understand the QFC Regulations and Rules together with this guide to understand their firms' specific obligations. The QFC Data Protection Office is always available to provide individual guidance should a question not be covered by this document.

Unless separately defined in this document, capitalised terms have the meanings set out in Article 39 of the Regulations (see also Article 39 of this guidance document).

It is important to remember that all firms are likely to Process Personal data in some form or another, whether it be the data of their employees, customers, suppliers, shareholders, Board members, etc. The Processing of this data and its protection are critical to the success of any firm as it builds trust and engagement with stakeholders and can enhance the firm's reputation.

The Regulations themselves are both principle and obligation-based. Where they are principle-based, the Regulations do not set out what a firm must do to be compliant; rather, they provide a framework for compliance and leave the exact details of how these will be implemented to individual firms. Firms must apply these Principles to their Personal Data Processing operations and must be able to demonstrate objectively they have complied with them. In addition, there are specific obligations that must be complied with, including reporting and response deadlines.

At its heart, the Regulations require firms handling Personal Data in connection with operations in the QFC to ensure that such Personal Data are Processed lawfully, transparently and fairly. In addition, the Regulations provide the Data Subject, the individual whose data it is, with a broad set of rights in respect of their Personal Data. These rights include the right to be informed, to access that data, and object to and restrict Processing.

Finally, firms should remember they are not alone when complying with these Regulations and Rules. The Data Protection Office will be here to help support and guide firms on their compliance journey, and firms are encouraged to reach out and discuss any issues they might encounter along the way.

Commissioner for the QFC Data Protection Office

Scope

The guidance has been written with reference to QFC Law No. (7) of the Year 2005 and all relevant Regulations and Rules within the QFC. The QFC operates under common law principles. The Regulations and Rules have been drafted with reference to international standards and best practices, including the EU General Data Protection Regulation1, the UK Data Protection Act 2018, and other data protection laws and regulations worldwide. Where a topic or particular question is not covered by this guide, firms are encouraged to seek guidance from relevant data protection authorities in jurisdictions with similar legislation, such as the Information Commissioner's Office in the UK.

[1]Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

Disclaimer

The information presented in this guidance document is only intended for clarification purposes and does not provide an opinion on the lawfulness of any individual Processing. The guidance does not constitute legal advice or a legal opinion, and it is not binding on the Qatar Financial Centre Authority ("QFCA") or the Data Protection Office. We, therefore, recommend legal advice is sought before making any decisions on the subject matter.

To the maximum extent possible, neither the QFCA nor the Data Protection Office shall be responsible for any liability that may arise from the use of or reliance upon this information. The Data Protection Office reserves all rights in relation to the enforcement of the Regulations. The information contained in this guidance document shall not affect its ability to investigate, determine, or otherwise take any action in relation to the subject matter hereof.

Part 1

Application, Commencement, and Interpretation

Part 1 of the Regulations provides general information on the application, scope, language, and commencement of the Regulations.

It provides information on where the Regulations get their authority and the overarching purpose of the Regulations.

Data controllers, data processors and data subjects should familiarise themselves with this Part paying particular attention to Article 7 (Scope). Article 7 provides specific information on when the Regulations are applicable and introduces an extraterritorial aspect to the Regulations.

Finally, firms should familiarise themselves with the definitions in Article 39, paying attention to the definitions of data controller, data processor, and data subject and the broad definition of processing.

Article 1 – Citation

ARTICLE 1 – CITATION

These regulations are the data protection regulations 2021.

Article 1 defines how the Regulations are to be referred. It is this citation that will be used throughout all communications and guidance relating to these Regulations.

Article 2 – Application

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 2 sets out where the power to issue the Regulations is derived. The article of the further states that the related matters in state law do not apply in the QFC. Article 18 of the QFC Law No. 7 of Year 2005 sets out how QFC Law interacts with State laws[2].

This article should be read in conjunction with Article 7 and provides information on the Authority to issue such Regulations in the QFC.

Article 3 – Commencement

ARTICLE 3 – COMMENCEMENT

These Regulations come into force on the date of their signature by the Minister.

Article 3 provides clarity on when the Regulations come into force.

Version 3 of the Regulations came into force on December 6, 2023.

[2]QFC Law No. 7 of year 2005 https://qfcra-en.thomsonreuters.com/sites/default/files/net_file_store/QFC_Law-V3-Oct09.doc.pdf

Article 4 – Language

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 4 states English is the language of the Regulations and that any other translation is not authoritative.

Article 5 – Purpose of these Regulations.

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.

Personal data belongs to the data subject and as such the regulations set out a framework by which the data and data subject rights are protected in relation to that data.

Where the Regulations refer to the rights and legitimate interests of individuals, it is referring to not only the rights set out in these Regulations but also the broader right to privacy and a private life set out in Article 21 of the Arab Charter on Human Rights1, of which the State of Qatar is a signatory, and states:

Article 21

1. *No one shall be subjected to arbitrary or unlawful interference with regard to his privacy, family, home, or correspondence, nor to unlawful attacks on his honour or his reputation.*

2. *Everyone has the right to the protection of the law against such interference or attacks.*

The Regulations are principle-based; they place the onus on the firms, as either/or Data Controller and Data Processor, as to how they ensure compliance. Firms acting in one or both of these capacities can approach compliance with the regulations according to their circumstances and business needs.

Despite the Regulations being principle-based, there remain several specific obligations on Data Controllers and Data Processors, such as providing clear information to Data Subjects when first collecting their Personal Data (Article 14) or having a record of all their Personal Data Processing operations (Article 30).

Parts 2, 3, 4 and 5 of this guidance deals comprehensively with the obligations placed on Data Controllers and Data Processors. Part 6 focuses on the Data Protection Office and its role, responsibility and powers. Part 7 deals with remedies for Data Subjects who have experienced a breach of these Regulations.

[3]Arab Charter on Human Rights https://nhrc-qa.org/en/arab-charter/

Article 6 – General Application of These Regulations

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 6 details the types of Processing that apply to the Regulations.

The Regulations are limited to two types of Processing:

Automatic Processing

automated system such as a computer system. Since most modern offices use computer systems throughout their organisations, most, if not all, of their Processing will fall into this classification.

Processing that does or is intended to form part of a filing system.

This part of the Article extends the application to cover manual records but only where they form part of, or it is intended they form part of a filing system. Where a manual record is not intended to be part of a filing system, even if it contains Personal Data, then it is not covered by these Regulations. A filing system is defined in the Regulations as "any structured set of Personal Data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis". The key feature here is if the data are structured in such a way as to facilitate the retrieval of the Personal Data then it will be a filing system.

Example

The UK's Information Commissioner's Office4 UK's Information Commissioner's Office, V2.0 May 2011. Data protection Frequently asked questions and answers about relevant filing systems, www.ico.org.uk.] gives a simple test to determine if the Processing does or is intended to form part of a filing system called the 'temp' test. The test is such that if a temporary employee could, given a short introduction, explanation, or an operating manual, extract specific information about an individual from the records, it would be considered a 'filing system'.

When the Regulations do not apply

This article explicitly excludes the Processing of Personal Data associated with a deceased individual from the Regulations.

[4]UK's Information Commissioner's Office, V2.0 May 2011. Data protection Frequently asked questions and answers about relevant filing systems, www.ico.org.uk.

Article 7 – Scope

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.

Article 7 provides information on the extent of the applicability of the Regulations, which can be referred to as the territorial scope of the Regulations.

Firstly, the Regulations apply where the Processing is undertaken by a firm licenced by the QFC, acting as either a Data Controller or Data Processor. This is irrespective of whether the Processing takes place in the QFC.

Secondly, the Regulations apply to Data Controllers and Data Processors who are not licenced by the QFC but, through ongoing arrangements, use a QFC licenced firm to Process Personal Data of Data Subjects who are in Qatar. Notwithstanding the language in Article 7(2), the Commissioner's interpretation is that there here are two elements to this provision: firstly, the Data Subject has to be in Qatar, and secondly, the Processing has to be on an ongoing basis. This does not mean that it has to be regular or frequent, but through ongoing arrangements that are more than on an occasional and incidental basis. The processing shall be considered as "occasional" if it occurs outside the regular course of business or activity of the Data Controller or Data Processor.

In this case, the Regulations apply to the non-QFC licenced firm but only in relation to that Processing. If the processing of Personal Data by a non-QFC licenced firm is conducted on an occasional basis, then the Regulations shall not apply.

Article 7(2) gives the Regulations extraterritorial effect in that they apply to and must be complied with by non-QFC licenced firms when the conditions contained in the Article are met.

Example

A Data Controller established in the QFC collects and processes their employees' personal information to pay salaries. The Data Controller sends this Personal Data to their head office based in Germany, where global salary payments are managed on behalf of the group entities.

The firms' head office in Germany is acting as a Data Processor for the QFC firm, and is processing such data as part of the head office's ongoing arrangements with the QFC firm (i.e. to manage salary payments of employees in the QFC firm). This Processing activity is subject to the QFC Data Protection Regulations.

Example

A Data Controller not established in the QFC, which is processing Personal Data of employees of their QFC subsidiary who are in Qatar to administer an employee discount program, is subject to the QFC Regulations for Processing of personal data for this purpose. As a Data Controller they must comply with all provisions of the Regulations that relate to Data Controllers for this processing activity. For example, in this case, the non-QFC Data Controller will have to provide employees of the QFC entity with a clear, concise transparency notice on how their personal data is processed, including how to exercise their Data Subject rights..

Cross-reference

See Articles 14 & 15 for information on the types of information that must be disclosed, and when, to a Data Subject.

See Article 30 for information on records of processing and what must be included for each Processing activity.

See Article 32 for information on the establishment of the Data Protection Office and the role of Data Protection Commissioner.

See Article 18 of the QFC Law No. 7 of Year 2005 for information on how the Regulations interact with the laws of the State of Qatar.

Part 2

General Provision for the Processing of Personal Data

Part 2 of the Regulations deals with the general provisions' firms must comply with when acting as a Data Controller as defined within the Regulations.

Firms must understand what a Data Controller and Data Processor is, what constitutes Processing, and who are their Data Subjects. In addition, firms must know when they are acting as a Data Controller or as a Data Processor as different provisions of the Regulations will apply depending on the firm's role as a Data Controller and/or Data Processor.

The Data Controller is defined as an individual or entity that determines the purposes and means of the Processing of Personal Data: i.e. why the processing is taking place and how it shall be achieved (e.g. the means used to achieve the processing objective). The Data Controller has influence over the data processing by virtue that it decides certain key elements about the processing.

Example

A financial institution is licenced in the QFC and processes Personal Data of its employees. It determines why it processes their Personal Data (i.e. to carry out its obligations as an employer, to make salary payments, etc.) and how (e.g. by using a payroll provider to administer salary payments). The financial institution is a Data Controller.

The ***Data Processor*** is an individual or entity that undertakes the Processing of Personal Data on behalf of a Data Controller. The Data Processor processes Personal Data for the benefit of the Controller and under its direct authority or control. A Data Processor must not process the data other than in accordance with the Data Controller's instructions. If a Data Processor goes beyond the Data Controller's instructions and starts to determine its own purposes and means of the processing, it will then be considered a Data Controller in respect of that processing.

Example

Company hires an IT service provider to perform general support on its IT systems. The IT service provider has access to a large amount of Personal Data available on the IT systems, even though access to such data is not the main object of the support service. The IT service provider provides the support services on behalf of the Company and on its instructions (e.g. by way of a written agreement). The IT service provider is a Data Processor.

Processing is 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. The definition of Processing covers a wide range of operations performed on Personal Data and will likely cover any action involving Personal Data. Examples of processing include employee management and payroll administration, video recording (such as CCTV), sending promotional emails, shredding documents containing personal data, and accessing a database containing personal data.

A ***Data Subject*** is 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. Companies and other entities (e.g. government bodies, othercorporations, and unincorporated bodies) are not Data Subjects. For example, employees of a firm would be categorised as Data Subjects.

Part 2 of the Regulations deals with:

- Article 8 – the Principles relating to the Processing of Personal Data, specifically;
    - Principle 1: Lawfulness, fairness and transparency;
    - Principle 2: Specific purpose;
    - Principle 3: Data minimisation;
    - Principle 4: Accuracy;
    - Principle 5: Storage limitation;
    - Principle 6: Integrity and confidentiality of Processing;
- Article 9 – Responsibility for Compliance with the Principles;
- Article 10 – The Lawful Basis to Process Personal Data;
- Article 11 – Specific requirements when using Consent as a lawful basis;
- Article 12 – Processing of Sensitive Personal Data;
- Article 13 – Providing specific, intelligible and clear information to Data Subjects regarding the Processing; and
- Articles 14 & 15 – Information to be provided where Personal Data are collected from the Data Subject.

Article 8 – Principles relating to 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 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 about the purposes for which they are Processed.

(4) Principle 4: Accuracy
Personal Data may be Processed only if it is accurate and up to date. Reasonable efforts (taking into account the purposes for which the data were Processed) must be made to ensure that inaccurate personal data Personal Data 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.

In general, the Regulations are principle-based. They set out fundamental principles and a framework but leave the exact details of how these will be implemented to individual firms.

Firms must apply these Principles to their Personal Data Processing operations and their specific circumstances and must be able to demonstrate objectively they have complied with them.

Cross-reference

See Articles 9, 25 & 26 for the requirements to demonstrate compliance with the Principles and the Regulations overall.

The Principles

Principle 1: Lawfulness, fairness, and transparency

There are three requirements within this principle, these are:

- Lawfully – Processing of Personal Data must be done within the limits of applicable laws. To Process Personal Data lawfully under the Regulations, firms must have an appropriate lawful basis upon which the Processing is takes place. All Processing of Personal Data undertaken by a firm must be based on at least one of the criteria set out in Article 10 of the Regulations. In addition, when a firm is Processing Sensitive Personal Data, one of the special conditions in Article 11 must also be met. If the Processing is not based on one of these conditions, then the Processing is not lawful. Fairly – This refers to how the Processing will affect the Data Subject and what they reasonably might expect will be done with their Personal Data. Data Subjects must be made aware that their Personal Data will be processed and how in order to allow them to make an informed decision about whether they agree with the Processing and enable them to exercise their rights. Where Personal Data are Processed in unexpected ways, firms should be able to justify why they are Processing Personal Data in such a way and how they will mitigate any adverse effects. Finally, Data Subjects should not be misled or deceived about how their data are collected or Processed.

- Transparently – Data Controllers must be open and clear towards Data Subjects when processing their Personal Data. Data Subjects should be told what, how and why their Personal Data are being Processed. Such information should be provided not only to individual customers or clients of firms, but also their employees by way of an employee privacy notice. The information must be provided as per Articles 14 & 15 and Rule 3. In addition, Article 13 provides for how that information should be provided, e.g., in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Cross-reference

See Article 10 for the lawful basis (bases) under which all Personal Data Processing must take place and Article 11 for the basis under which Sensitive Personal Data can be Processed.

See Articles 13, 14 & 15 and Rule 3 for information on the transparency requirements.

Principle 2: Specific purpose

Principle 2 is often referred to as the purpose limitation. Personal Data should only be Processed for specific, explicit and legitimate purposes and only in accordance with the relevant Data Subject's rights. In addition, Personal Data cannot be further Processed in a way incompatible with those purposes or those rights.

This means firms should clearly understand why they are collecting Personal Data and for what purpose. It must be processed lawfully and be sufficiently documented in the Article 30 record of processing and transparently disclosed to Data Subjects via the Article 13 & 14 privacy notice.

Where the firm wishes to use the data for another purpose other than the one for which it was originally collected and disclosed to the Data Subject, that new purpose will need to be lawful, fair, and transparent.

Cross-reference

Articles 13, 14 and Rule 3 state the purpose of the Processing must be communicated to the Data Subject.

Article 30 and Rule, state the purpose must be captured in the record of processing.

Principle 3: Data minimisation

This principle is one of three Principles focused on data standards, including Principle 4, accuracy and Principle 5, storage limitation. Principle 3 focuses on the adequacy, relevance and limitation of what is necessary for the purposes for which Personal Data are Processed.

Specifically:

- Adequate means the Personal Data collected should be sufficient to meet the purpose of the Processing.
- Relevant means that the Personal Data must have a direct link to that purpose.
- Limited to what is necessary means the data collected should not exceed the minimum needed to meet the stated purpose.

In essence, this means firms should only collect the minimum amount of necessary Personal Data needed to achieve the purpose of the Processing.

Example

A firm offers a shared platform for restaurants to provide takeaway and delivery orders for customers. The platform requires your name, address, and payment details to provide its service. The platform does not ask for additional information such as nationality or gender, as this is not necessary or required to offer the service they are providing.

Principle 4: Accuracy

Accuracy is the second principle that deals with data standards. This principle requires firms that hold Personal Data to ensure data are accurate and not factually misleading and, depending on how the data are used, is up to date or erased.

Firms should have a process to review Personal Data periodically to check if it needs to be updated or to delete any unneeded data. In addition, they must clearly understand the purpose of Personal Data as this will affect whether the data needs to be updated or not.

This principle is linked to the Data Subject's right of rectification in Article 17.

Example

A firm must send clients an annual statement in the post each year. Some statements are marked 'return-to-sender' because the individual no longer lives at that address. Firms should have a process in place to identify any post that is returned to them, to no longer send statements to those addresses, and to contact these clients through other channels to confirm a new postal address.

Consequently, where the firm must keep a record of previous addresses, this historical information will be accurate. Where the client currently lives does not impact the accuracy of their previous addresses.

Cross-reference

See Article 17 for information on the Data Subject right to rectification.

Principle 5: Storage limitation

Storage limitation is the final principle related to data standards. It is focused on ensuring firms delete or anonymise Personal Data they no longer have a purpose to Process. This principle applies equally to data that is irrelevant to the Processing and inaccurate or out-of-date.

Firms should not keep Personal Data for longer than is necessary for the purposes for which the Personal Data is processed. Once the Personal Data is no longer needed, it should be securely deleted or destroyed.

The amount of time a firm can retain Personal Data are not stated in the Regulations or Rules, so firms must identify a retention period for data (i.e. by determining how long they require Personal Data for the purpose for which the Personal Data is processed) and ensure after this time it is deleted or anonymised.

Firms must verify whether any retention requirements are placed on them by other laws and regulations when determining their retention periods (for example, under Employment or Company laws).

This principle is linked to the Data Subject's right of erasure in Article 18 but will impact the right of access and other rights requests.

Example

When determining the retention period for employee data, firms should review their needs and related legal requirements such as the QFC Employment Regulations, which place a minimum retention period for specific employee data after the employment terminates.

If the firm wishes to retain data longer than this period, it must have a clear purpose and lawful basis under Article 10.

After this time, the firm no longer has a purpose nor lawful basis for retaining the data, and it must be deleted or anonymised.

Cross-reference

See Article 18 for information on the Data Subject right to erasure.

Principle 6: Integrity and confidentiality of Processing

This principle is focused on security and states Personal Data are "Processed in a way that ensures that the data are appropriately secure, using appropriate technical and organisational measures".

"Appropriately secure" refers to the risks associated with the Processing of the Personal Data and considers factors such as the types and categories of Personal Data and Data Subjects and any onward transfers to third parties.

"Using appropriate technical and organisational measures" is the second step and looks at both the technical controls such as encryption or logical access and organisational measures such as policies, employee training and development.

In terms of security, the principle focuses on protecting the data "against unauthorised or unlawful Processing and accidental loss, destruction or damage.

See the guidance on Article 29 for more information on practically complying with this principle.

Cross-reference

See Articles 26 and 27 for more information on data protection by design and by default and the requirements for data protection impact assessments.

See Article 29 for information on the security of Processing.

Article 9 – Responsibility for Compliance with the Principles

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 9 is often referred to as the 'accountability' Principle and places the onus on the Data Controller to show how they are complying with the Principles in Article 8.

Firms should read this Article in conjunction with Article 25 as the requirement to demonstrate compliance with the Principles and implement appropriate and effective technical and organisational measures are interlinked.

This Article strengthens the 'use test' in the Data Protection Regulations 2005, whereby a firm is not compliant where they cannot demonstrate compliance with the Regulations.

Example

Where a Data Controller has identified Article 10(1)(C) (i.e. the Processing is necessary to comply with a legal obligation) as the lawful basis for Processing Personal Data, it should be able to identify the law or regulations that compel them to Process the Personal Data in question.

Information on the legal obligation should be communicated to Data Subjects in compliance with Articles 13 and 14 and should be captured as part of the record of Processing operations under Article 30.

Cross-reference

Article 25 provides more information on the responsibilities of Data Controllers, particularly the requirement to demonstrate Processing is performed per the Regulations.

Article 10 – Lawfulness of Processing

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 10 provides the lawful bases under which Personal Data can be Processed and is directly linked to Principle 1:

Lawfulness, fairness and transparency and Principle 2: Specific purpose in Article 8.

The lawful basis on which Processing is based depends on the intended purpose of the Processing and not the Personal Data itself. This means firms may Process Personal Data of the same type but for different purposes and on different lawful bases.

1. Consent

Consent is one of the lawful bases for processing Personal Data. For consent to be valid, it must meet the conditions set out in Article 11. See Article 11 – Conditions for Consent section below.

Cross-reference

See Articles 11 for information on the conditions for valid consent.

2. Necessary to perform or enter into a contract

This lawful basis applies where:

- There is a contract in place with the Data Subject, and the firm needs to Process their Personal Data to comply with obligations under that contract; or
- The contract has not been entered. However, the firm has been asked to take steps, such as providing a quote, so the parties can decide if they want to enter the contract. It does not matter if the contract is ultimately not entered into, just that the Processing was on the contemplation of such a contract.

The critical phrase here is "necessary to perform a contract" or "necessary in order to take steps to enter into a contract". In understanding whether the Processing is "necessary" to perform a contract, consideration must be given to the nature and ultimate purpose of the contract. For example, simply putting a requirement to provide Personal Data into a contract may not fully meet this lawful basis if the firm can fulfil the contract without Processing the Personal Data.

Example

A firm offers a collection and delivery service to its customers and, as part of the contract, requires their name, address and contact information of the customers. In this case, these pieces of Personal Data are necessary to fulfil the purpose of the contract and to enable the firm to provide its services to the customers, and would be legitimate.

3. Obligation imposed by law

Many laws, regulations, rules, etc., place specific obligations on firms. To meet those obligations, firms may have to process Personal Data in a particular way.

When Processing Personal Data under this lawful basis, the firm must be able to reference the specific legal obligation placed upon them for the Processing to be lawful and to fulfil the accountability requirements in Article 9.

The law or regulation may not specifically mention the Processing of Personal Data; however, if the Processing of the Personal Data are deemed necessary to meet the requirements of a legal obligation, then this lawful basis applies. Firms should ensure there is no less intrusive way to meet the needs of the obligation without the Processing of Personal Data. If there is, then the Processing of Personal Data under this basis may not be lawful.

Firms must be able to point to the relevant legal or regulatory requirement when using this lawful basis and must include it in the relevant privacy notice.

Example

As part of the QFC Employment Regulations, firms are obliged to maintain specific records of employees. The Regulations state this record must include, for example, nationality, salary, and academic and professional qualifications. Firms can refer to this requirement when processing employees' personal data and must include it in their employee privacy notice.

4. Vital interest

Vital interest is most commonly used in emergency situations where the Data Subject or another person's life is at risk. A key feature of this lawful basis is that the Data Subject is unable to provide valid consent.

Given the likely nature of the data required for this lawful basis (i.e. health data), the provisions of Article 12, Processing of Sensitive Personal Data, would also apply.

It is unlikely this lawful basis will be used widely by QFC firms; however, it is conceivable that it could be needed following a health & safety incident at a place of employment.

Example

An employee of a QFC firm has a medical emergency whilst at work and is unresponsive. If the employer knows, for example, the individual has a pacemaker installed, they can disclose this information to the paramedics so they may take this information into account when administering treatment.

Cross-reference

See Articles 12 for more information on the lawful basis of vital interest when Sensitive Personal Data are involved.

5. Public interest

Public interest is focused on Processing that benefits society in general and goes beyond merely the commercial interest of the firm. Public interest must have a regulation, law or statute applicable to the firm that provides the public interest. A law or regulation may require a firm to collect or Process Personal Data in a particular way. The law may or may not be specific on the type of Processing that must occur; however, to rely on the lawful basis, firms need only show their Processing is done to achieve the public interest set out in the relevant law.

As with previous lawful bases, the test here is one of necessity. The processes must be necessary to achieve the interest as set out in the law. For the Processing to be "necessary", it should be more than standard practice. The lawful basis would not apply if you can reasonably achieve the purpose by some other less intrusive means or by processing less data.

Accordingly, firms should ensure their Article 30 records reflect the necessity of such Processes when relying on public interest.

Cross-reference

See Articles 30 for information on the requirement to have and what must be included in the record of processing.

6. QFC body in the performance of its functions

This paragraph is explicitly directed at QFC entities and institutions. It gives them the lawful basis to Process Personal Data when performing a task set out in the QFC Law, Regulations or Rules. Similar to public interest, there must be a law or regulation empowering the QFC entity or institution to perform a function or power.

As with all other Data Controllers, QFC entities or institutions must be able to identify the relevant law or regulation under which they get their authority.

Example

Under the Data Protection Regulations, the Data Protection Office, as an institution of the QFC, has the power to investigate complaints. It is under this provision of the Regulations and under Article 10(5)(B)(v) that allows the Data Protection Office to collect Personal Data to meet this function.

7. Legitimate interest

Unlike the other lawful bases, legitimate interest does not relate to a specific purpose for Processing Personal Data but is more adaptive to the needs of the Data Controller. Therefore, there can be many different purposes that meet the definition of a legitimate interest.

Where a firm is using this lawful basis, it must undertake a test to ensure its interests do not override the rights and legitimate interests of the Data Subject. This test is often referred to as the 'balancing test'.

When testing if the firms' legitimate interest does not override the rights and legitimate interests of the Data Subject, firms should examine three important elements of their legitimate interest, namely:

1. The purpose of the processing;
2. How necessary that processing is to achieve the purpose; and
3. Any overriding rights and legitimate interests of the Data Subject.

The first element that must be understood is if the purpose of the Processing represents a legitimate interest to the firm. Any interest that benefits one or more parties involved in the Processing of data can be legitimate. Those interests can be commercial and include fraud prevention, network and information security, and internal administrative purposes; this list is not exhaustive.

The second element refers to the Personal Data and Processing itself. A quick question to ask is whether all the Personal Data is being used to achieve the purpose and whether such use is excessive. Firms should also ask if there is another, less intrusive way to achieve the objective using less Personal Data. This part of the test should consider aspects of the data itself, for example, the use of Sensitive Personal Data and the Data Subject's characteristics, such as their age.

Finally, the legitimate interest the firm wants to pursue needs to be assessed against the rights and legitimate interests of the Data Subject. The firm will need to evaluate the Data Subject's legitimate interests against their own. This should consider if the Data Subject reasonably expects their data to be used in this way and what impact the use of their data will have on them.

Example

Where a firm Processes Personal Data outside the service they provide to the customer, such as for office management or financial accounting purposes, this Processing is within the firm's legitimate interest in managing its business operations and would likely pass the 'balancing test'.

Firms must choose the correct lawful basis for the Processing as the wrong basis will render any Processing based thereunder invalid if incorrect.

Article 11 – Conditions for Consent

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.

This article provides clarity on how the lawful basis of consent is validly obtained and used.

Consent is often used when a Data Controller wants to give a Data Subject real choice and control over how their Personal Data are used, and no other lawful basis is appropriate.

When managed correctly, consent puts Data Subjects in control of their data, builds customer trust and engagement, and can enhance a firm's reputation.

CONSENT IS

a clear statement through clear affirmative action

freely given, informed and unambiguous

as easily withdrawn as given

recorded and evidenced by the controller

CONSENT IS NOT

inferred by silence, prefilled boxes or inactivity

unnecessarily conditional on the provision of a service

unclear and ambiguous

bundled with other consents or tearms & conditions

Valid Consent

For consent to be deemed valid, there are a number of key requirements which must be met, consent must be:

(1) Freely Given: This means Data Subjects must be given a real choice on whether to provide consent. It means they should not suffer detriment if they choose not to provide consent. Data Subjects cannot be pressured into giving their consent. The provision of services cannot be unnecessarily conditional on the consent. Firms must look at the inherent power and knowledge imbalance between them and Data Subjects.
See below for more information on the use of consent in the workplace.

(2) Specific: What the Data Subject is consenting to must be clearly explained to them. This should include who is asking for the consent and the purpose of the Processing to which the consent relates. Different consents should not be bundled together and must be broken into individual consents for each purpose. A good example of this is marketing consents: individual consents should be obtained for each type of electronic marketing, such as email/SMS/WhatsApp, and postal.

(3) Informed: The wording of consents should state clearly and simply with whom the Data Subject is consenting and for what Processing activity. The language used should be easily understandable and accessible for all Data Subjects.

(4) An unambiguous indication: Consent obtained from the Data Subject must be clear and should involve an affirmative action such as an opt-in. Firms should avoid language which is overly legal or technical as this can render the consent impossible to understand for the Data Subject. It should be clear that the Data Subject intended to give their consent to the Processing so firms cannot rely on inactivity, pre-ticked boxes, silence, or other defaults when obtaining consent.

(5) As easy to withdraw as it was to provide: This means Data Subjects must not be put under any unnecessary burden or hardship to withdraw a consent that was validly provided. For example, where a Data Subject has provided their consent via an opt-in tick box on a website or app, removing that consent should be as simple as unticking the box. The withdrawal of consent is forward-looking and does not make unlawful any Processing based on the consent before it was withdrawn. It is also a feature of consent that withdrawal can take place at any time the Data Subject chooses, and the Data Subject, therefore, must be informed of this when they give their consent.

Managing consent

In order to demonstrate firms have validly obtained consent, they must be able to show:

- the Data Subject has consented to the Processing;
- how consent was obtained;
- when the Data Subject provided this consent; and
- what specific Processing the Data Subject consented to.

Firms might consider the use of consent management tools which are an excellent way to manage consents and put Data Subjects in control of their choices.

Duration of consent

Validly obtained consents do not expire; however, they will reduce over time. Firms are encouraged to keep consents under review and update them when necessary, such as when the original purpose for the consent changes or evolves.

Sensitive Personal Data and explicit consent

Firms who wish to Process Sensitive Personal Data1 can only do so when they have met one of the special conditions under Article 8 of the Regulations. One of the special conditions where the Processing of Sensitive Personal Data are permitted is when it is done on the ‘explicit consent’ of the Data Subject.

Explicit consent places a higher burden on firms to demonstrate consent was validly obtained. This is because of the special nature of Sensitive Personal Data and potential harm from its use or misuse to the Data Subject. Therefore, when constructing the request for explicit consent, firms should ensure the specific nature of the Sensitive Personal Data are disclosed and any further relevant information, such as its use in automated decision-making, including profiling or transfers to third parties or outside the QFC.

Finally, it is important to ensure that where explicit consent is being sought, given the Sensitive Personal Data involved, the consent request should be separate from any other consents the firm is seeking.

Consent in the workplace

As mentioned above, one of the criteria for valid consent is that it must be freely given, and Data Controllers must be careful when using consent where there is an inherent power and knowledge imbalance between them and Data Subjects. This is very important particularly in the employer/employee relationship.

The nature of the employment relationship and the reliance the employee has on the employer for their livelihood means that the employee may feel pressure to consent to processing they are not comfortable with, even if no objective pressure is being applied by firm. They may feel that they must consent to not stand out or feel they may face negative consequences by refusing.

Consent may be a viable lawful basis for processing employee Personal Data such as where there is as a consequence, free benefit to the employee, like availing of an employee discount programme. In these cases, the firm will have to adequately document that the consent is freely given and, importantly, that the employee faces no negative consequences for refusing to give consent to begin with or by withdrawing that consent at a later date. If a firm wishes to rely on consent as a lawful basis for Processing Personal Data, it is advisable that they undertake a data protection impact assessment per Article 27 prior to any Personal Data Processing. This will help assess if the consent is freely given and help ensure that the firm has considered other lawful basis for the Processing and the risks and impact on the employees.

Finally, firms should consider other lawful basis, such as contractual necessity or legitimate interest for Processing personal data of employees, keeping in mind that there may be other restrictions on the Processing should it involved Sensitive Personal Data per Article 12.

Consent for marketing & the use of website cookies

Consent is most commonly found when firms capture and Process Personal Data for marketing purposes. One way firms do this is by placing cookies on their website or using other online tracking methods.

Cookies are small pieces of information placed on devices by the website visited. Cookies help track preferences and can be used to help keep websites secure.

Typically, cookies are broken down into four categories, which are:

- **Strictly Necessary Cookies:** these are needed so websites can function correctly.
- **Analytics Cookies:** these allow firms to count visits and traffic sources and allow firms to measure and improve website performance. These cookies tend only to collect aggregated data and are therefore anonymous.
- **Functional Cookies:** these enable websites to provide enhanced functionality and personalisation. They can be provided by the firm or third-party providers whose services have been added to the site.
- **Targeting Cookies:** Advertising companies use them to build a profile of user interests to present targeted adverts on other sites on the internet.

Example

Where a firm uses marketing cookies on their website which Processes Personal Data such as IP address, location information, etc., they must ensure they are providing visitors with the option to consent to the collection and use of that data before Processing occurs. This is often demonstrated by a cookie consent pop up banner. Here, only strictly necessary cookies default to the 'on' position and visitors must actively choose to turn on other cookies, such as those for marketing. Care must be taken to ensure that withdrawal of consent must be as easy as it was to provide such consent when deciding how the visitor can withdraw their consent. Hiding the cookie controls in a link within a privacy or cookie notice which requires the visitor to click and scroll through various documents will likely fall foul of this requirement. Firms should consider leaving access to the cookie contact centre on pages navigated to by visitors to ensure they can easily exercise their right to withdraw their consent.

Cross-reference

This article is linked and should be read in conjunction with Article 10, Lawfulness of Processing, Article 18, the Right to Erasure, and Article 19, the Right to Object.

Article 12 – Processing of Sensitive Personal Data

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 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

(iii) 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).

QFC Data Protection Rules

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.

Sensitive Personal Data are data that, given their nature or characteristic, could have an adverse or negative effect on the Data Subject should they be Processed incorrectly or disclosed to unauthorised persons.

As defined in Article 39 of the Regulations, Sensitive Personal Data are “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”.

The Processing of Sensitive Personal Data are prohibited unless one of the special conditions of Article 12 applies. This means when Processing Sensitive Personal Data, firms must ensure they have a lawful basis to Process the data per Article 10 and meet one of the special conditions contained in Article 12.

The options contained in the Article include Processing based on:

1. Explicit written consent

The Data Subject must give explicit written consent for the Processing of Sensitive Personal Data. Explicit consent is not defined within the Regulations; however, it should, at a minimum, meet all requirements of valid consent in Article 11. See Article 11 – Conditions for Consent section above. Where explicit written consent for the Processing of sensitive Personal Data is being sought, this consent should be separate from other consents, and the Data Subject must be provided with information as to the nature of the data Processed. In addition, the consent for Processing Sensitive Personal Data must be in writing.

As with the use of all consent-based Processing, firms should be mindful of any power imbalance between it as Data Controller and the Data Subject, particularly when the Data Subject is an employee.

Example

A firm wishes to understand the profile of its customer base: for example, their age, gender and religious affiliation . The information is not required to provide the service to the customers and since some of the information is Sensitive Personal Data, the firm decides it will base the Processing on the explicit written consent of the customers. The firm provides customers with an option to select their age, gender and religious brackets, the purpose of the Processing, the details of the profiling and its effects, and a separately worded consent option when they log into their account online. The customer must actively choose the 'I consent to you using this information for the purposes specified' option and are free to untick the option if and when they decide to do so. The customer faces no repercussions if they choose not to provide the information.

2. Employment law requirements

This condition applies when the firm is Processing Sensitive Personal Data when complying with employment law provisions. The firm should be able to identify the provision of the relevant laws or regulations upon which they rely. As with Article 10(1)(C), the law or regulation may not specifically mention the Processing of Personal Data; however, if the Processing of the Personal Data is deemed necessary to meet the requirements of a legal obligation or for the employer to exercise their rights in accordance with the relevant law, then this lawful basis applies. Firms may refer to governmental or industry guidance to justify the necessity of the Processing.

Example

The QFC Employment Regulations require firms to maintain a register of injuries sustained by Employee whist at work. Firms can rely on this requirement to Process health information related to such incidents.

3. Vital interests

Similar to vital interest under Article 10, the Processing must be essential for someone's life, and they must not be in a position to consent themselves. If they can provide valid consent but have refused, then the Sensitive Personal Data cannot be Processed. This condition is mainly reserved for cases of emergency medical care.

Example

If an employee has an unresponsive accident at work their medical history, such as any medical allergies, can be shared with the ambulance or the hospital per Article 12(3).

4. Providing a policy for life or health insurance by insurance companies

When a Life or General Insurance company provides a life or health insurance contract, the Processing of Sensitive Personal Data are permitted. This includes managing and Processing any related claims.

Example

An insurance company that offers health or life insurance products and calculates its premiums on certain health factors of its customers can process such information when offering such products. However, firms must ensure the relevant privacy notice includes a reference to this type of information and its lawful basis.

5. Not-for-profit bodies

This condition includes, for example, charities and clubs Processing Sensitive Personal Data as part of their legitimate activities. Firms cannot share data with any other third party without the consent of the Data Subject. The Processing is limited to members, former members, or other individuals in regular contact with the firm, e.g. beneficiaries, supporters etc. There is no 'necessary' test for this condition to be met, only that the Processing in question is part of the firm's legitimate activities.

Example

A charity processes its members' health information, which it supports through counselling services. The charity can rely on this lawful basis to process Personal Data concerning the health conditions of its members to provide them with the appropriate service.

6. Manifestly made public by the Data Subject

This condition covers data the Data Subject intended to make public and assumes a deliberate act by the individual. The critical point here is that it has to have been the Data Subject who has made the data public. It is not enough that it is in the public domain or they were merely aware the data are public. Also, manifestly made public assumes the data has been made available to the public generally and not in a specific and limited way.

Firms should be careful when relying on data they think the Data Subject has made public, as they will need to demonstrate it was manifestly made public by the Data Subject. Firms that collect data this way must comply with all aspects of the Regulations, including the Principles in Article 8 and Data Subjects rights in Articles 16 to 22, including the transparency obligations in Articles 14 and 15.

Example

An individual makes a public post on a social media platform or an article in a national newspaper that discusses their health status or ethnicity. The individual could reasonably be assumed to be aware this information is now in the public domain.

Posts made in a privacy mode or when made in a limited professional publication will likely fail the test of manifestly made public.

7. Legal claims or a court is acting in its judicial capacity

The purpose of the Processing is to establish, exercise or defend legal claims. 'Legal claims' include Processing necessary for actual or prospective court proceedings, obtaining legal advice, or establishing, exercising or defending legal rights in any other way. The term 'necessary' is key to the first part of this condition. The firm must demonstrate that Processing is necessary in this case. If a court is acting in its judicial capacity, then the Processing of Sensitive Personal Data is allowed.

Example

When adjudicating a case involving Sensitive Personal Data, such as health data, the court relies on this provision for Processing when deciding on the case.

8. Necessary to perform a task carried out by a QFC body in the performance of its functions

Where a QFC body, including the QFC Authority, the QFC Regulatory Authority, the Civil and Commercial Court, the Regulatory Tribunal, or a QFC Institution is performing one of their functions, as set out in laws or regulations, and the

Processing of Sensitive Personal Data is necessary for that purpose. The relevant QFC body will have to be able to demonstrate that the Sensitive Personal Data is necessary for the performance of its function and the function could not have been achieved in another, less intrusive way.

Example

A QFC body, such as the QFCA, Processing Personal Data as part of an inspection or investigation carried out pursuant to the Compliance and Enforcement Rules (CER) of the QFCA Rules Version 10 will be carried out per this lawful basis. The QFCA must ensure Personal Data Processed under this Rule is limited to what is necessary to achieve the objectives set out in the Rules.

9. Reasons of substantial public interest

Much like the lawful basis of public interest in Article 10, substantial public interest is focused on Processing that has benefits for society and will go beyond the commercial interest of the firm. However, for substantial public interest to be met, those benefits must be tangible and real-world benefits to society.

The Regulations do not provide a list of what constitutes substantial public interest. However, like public interest, firms can only use this condition where it is borne out of a legal obligation or requirement applicable to the firm.

The types of circumstances that might constitute substantial public interest include:

- Preventing or detecting unlawful acts;
- Protecting the public against dishonesty, etc.;
- Regulatory requirements relating to unlawful acts and dishonesty, etc.;
- Preventing fraud;
- Suspicion of terrorist financing or money laundering; and
- Safeguarding of individuals at risk.

When using this condition for the Processing of Sensitive Personal Data, firms must ensure that:

- Processing is proportionate to the aim or aims pursued;
- Processing respects the Principles in Article 8; and
- They provide suitable and specific measures to safeguard the rights of the Data Subject.

When the Regulations refer to 'proportionate', it means the amount and scale of the Sensitive Personal Data being used in the Processing must be in balance with the aims of the Processing. If an excessive amount of Sensitive Personal Data is needed to meet the aim, it may fall foul of this test.

Finally, firms should be very cautious when using this condition when Processing Sensitive Personal Data. The firm would need to demonstrate and justify that this condition is suitable over all other conditions, in particular the consent of the Data Subject.

10. Health or preventative medicine

As with other conditions for Processing Sensitive Personal Data, if relied upon, the firm must be able to justify that the Processing is 'necessary' and that the purpose could not have been achieved in another, less intrusive way.

The Processing in this section is limited to the following:

1) Preventive medicine;
2) Medical diagnosis;
3) The provision of care or treatment; or
4) The management of healthcare services.

This part of the Article is limited to:

- A health professional:
  1) Who is subject to national laws or regulations;
  2) Established by competent national bodies; and
  3) With an obligation of professional secrecy; or
- Another person is also subject to an equivalent obligation of professional secrecy.

The term health professional is not defined but covers doctors, nurses, dentists, opticians or optometrists, osteopaths, chiropractors, paramedics, physiotherapists, and pharmacists.

The Data Controller must demonstrate they are subject to national laws or regulations established by competent national bodies and that these laws or regulations bind them to an obligation of professional secrecy.

11. On a permit obtained from the Data Protection Office

Firms can apply for a permit from the Data Protection Office to process Sensitive Personal Data when none of the other options in this article are appropriate.

The permit application process is simple and can be accessed through the client portal available here. And a guide to how to request a permit can be found on the

Cross-reference

This article is linked and should be read in conjunction with Article 10, lawfulness of Processing, Article 11, conditions for consent, Article 26, data protection by default and by design, Article 27, data protection impact assessment and Article 29, security of Processing.

Article 13 – Transparent information, communication and exercise of the rights of the Data Subject

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 of 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.

This Article focuses on how firms must communicate with Data Subjects when providing them information under Articles 14 and 15 and responding to a Data Subject rights request under Articles 16 to 22.

Nature of communication to Data Subject

When providing information under Articles 14 and 15 or responding to a rights request under Articles 16 to 22, the firm must do so in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

- Concise: the information should not be too long but should provide enough information to meet the requirements of Rule 3;
- Transparent: it should cover all Personal Data Processing activities in a way that makes it clear to the Data Subject how their data are being processed;
- Intelligible: the Data Subject should understand the language used, which means firms should know their audience and adjust their language accordingly;

- Easily accessible: the Data Subject should be able to access information, on how firms Process their data in a straightforward way that fits with the service and how their data was provided. Where services are all online, the Data Subject should be able to access the privacy-related information via this online channel. Firms would need to be mindful of Data Subjects that have visual or other forms of impairment which would render a text-based version of the data inaccessible; and
- Using clear and plain language: similar to 'intelligible', this means firms should avoid overly technical language or jargon which will be difficult to understand.

The Article states the information should be easily accessible, taking into account the needs of the Data Subject. Where most transparency notices are in writing, other forms are allowed, such as orally in a face-to-face meeting or through technology such as text-to-speech. To meet the accountability principle, firms should be mindful of how they can demonstrate they provided the information to Data Subjects.

Time limits to respond to Data Subject rights requests

The Article puts a strict time limit on firms when responding to Data Subject rights requests. Firms must respond without undue delay and at least within 30 days of receiving a valid request. There are certain limited circumstances where this time limit can be extended; see below for more information on when this may apply.

Identifying the Data Subject

A request is only valid if the firm can confirm it has come from the Data Subject or an authorised representative. Where the firm has doubts about the identity of the Data Subject, the firm may request information necessary to confirm their identity. In this case, the 30-day time limit does not start until the identity has been confirmed.

Extending the time limit to respond

Firms can extend the time limit to respond to a Data Subjects' rights request in a limited number of circumstances. For example, due to the nature or complexity of the request or when there are several requests from the same individual. In these cases, the firm can extend the period by an additional 60 days. However, the burden to show the request is complex and excessive lies with the firm and is a high hurdle to clear, so this exception should only be relied upon in exceptional circumstances. Where there is a genuine need to extend the period to respond, firms should document the rationale for the extension.

In these cases, firms must still respond to the Data Subject within 30 days, informing them they will be extending the time limit and detailing the reasons for the delay.

Refusing to act on a request

Not all Data Subject rights apply in all circumstances. This means there are times when a firm can lawfully deny a Data Subjects' rights request. Firms can refuse to act on a request if they find it to be manifestly unfounded or excessive in the number or frequency of requests.

When doing so, the firm must still respond to the rights request within 30 days with the reason for not taking action. The firm must also inform the Data Subject that they have the right to lodge a complaint with the Data Protection Office regarding the failure to act.

Firms that refuse to act on a request must document this refusal and any rationale that supports their decision and make it available to the Data Protection Office, if required.

What does manifestly unfounded or excessive mean?

When the intention behind the request does not align with request.

For example, where:

- The request is for rectification, but the Data Subject offers to withdraw the request for some benefit;
- The Data Subject has stated they wish to cause disruption to the firm; or
- There are many different requests over a short period of time e.g., access, erasure, rectification, etc., where the intention is to cause disruption.

Charging

As a matter of default, firms cannot charge a fee for fulfilling any Data Subject rights requests. This ensures access to Data Subject rights is universal and does not exclude those who cannot afford to pay.

In exceptional circumstances where the request is manifestly unfounded or excessive, the firm may charge a reasonable fee.

Firstly, manifestly unfounded or excessive is a subjective test, and firms will need to be comfortable with the request falling into this category. They should document the rationale along with any decision to charge a fee.

Secondly, the fee must be reasonable. In this case, the fee should cover only the administrative expenses in fulfilling the request. Anything else will likely be excessive. Firms should document the basis for calculating any fee charged to a Data Subject.

The firm should contact the Data Subject without undue delay regarding any fees imposed. The time limits to respond to such requests only start after the fee is received.

As access to the rights must be universal, charging a fee is a high hurdle to cross, and firms must be sure the request meets the definition before considering charging a fee.

Cross-reference

See Article 16-22 for more information on when each Data Subject right applies and when they do not.

Article 14 & 15– Information to be Provided where Personal Data are Collected from the Data Subject

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.

QFC Data Protection Rules

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.

Article 14 requires firms to provide specific information to data subjects when their data are first collected directly from them.

Article 15 concerns circumstances when the personal data are not obtained directly from a data subject but through a third party and the time limits to provide the necessary information.

Together, these two articles ensure that the firms are transparent with data subjects regarding what information they collect, how they use it, and their rights regarding their personal data.

This requirement is often referred to as the 'right to be informed' and is one of the cornerstones to ensure data subjects can effectively enforce their rights. This privacy information is often provided through a privacy notice(s).

Time limit to provide the information

When the personal data are first collected from the data subject

When collecting personal data directly from the data subject, firms must provide them witha clear and separate privacy notice from any other information when the data are first collected. This notice should not be included in other documents, such as the Terms & Conditions of service, as it serves a different purpose.

When the data are collected through a third party

When collected from someone other than the data subject, the information must be provided:

- At the latest, within 30 days of obtaining the data;
- When the firm first communicates with the data subject; or
- If the data are disclosed to a third party, when the data is first disclosed.

What information must be provided

The following information must be provided to the data subject;

- The identity and contact details of the data controller;
- The purposes of the processing;
- The lawful basis of the processing;
- The categories of personal data concerned;
- The names or categories of third parties to whom the data are disclosed;
- How long the data are retained;
- A list of the data subject rights and how they can enforce them;
- The consequence for not providing information;
- If applicable:
    - The legitimate interests of the data controller or third parties;
    - The right to withdraw consent;
    - For international transfers, a description of the safeguards in place and where to get a copy of them;
    - For automated decisions, meaningful information, significance and consequences of those decisions;
- The right to lodge a complaint with the data protection office.

Circumstances where the information does not have to be provided

In limited circumstances, where the firm collects personal data from someone other than the data subject, the information contained in the rules does not need to be provided where:

- They already have the information;

In this case, the firm must show that the data subject has already received the privacy information. This can be difficult as the firm did not receive the information directly from the data subject, so it might be difficult to prove what information they received.

- Doing so would be impossible or would involve disproportionate effort;

This is a high hurdle, and the effort involved would have to be disproportionate to the purpose of the processing. For example, where a firm holds emergency contact information of employees, it may be disproportionate to contact each person and provide a privacy notice as their information will only be used in the unlikely event of an accident.

- Complying with the obligation would make impossible, or seriously impair, the achievement of the objectives of the processing;

The purpose of the processing would have to become impossible or be seriously impaired by providing the information to be a valid exception. For example, fraud investigation undertaken by a financial institution may be impaired or prove impossible if that person is put on notice of the investigation.

- The firm is required by law to obtain or disclose the personal data and the law provides appropriate measures to protect the data subject's legitimate interests.

The firm must show which law provides the basis for collecting the data from the third party.

Things to consider

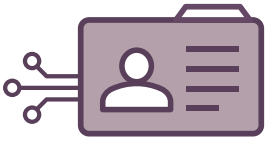
Firms should consider a layered approach to the providing the privacy information. In this way relevant information is presented to firms at the time the personal data are captured rather than directing them to one large unwieldy notice.

Cross-reference

See Article 13 for more information on how to communicate with Data Subjects. For example, information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

See Article 19 for more information on communicating the right to object to Data Subjects.

Part 3



Data Subject Rights

Part 3 of the regulations deals with the various rights data subjects have in relation to their Personal data. Data controllers must be able to demonstrate they can identify, assess and respond to such requests in line with times limits and requirements set forth in Articles 13, 14 & 15.

In this Part of the Regulations Data Subjects have rights regarding:

- Access;
- Rectification;
- Erasure;
- Object;
- Restriction;
- Data portability; and
- Automated individual decision-making, including profiling.

These rights are complemented by the right to transparent information per Articles 14 & 15, the right to lodge a complaint with the data protection office per Article 34 and the right to compensation per Article 35. Specific information on these rights can be found in the relevant section in this guidance.

Data subject rights do not apply equally in all circumstances and firms must be aware of when each right applies to ensure they act on each right correctly.

Which rights apply generally, and which rights are conditional?

Some rights apply generally, in that they apply regardless of the lawful basis under which the firm is processing the personal data: these are the right of access, rectification, and restriction.

The use of automated decision making, including profiling that has a legal effect or would otherwise significantly affect the data subject is limited to specific situations, see the relevant section of this guidance for information on its correct use.

The applicability of the remaining data subject rights is limited and based on the lawful basis under which the firm is Processing the data. The guidance to each Article in Part 3 will provide more information on when each right applies.

General requirement for all data subject rights

Article 13 places specific requirements on firms when communicating with a data subject, particular with regard to the exercise of the rights.

- Nature of communication to data subject;

All communication with a data subject must be concise, transparent, intelligible, and easily accessible using clear and plain language.

- Time limits to respond to data subject rights requests;

Data subject rights requests must be fulfilled within 30 days.

- Extending the time limit to respond;

The 30-days can be extended by a further 60 days in limited and exceptional circumstances.

- Identifying the data subject;

A rights request is only a valid request when it comes from the Data Subject; this means the firm can take steps to identify the Data Subject before proceeding with the request.

- Refusing to act on a request;

There are limited and exceptional circumstances where the firm can refuse a request. These circumstances are usually when the request is manifestly unfounded or excessive such as in the number or frequency of requests.

- Charging;

Firms cannot charge for fulfilling a data subject rights request; however, in exceptional and limited circumstances, firms can charge an administrative fee where the request is manifestly unfounded or excessive.

- Accountability.

Firms must be able to demonstrate they comply with the principles and regulations as a whole per Articles 9 and 25. These means that where they extend the deadline to respond, refuse to act or charge a fee, it must be clearly documented as it is likely to be requested if the data subject makes a complaint to the data protection office.

Article 16 – Right to Access

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 is being processed. If the data subject's personal data is 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 is 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 to in paragraph (3) must not adversely affect the rights and legitimate interests of others.

QFC DATA PROTECTION RULES

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 has been disclosed, unless doing so would be impossible or would involve a disproportionate effort. The data controller must inform the data subject about those recipients if the data subject requests it.

When is it applicable?

The right to know if a firm is processing the personal data of an individual and to obtain a copy of that personal data are a fundamental right of all data subjects.

The right of access has two main characteristics. Firstly data subjects have the right to know whether data about them are being processed. Secondly, if personal data are being processed, they have a right to a copy of that personal data.

When responding to a data subject right of access request, firms must provide the data subject with information on how their data are processed. This should be specific to the information the firm processes for that data subject. For example, information on how employee data are processed would not be provided to customers.

There are limited exemptions to this right within the Regulations, primarily contained in Article 37 and applicable to QFC bodies when discharging their powers and functions.

Recognising a request

A request can come into the firm in many ways and therefore firms must have systems and controls to identify and validate a data subject access request. These ways may include email, post, phone and any other valid and recognised manner in which the firm communicates with their data subjects.

Firms should ensure appropriate employees are trained to recognise a data subject access request when one is validly made.

What information must be provided

The following information must be provided to the data subject;

- The purpose of the processing;
- The lawful basis of the processing;
- The categories of personal data concerned;
- The names or categories of third parties to whom the data are disclosed;
- How long the data are retained;
- A list of the data subject rights and how they can enforce them;
- If applicable:
    - For international transfers, a description of the safeguards in place;
    - For automated decisions, meaningful information, significance and consequences of those decisions;
    - If the personal data was collected from a source other than the data subject, information about that source;
- The right to lodge a complaint with the data protection office.

Providing a copy of the data

If requested, the firm must provide a copy of all personal data they hold to the data subject in a secure and timely manner.

Firms should have a process to identify where the personal data are held within their systems. The Article 30 record of processing, if done correctly, will detail all the processes which use personal data within the firm and will greatly assist in this task.

Engaging with the data subject is a great way to understand the nature of their request, what information they are looking for and how best to provide it to them.

Other things to note

Record-Keeping – firms should record when a data Subject made a request and the outcome of the request, including details of the information provided to them and when it was fulfilled.

Time limits to respond – data subject rights requests must be fulfilled within 30 days.

Extending the time limit – the 30 days can be extended by a further 60 days in limited and exceptional circumstances. See Article 13 for more information on how and when the time limit can be extended.

Refusing to act on a request – there are limited and exceptional circumstances where the firm can refuse a request. These circumstances are usually when the request is manifestly unfounded or excessive such as in the number or frequency of requests.

Charging – firms cannot charge for fulfilling a data subject rights request; however, in exceptional and limited circumstances, firms can charge an administrative fee where the request is manifestly unfounded or excessive.

Cross-reference

See Article 13 for information on how to communicate with a Data Subject, in particular:

- *Nature of communication to Data Subject;*
- *Time limits to respond to Data Subject rights requests;*
- *Identifying the Data Subject;*
- *Extending the time limit to respond;*
- *Refusing to act on a request; and*
- *Charging.*

See Article 30 for information on the record of processing operations.

See Article 37 for information on the limited exemption to this Data Subject right.

Article 17 – Right to rectification

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.

(1A) Where rectification of personal data is not feasible for technical reasons, the data controller need not comply with a request for rectification of the personal data under paragraph (1), where:

(A) The data controller collected the personal data from the data subject; and

(B) The information provided to the data subject under Article 14 was explicit, clear and prominent with respect to the manner of processing the personal data and expressly stated that rectification of the personal data at the request of the data subject would not be feasible.

(2) 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.

When is it applicable?

The right to rectification applies to all data subjects whose personal data are processed by the firm.

There are limited exemptions to this right within the regulations, primarily contained in Article 37 and applicable to QFC bodies when discharging their powers and functions.

What is the right to rectification?

Data Subjects have the right to have:

- Any incorrect information corrected (rectified);
- Incomplete information completed; and
- A statement added to incomplete information.

Closely linked to Article 4 on accuracy, this right requires firms to only Process Personal Data that is accurate and to correct inaccurate data without undue delay.

Firms must make reasonable efforts to correct Personal Data they know to be incorrect and respond to requests to correct incorrect data within the time limits.

As with all Data Subject rights requests, firms must be able to:

- Identify a request to rectify data has been received;
- Determine if the request is valid; and
- Correct the data or add a statement.

Where the firm contends the data are accurate or due to technical issues, the firm cannot correct the data; the firm must offer the Data Subject an opportunity to add a statement to data regarding its accuracy.

If rectification is not feasible

The Regulations provide an exemption from the requirements of Article 17 in situations where the rectification of data is not feasible, due to technical reasons. This is often due to the use of certain technologies, such as Distributed Ledger Technologies, where individual records are immutable. In order to rely on this exemption, Data Controllers must be able to demonstrate the rectification is not feasible, and not merely difficult or costly.

In these instances, the data controller may use technology provided the conditions outlined in Article 17(1A) are satisfied, specifically:

- That the personal data is collected directly from the data subject, and not through a third party; and
- The data subject has been informed, in an explicit, clear and prominent way, through the Article 14 notice, that rectification will not be feasible.

When relying on this exemption, firms must explicitly inform data subjects about the limitations on their right to rectify data before commencing any processing activities. Firms will have to determine the best way to ensure that this information has been brought to the data subjects attention.

What qualifies as ‘explicit, clear, and prominent’ should be determined by the firm, considering the needs of its data subjects and the way it interacts and communicates with them. Information regarding this limitation should not be merely included amongst other data subject rights information in a manner that could dilute its importance. Instead, it should be presented in such a way as to ensure that it is immediately noticeable to data subjects. This may be achieve through the use of a pop-up notice or similar mechanism that requires data subjects to acknowledge having read and understood this limitation before they can proceed. This method guarantees that the notice is not only seen but also acknowledged.

Other things to note

Record-Keeping – firms should record when a Data Subject made a request and the outcome of the request including details of the information provided to them and when it was fulfilled.

Time limits to respond – data subject rights requests must be fulfilled within 30-days.

Extending the time limit – the 30-days can be extended by a further 60-days in limited and exceptional circumstances. See Article 13 for more information on how and when the time limit can be extended.

Refusing to act on a request – firms must always document circumstances where it refuses to act upon a data subject rights request, including when it relies on the exception provided in Article 17(1A). Circumstances where the firm can refuse a request are limited. Including the exemption in Article 17(1A), these circumstances are usually when the request is manifestly unfounded or excessive such as in the number or frequency of requests.

Charging – firms cannot charge for fulfilling a data subject rights request; however, in exceptional and limited circumstances, firms can charge an administrative fee where the request is manifestly unfounded or excessive.

Cross-reference

See Article 13 for information on how to communicate with a Data Subject, in particular:

- *Nature of communication to Data Subject;*
- *Time limits to respond to Data Subject rights requests;*
- *Identifying the Data Subject;*
- *Extending the time limit to respond;*
- *Refusing to act on a request; and*
- *Charging.*

See Article 30 for information on the record of processing operations.

See Article 37 for information on the limited exemption to this Data Subject right.

Article 18 – Right to Erasure

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.

(6) Where erasure of Personal Data is not feasible for technical reasons, then the Data Controller need not comply with a request for erasure of the Personal Data under paragraph (1), where:

(A) The Data Controller collected the Personal Data from the Data Subject; and

(B) The information provided to the Data Subject under Article 14 was explicit, clear and prominent with respect to the manner of Processing the Personal Data and expressly stated that erasure of the Personal Data at the request of the Data Subject would not be feasible.

Often referred to as the 'right to be forgotten', this right is closely linked with Principle 5, storage limitation.

When is it applicable?

The right to erasure does not apply in every case: it does not apply when the Processing is based on a legal obligation to do so, it is in the public interest or when Processed by a QFC body performing its powers and functions.

Specifically, the right to erasure is applied when:

- The data are no longer needed;

The purpose for the Processing has passed, and there is no additional lawful purpose to Process the data.

- The data Subject has withdrawn their consent;

Where Processing is based on the consent of the data Subject and that consent is withdrawn and erasure requested, once there is no other lawful basis for the Processing, the data must be erased.

- The data Subject objects to the Processing;

Where the data Subject objects to Processing, per Article 19(1), that takes place on the legal bases of public interest (Article 10(1)(E)(i)) or legitimate interest (Article 10(1)(F)) and that objection is upheld, the firm must erase the data.

- The data have been unlawfully Processed;

This applies when it can be established the firm does not have a valid lawful basis to Process the Personal Data. Therefore, firms must carefully examine all their Processing activities to ensure they have a lawful basis to Process it and, if not, to ensure it is erased.

- Where the firm must delete data due to a legal obligation to do so.

Where a law or regulation mandates data to be retained for a specific period, when that period has elapsed, the firm no longer has a lawful basis for its Processing and must now delete the data.

There are limited exemptions to this right within the Regulations, primarily contained in Article 37 and applicable to QFC bodies when discharging their powers and functions.

Data Processors and other Data Controllers

Firms must ensure any Data Processors to whom they transfer Personal Data are included in any valid erasure request.

In addition, where the firm transfers any Personal Data to another Data Controller, they must take reasonable steps to inform that Data Controller of the Data Subject's request to have their Personal Data erased, this includes:

- Any links to the data;
- Copies of the data; and/or
- Replication of the data.
- In fulfilling this requirement, the firm may consider the cost and technology available when Processing the request.

Backups and contingency

Valid requests for erasure include all data held by the firm and will include Personal Data held on backup services.

Firms must ensure they have carefully considered how they will operationally apply erasure to all Personal Data they hold.

What is critical here will be what information is communicated to the Data Subject regarding the erasure of their data. For example, where data are deleted from 'live' systems without undue delay and within the 30-day time limit but retained on backup services for an extended period, firms must assess the risk of these backups and any additional retention times in place. This assessment may include reviewing where the data are held, who has access and the protocol for their recovery following an incident. The Data Protection Office will review each company's approach to erasure and backups on a case-by-case basis.

If erasure is not feasible

The Regulations provide an exemption from the requirements of Article 18 in situations where the erasure of data is not feasible, due to technical reasons. This is often due to the use of certain technologies, such as Distributed Ledger Technologies, where individual records are immutable. In order to rely on this this exemption, Data Controllers must be able to demonstrate that erasure of data that are no longer required is not feasible, and not merely difficult or costly.

In these instances, the Data Controller may us such technology provided the conditions outlined in Article 18(6) are satisfied, specifically:

- That the Personal Data is collected directly from the Data Subject, and not through a third party; and
- The Data Subject has been informed, in an explicit, clear and prominent way, through the Article 14 notice, that erasure will not be feasible.

When relying on this exemption, firms must explicitly inform Data Subjects about the limitations on their right to have their Personal Data erased before commencing any Processing activities. Firms will have to determine the best way to ensure that this information has been brought to the Data Subjects attention.

What qualifies as 'explicit, clear, and prominent' should be determined by the firm, considering the needs of its Data Subjects and the way it interacts and communicates with them. Information regarding this limitation should not be merely included amongst other Data Subject rights information in a manner that could dilute its importance. Instead, it should be presented in such a way as to ensure that it is immediately noticeable to Data Subjects. This may be achieve through the use of a pop-up notice or similar mechanism that requires Data Subjects to acknowledge having read and understood this limitation before they can proceed. This method guarantees that the notice is not only seen but also acknowledged.

Other things to note

Record-Keeping – firms should record when a Data Subject made a request and the outcome of the request including details of the information provided to them and when it was fulfilled.

Time limits to respond – Data Subject rights requests must be fulfilled within 30-days.

Extending the time limit – the 30-days can be extended by a further 60-days in limited and exceptional circumstance. See Article 13 for more information on how and when the time limit can be extended.

Refusing to act on a request – firms must always document circumstances where it refuses to act upon a Data Subject rights request, including when it relies on the exception provided in Article 18(6). Circumstances where the firm can refuse a request are limited. Including the exemption in Article 18(6), these circumstances are usually when the request is manifestly unfounded or excessive such as in the number or frequency of requests.

Charging – firms cannot charge for fulfilling a Data Subject rights request, however, in exceptional and limited circumstances firms can charge an administrative fee where the request is manifestly unfounded or excessive.

Cross-reference

See Article 13 for information on how to communicate with a Data Subject, in particular:

- *Nature of communication to Data Subject;*
- *Time limits to respond to Data Subject rights requests;*
- *Identifying the Data Subject;*
- *Extending the time limit to respond;*
- *Refusing to act on a request; and*
- *Charging.*

See Article 30 for information on the record of processing operations.

See Article 37 for information on the limited exemption to this Data Subject right.

Article 19 – Right to Object

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.

When is it applicable?

Like the right to erasure, the right to object does not apply in all cases; only to the Processing of Personal Data where the Processing is necessary:

- To perform a task carried out in the public interest (Article 10(1)(E)(i));
- For the Data Controller's, or another person's, legitimate interests Article 10(1)(F); and
- When their Personal Data are used for direct marketing.

Where the Processing is based on the lawful basis of legitimate interest, the firm must assess the Data Subject's objection in light of the 'balancing test'. This test is required when using this lawful basis. If the test indicates that the Data Subject's legitimate interests are not overridden by the firm's legitimates interests, then the object request can be refused. See the guidance in relation to Article 10 for more information on the 'balancing test'.

The Data Subject's objection can also be rejected when the firm is Processing Personal Data based on the lawful basis of necessity to establish, pursue or defend a legal claim.

There are limited exemptions to this right within the Regulations, primarily contained in Article 37 and applicable to QFC bodies when discharging their powers and functions.

Object to Marketing

Regardless of the lawful basis chosen by the firm for marketing purposes, where the Data Subject objects to their Personal Data being used for such purposes, the firm must stop Processing their data for that purpose without undue delay.

Restriction of Processing while reviewing the validating of the request

Where a firm has received an objection request, the firm must ensure the data are restricted, per Article 20, until they have completed their review of the validity of their legitimate interest in the Processing.

Informing the Data Subject

In conjunction with Articles 13, 14 & 15 and Rule 3, Data Subjects must be provided with information on their right to object not later than when the firm first communicates with them.

Other things to note

Record-Keeping – firms should record when a Data Subject made a request and the outcome of the request including details of the information provided to them and when it was fulfilled.

Time limits to respond – Data Subject rights requests must be fulfilled within 30-days.

Extending the time limit – the 30-days can be extended by a further 60-days in limited and exceptional circumstances. See Article 13 for more information on how and when the time limit can be extended.

Refusing to act on a request – there are limited and exceptional circumstances where the firm can refuse a request. These circumstances are usually when the request is manifestly unfounded or excessive such as in the number or frequency of requests.

Charging – firms cannot charge for fulfilling a Data Subject rights request; however, in exceptional and limited circumstances, firms can charge an administrative fee where the request is manifestly unfounded or excessive.

Cross-reference

See Article 10(1)(F) for information on the lawful basis of legitimate interest and the 'balancing test'.

See Article 11 for information on the lawful basis of consent and the conditions for a valid consent include the conditions that it must be as easy to withdraw as it was to provide.

See Article 13 for information on how to communicate with a Data Subject, in particular:

- *Nature of communication to Data Subject;*
- *Time limits to respond to Data Subject rights requests;*
- *Identifying the Data Subject;*
- *Extending the time limit to respond;*
- *Refusing to act on a request; and*
- *Charging.*

See Article 20 for information on right to the restriction of Processing, in particular where a Data Subject has objected to the Processing, the firm must restrict Processing of that data until such time as it has been validated.

See Article 37 for information on the limited exemption to this Data Subject right.

Article 20 – Right to Restriction of Processing

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.

When is it applicable?

The right to the restriction of Processing, similar to the rights to erasure and to object, does not apply in all circumstance, only where:

- The accuracy of the data are contested;

Where the Data Subject contests the accuracy of the data, the restriction remains in place until such time as the firm confirms or rejects the Data Subject's assertion. Where the Personal Data are found to be inaccurate, the Data Subject has the right to have it rectified per Article 17.

- The Processing is unlawful, and the Data Subject opposes the erasure;

This can arise where the Data Subject needs the data for other purposes, such as complaints, etc.

- The Data Subject requires the data for the establishment, exercise or defence of legal claims but is no longer needed by the firm;

The legal claim may or may not involve the firm; however, the restriction preserves the data for the benefit of the Data Subject.

- The Data Subject has objected to the Processing, and while the firm is verifying the validity of that request.

Personal Data are only restricted until the firm has completed its review of the validity of the Data Subject objection request.

There are limited exemptions to this right within the Regulations, primarily contained in Article 37 and applicable to QFC bodies when discharging their powers and functions.

How to restrict Processing

Given the definition of Processing under the Regulations, restricting data Processing can be a challenge for firms and how firms approach restriction will vary from firm to firm.

Firms should consider measures such as transferring the data to another system or restricting access to or making the data unavailable to users.

Firms can consider the availability and cost of technology when applying measures to restrict Processing of Personal Data following a valid request.

What can be done with restricted data?

Generally, the only Processing allowed on restricted data is storage. Firms can Process the data if:

- They have the consent of the Data Subject;
- They must protect the rights of another Person;
- They are establishing or defending a legal claim; or
- Tt is in the public interest.

Lifting the restriction

When the firm has determined the request to restrict Processing is invalid or if they have rectified Processing to the satisfaction of the Data Subject, they can recommence Processing once they have notified the Data Subject before doing so.

Other things to note

Record-Keeping – firms should record when a Data Subject made a request and the outcome of the request including details of the information provided to them and when it was fulfilled.

Time limits to respond – Data Subject rights requests must be fulfilled within 30-days.

Extending the time limit – the 30-days can be extended by a further 60-days in limited and exceptional circumstance. See Article 13 for more information on how and when the time limit can be extended.

Refusing to act on a request – there are limited and exceptional circumstances where the firm can refuse a request. These circumstances are usually when the request is manifestly unfounded or excessive such as in the number or frequency of requests.

Charging – firms cannot charge for fulfilling a Data Subject rights request, however, in exceptional and limited circumstances firms can charge an administrative fee where the request is manifestly unfounded or excessive.

Cross-reference

See Article 13 for information on how to communicate with a Data Subject, in particular:

- *Nature of communication to Data Subject;*
- *Time limits to respond to Data Subject rights requests;*
- *Identifying the Data Subject;*
- *Extending the time limit to respond;*
- *Refusing to act on a request; and*
- *Charging.*

See Article 37 for information on the limited exemption to this Data Subject right.

Article 21 – Right to data portability

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.

When is it applicable?

When is it applicable?

The right to data portability does not apply in all circumstances and only applies to Personal Data:

- Where Processing is based on consent or in accordance with a contract; and
- Processed electronically; therefore, any paper files are excluded from this right.

The firm must provide the Data Subject with the Personal Data they have provided in a structured, commonly used and machine-readable format. This means the firm must decide on the most suitable format, for example, as a comma-separated value or csv file.

Finally, the Data Subject has the right to have this information transferred to another Data Controller of their choice.

This right gives the Data Subject the ability to move service providers without providing their information again. It also protects them from business practices that use technology to lock them into one provider. Data Subjects can use their Personal Data to shop around for the best deals for services they want.

There are limited exemptions to this right within the Regulations, primarily contained in Article 37 and applicable to QFC bodies when discharging their powers and functions.

Personal Data which the Data Subject has provided

This right only applies to Personal Data provided by the Data Subject to the firm. For example, this could be information provided in an application form or through a website's sign-up page. However, it will also apply to information gathered directly from a Data Subject such as transaction history.

Limitations to the right

There are certain limitations to this right; for example, it is not applicable when Processing is in the public interest per

Article 10(1)(E)(i) or where the Processing is in the exercise of official authority vested in the Data Controller.

Finally, firms must ensure that by fulfilling a data portability request, they are not adversely affecting another person. This is especially true when there is a joint account or where Personal Data are intermingled with other Data Subjects' Personal Data.

Other things to note

Record-Keeping – firms should record when a Data Subject made a request and the outcome of the request including details of the information provided to them and when it was fulfilled.

Time limits to respond – Data Subject rights requests must be fulfilled within 30-days.

Extending the time limit – the 30-days can be extended by a further 60-days in limited and exceptional circumstances. See Article 13 for more information on how and when the time limit can be extended.

Refusing to act on a request – there are limited and exceptional circumstances where the firm can refuse a request. These circumstances are usually when the request is manifestly unfounded or excessive such as in the number or frequency of requests.

Charging – firms cannot charge for fulfilling a Data Subject rights request; however, in exceptional and limited circumstances, firms can charge an administrative fee where the request is manifestly unfounded or excessive.

Cross-reference

See Article 13 for information on how to communicate with a Data Subject, in particular:

- *Nature of communication to Data Subject;*
- *Time limits to respond to Data Subject rights requests;*
- *Identifying the Data Subject;*
- *Extending the time limit to respond;*
- *Refusing to act on a request; and*
- *Charging.*

See Article 37 for information on the limited exemption to this Data Subject right.

[5]UK GDPR - https://www.legislation.gov.uk/eur/2016/679/contents

Article 22 – Automated Individual Decision-Making, Including Profiling

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

When is it applicable?

Article 22 applies to all automated individual decision making, including profiling, which has a legal effect or would significantly affect the Data Subject. The Article places a prohibition on such Processing subject to the exclusions in Article 22(2).

The key provision here is to have a "legal effect on them or would otherwise significantly affect them". Therefore the prohibition is limited only to automated individual decision-making Processes, including profiling, that have a legal effect or other significant effect on Data Subjects. A legal effect is something that affects an individual's legal rights or has a serious impact on the individual. If a decision-making process does not have influence on individuals' legal rights, it may still produce an effect that is equivalent or significantly impacts individuals in a similar way. For the decision-making process to "significantly affect" individuals, it should have the potential to: (i) significantly affect the circumstances, behaviour or choices of the individuals concerned; (ii) have an extended or permanent impact on the individual; or (iii) lead to the exclusion or discrimination of individuals. Examples include decisions that affect someone's financial circumstances, such as their eligibility to obtain credit, or affects their access to health services, or decisions that deny someone an employment opportunity.

This means firms must assess any automated individual decision-making Processes, including profiling, to assess whether it meets these criteria. If the Processing meets these criteria and none of the exclusions apply, Processing cannot occur. However, if at least one of the exclusions apply, the Processing may proceed.

There are limited exemptions to this right within the Regulations, primarily contained in Article 37 and applicable to QFC bodies when discharging their powers and functions.

Automated decisions and profiling

Automated decisions are decisions made exclusively without the intervention or involvement of a human. Examples include a recruitment aptitude test which uses pre-programmed algorithms and criteria or an online process to award a financial loan.

Profiling, which tends to be automated, analyses aspects of an individual to predict their decisions, preferences and interest. The UK's GDPR1 defines profiling as meaning:

> *any form of automated Processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.*

Exemptions

The Regulations provide exemptions to the prohibition on automated individual decision making, including profiling, which has a legal or other significant effect on the Data Subject, namely:

- It is necessary to enter into or perform a contract;

The firm must demonstrate that Processing is necessary to enter into or perform the contract and not merely a condition of the contract.

- It is made pursuant to these Regulations; or

The Regulations can make provisions for specific automated individual decision making, including profiling, which has a legal or other significant effect on the Data Subject. Note – none are currently specified in the Regulations.

- The Data Subject has given their explicit written consent.

The consent must meet the conditions of valid consent under Article 11; that is it must be a freely given, specific, informed, and unambiguous indication that they agree to the Processing. In addition, the consent must be in writing.

What rights do Data Subjects have?

Where a firm has determined they undertake automated individual decision making, including profiling, which has a legal or other significant effect on the Data Subject and that one of the exemptions apply to the Processing, then the Data Subject has the following rights to:

- Obtain human intervention;
- Express their point of view; or
- Contest the decision.

Firms must have procedures in place to identify such a request and action it appropriately, including demonstrating they comply with the Principles and Regulations, per Articles 9 and 25. Specifically, firms must give the Data Subject a way in which they can exercise their rights.

Transparent information to the Data Subject

Firms are required to provide specific information to a Data Subject when collecting their Personal Data. Articles 14 & 15 and Rule 3 require specific information be provided to the Data Subject, such as the purpose of the Processing and the lawful basis.

Rule 3 states firms must provide Data Subjects with information on whether automated decision-making will be used, and if so:

- Meaningful information about the logic applied; and
- The significance, and the likely consequences, of the decision-making for the Data Subject.

The firm must inform Data Subjects of their rights concerning any automated individual decision making, including profiling, which has a legal or other significant effect on them and how to exercise their rights.

Use of Sensitive Personal Data

Where a firm wishes to use Sensitive Personal Data in automated individual decision making, including profiling, which has a legal or other significant effect on the Data Subject, then they can only do so when:

- They have obtained the explicit written consent of the Data Subject; or

The conditions for valid consent in Article 11 apply here, with the added requirement that the consent for Sensitive Personal Data Processing must be in writing.

- The Processing is necessary for substantial public interest.

This only relevant when the substantial public interest condition of Article 12 applies to the Processing of Sensitive Personal Data. See the relevant section of Article 12 for more information.

Other things to note

Record-Keeping – firms should record when a Data Subject made a request and the outcome of the request including details of the information provided to them and when it was fulfilled.

Time limits to respond – Data Subject rights requests must be fulfilled within 30-days.

Extending the time limit – the 30-days can be extended by a further 60-days in limited and exceptional circumstances. See Article 13 for more information on how and when the time limit can be extended.

Refusing to act on a request – there are limited and exceptional circumstances where the firm can refuse a request. These circumstances are usually when the request is manifestly unfounded or excessive such as in the number or frequency of requests.

Charging – firms cannot charge for fulfilling a Data Subject rights request; however, in exceptional and limited circumstances, firms can charge an administrative fee where the request is manifestly unfounded or excessive.

Cross-reference

See Article 9 and 25 for information on the accountability requirements of the Regulations.

See Article 11 for information on the lawful basis of consent and what constitutes a valid consent.

See Article 12 for information on the Processing of Sensitive Personal Data in particular the condition of substantial public interest.

See Article 13 for information on how to communicate with a Data Subject, in particular:

- *Nature of communication to Data Subject;*
- *Time limits to respond to Data Subject rights requests;*
- *Identifying the Data Subject;*
- *Extending the time limit to respond;*
- *Refusing to act on a request; and*
- *Charging.*

Articles 14 & 15 require firms to provide Data Subjects with information on how their Personal Data are Processed by the firm. With regards to automated individual decision making, including profiling, this information must include both meaningful information about the logic applied and the significance, and the likely consequences, of the automated decision-making for the Data Subject.

See Article 37 for information on the limited exemption to this Data Subject right.

Part 4

Transfers of Personal Data outside the QFC

Part 4 of the Regulations deals with the transfer of Personal Data to a jurisdiction outside the QFC, including the State of Qatar.

Article 23 provides for a list of adequate jurisdictions issued by the Data Protection Office, to which Personal Data can be transferred without additional steps.

Article 24 provides a number of transfer mechanisms to jurisdictions not included on the list of adequate jurisdictions.

Transfer Overview

Transfers of Personal Data outside the QFC are permitted once the jurisdiction to which the Personal Data are being transferred offers an adequate level of protection for that Personal Data. The QFC's Data Protection Office has published a list of adequate jurisdictions for this purpose.

The QFC Data Protection Office List of Adequate Jurisdictions can be downloaded from QFC/resource-centre/data-protection.

Where a jurisdiction is not on the list, firms may proceed with the transfer only where one of the conditions in Article 24 of the Regulations apply. Figure 1 provides an overview of the QFC data transfer process for jurisdictions not included on the list of adequate jurisdictions.

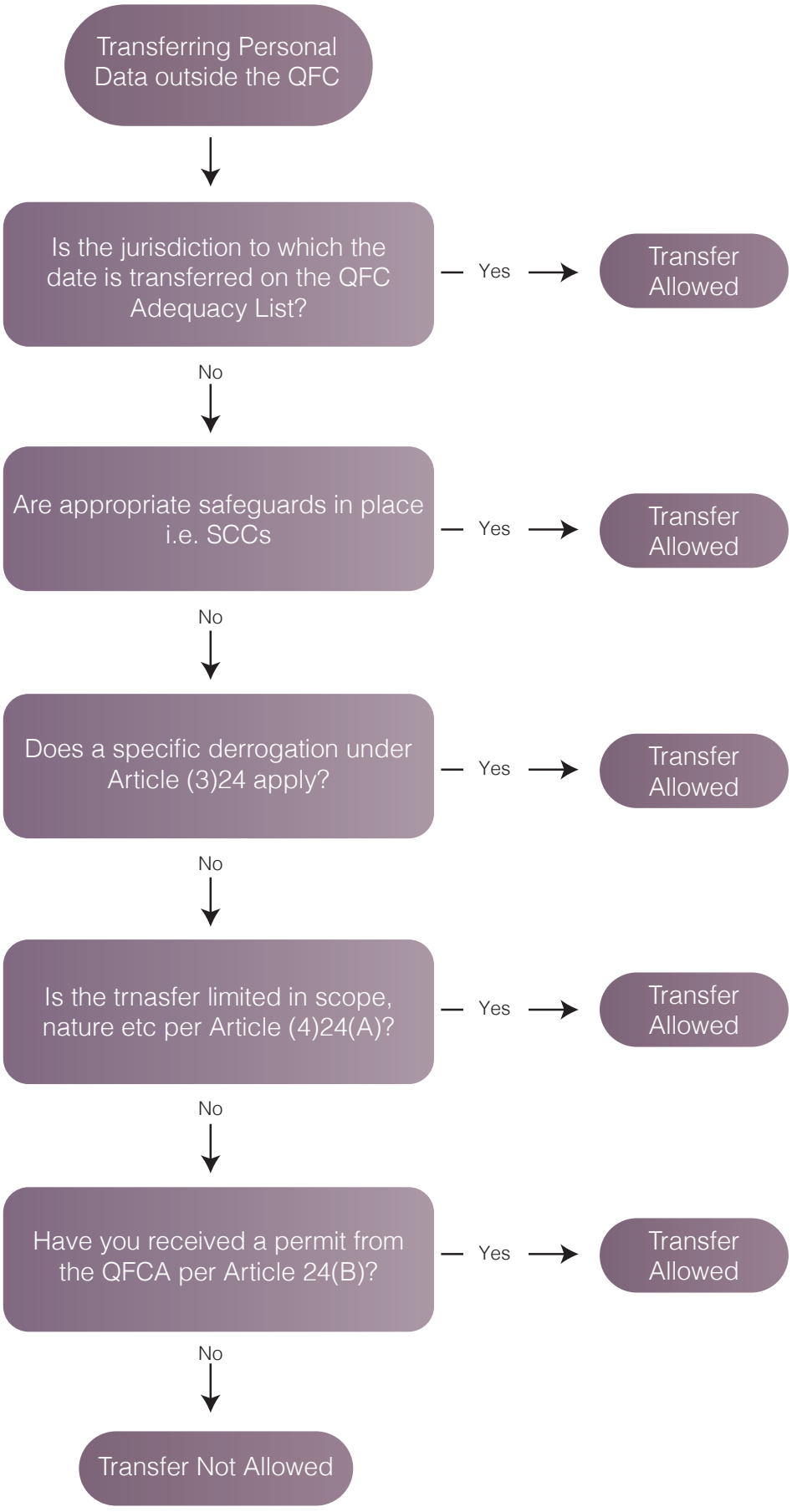


Figure 1. Data Transfer Flowchart

Article 23 – Transfers Out of the QFC: Adequate Level of Protection

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.

Transfers of Personal Data outside the QFC can only take place where the jurisdiction to which they are transferred offers an adequate level of protection compared to the QFC (and note that this also applies to any transfers outside the QFC to onshore Qatar).

Where a jurisdiction is on the list of adequate jurisdictions for data transfers, the firm can make the transfers without having to implement any specific measures. However, firms should still ensure that any third parties that receive and process personal data are doing so compliantly and securely, in order to protect such data.

Firms are encouraged to review the list of adequate jurisdictions to which they send Personal Data from time to time to ensure the Recipient jurisdiction remains on the list.

For cases when the Recipient jurisdiction is not on the list of adequate jurisdictions, please see Article 24 for more information.

The QFC Data Protection Office List of Adequate Jurisdictions can be downloaded from QFC/resource-centre/data-protection.

Note – If the transfer is to a Data Processor, the requirements in Article 28 and Rule 7 will also apply.

Example

A firm wishes to engage the services of a cloud service provider which has data servers located in Germany. Since the cloud service provider is processing Personal Data on the firm's behalf, it will be a Data Processor. Since the cloud service provider will have access to the Personal Data, held on its data servers in Germany, a data transfer will occur from QFC to Germany. The firm should check the list of adequate jurisdictions on the QFC's website. Germany is on the list of adequate jurisdictions; therefore, no additional steps are required to transfer the data.

It should be noted that the requirements for engaging a Data Processor, such as a requirement to have a written contract in place, still apply.

Cross-reference

See Article 28 for the requirements when appointing a Data Processor and Rule 7 on what, as a minimum, must be included in the data processing agreement.

See Article 24 for more information on sending Personal Data to a jurisdiction that is not on the list of adequate jurisdictions.

Article 24 – Transfers out of the QFC: Absence of an adequate level of protection

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;*
- *(C) The limited circumstances in paragraph (4) apply; or*
- *(D) The transfer is based on an approved transfer mechanism as set out in paragraph (6).*

(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).

(6) The approved transfer mechanisms referred to in paragraph (1)(D) are the following:

(A) Binding Corporate Rules that fulfil the requirements set out in the Data Protection Rules and have been approved by the Data Protection Office; or

(B) Another internationally acceptable transfer mechanism approved by the Data Protection Office.

QFC Data Protection Rules

5. TRANSFERS OF PERSONAL DATA OUT OF THE QFC

1. 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.

2. BINDING CORPORATE RULES

For the purposes of Article 24 of the Regulations, the Data Protection Office may approve Binding Corporate Rules for transfers of Personal Data outside the QFC subject to the following conditions:

Such Rules must specify at least:

(A) The structure and contact details of the relevant Group and of each of its members;

(B) The types of data transfers to be covered by the Rules, including:

(I) The categories of Personal Data that would be covered;

(II) The type of Processing that would be covered, and its purposes;

(III) The type of Data Subjects that may be affected; and

(IV) The identification of the relevant jurisdiction(s) outside of the QFC in relation to which the Rules may apply

(C) Their legally binding nature, both internally and externally;

(D) The application of the general data protection principles, including:

- *(i) Purpose limitation;*
- *(ii) Data minimisation;*
- *(iii) Limited storage periods;*
- *(iv) Data quality;*
- *(v) Data protection by design and by default;*
- *(vi) Legal basis for Processing;*
- *(vii) Processing of Special Categories of Personal Data;*
- *(viii) Measures to ensure data security; and*
- *(ix) The requirements in respect of onward transfers to bodies not bound by the Binding Corporate Rules;*

(E) The rights of Data Subjects and the means to exercise those rights, including the right to obtain redress and, where appropriate, compensation for a breach of the Binding Corporate Rules;

(F) How the information on the Binding Corporate Rules, in particular on the provisions referred to in paragraph (D) and (E), are to be provided to the Data Subjects in addition to the information required by Articles 13, 14 and 15 of the Regulations;

(G) The responsibility of any person or entity within the Group in charge of monitoring compliance with the Binding Corporate Rules;

(H) The complaint procedures;

(I) The mechanisms within the Group for monitoring compliance with the Binding Corporate Rules and cooperating with the Data Protection Office to ensure compliance, such mechanisms to include at a minimum:

- *(i) Data protection audits and methods for ensuring corrective actions to protect the rights of Data Subjects; and*
- *(ii) Communication of the results of such monitoring activity to the board of the parent company of a Group and, upon request, to the Data Protection Office;*

(J) The procedures for reporting and recording changes to the rules and reporting those changes to the Data Protection Office;

(K) The reporting mechanisms for notifying the Data Protection Office of any legal requirements to which a member of the Group is subject outside the QFC and which are likely to have a substantial adverse effect on the protections provided by the Binding Corporate Rules; and

(L) The data protection training provided to personnel with permanent or regular access to Personal Data.

Article 24 provides details on when a Data Controller may transfer Personal Data to a jurisdiction outside the QFC that the Data Protection Office has not granted adequacy status under Article 23.

This Article provides three (3) scenarios when such transfers are permitted; these are:

(1) Appropriate Safeguards under paragraph (2);

(2) Specific Derogations under paragraph (3);

(3) Limited Circumstance under paragraph (4); and

(4) The transfer is based on

Appropriate Safeguards

Transfers using appropriate safeguards are permitted for:

(1) Public authorities, such as the QFCA; and

(2) All other firms when using standard contractual clauses.

Where a public authority has a legally binding and enforceable agreement to transfer Personal Data to another such body, the transfer can occur without further steps.

For other firms, there must be a legally binding and enforceable agreement, such as a contract, and that agreement must contain the standard contractual clauses adopted and issued by the Data Protection Office.

Standard Contractual Clauses issued by the QFC Data Protection Office

The QFC Data Protection Office has issued a set of standard contractual clauses (SCC's) to ensure appropriate safeguards are in place between the parties involved in the transfer of Personal Data. The SCCs are designed to provide appropriate safeguards for the Personal Data, and, therefore, Data Subjects whose data are being transferred. The SCCs should ensure the level of protection applied to the Personal Data are essentially equivalent to that provided through the QFC's Data Protection Regulations.

The role of SCCs is to ensure appropriate data protection safeguards for international data transfers are in place between the parties.

Therefore, the Data Controller or Processor transferring Personal Data to a third country (the 'data exporter') and the Data Controller or Processor receiving the Personal Data (the 'data importer') are free to include those SCCs in a wider contract. The parties can add other clauses or additional safeguards, provided they do not contradict, directly or indirectly, with the SCCs or prejudice the fundamental rights or legitimate interests of Data Subjects.

The SCCs combine general clauses to cater for the following transfer scenarios;

(1) Data Controller to Data Controller;

(2) Data Controller to Data Processor; and

(3) Data Processor to Data Processor.

More than two parties can adhere to the SCCs, and other controllers and processors should be able to accede to the clauses if and when required.

As with all contracts, firms must ensure they have appropriate and effective mechanisms to ensure compliance with the relevant clauses.

A copy of the QFC Standard Contractual Clauses can be downloaded from QFC/resource-centre/data-protection.

Speci ic Derogations

Where a transfer cannot be based on an adequacy decision and where there are no SCCs in place on which to base the transfer, then firms can only transfer when one of the following applies:

- On the explicit consent of the Data Subject;
- On the performance of a contract between the Data Subject and firm;
- On the performance of a contract in the interest of the Data Subject;
- When necessary to comply with a legal obligation;
- When necessary to protect the vital interests of an individual;
- When necessary to perform a task carried out in the public interest;
- When necessary for a QFC body to perform its functions and powers;
- When necessary for the establishment, exercise or defence of a legal claim.

Limited Circumstance

Where a transfer cannot be based on an adequacy decision, or there are no SCCs in place, or where none of the specific derogations apply, then firms can only make the transfer when:

- Is not repeating or not part of a repetitive course of transfers;
- It concerns only a limited number of Data Subjects;
- It does not contain any Sensitive Personal Data;
- It is for the legitimate interests of the firm; and
- An assessment of the circumstances surrounding the data transfer has taken place, and there are suitable safeguards in place to protect the Personal Data.

Note – each one of these conditions must be met. As with all aspects of the Regulations, the firm should fully document how and when these limited circumstances are used for a data transfer.

Permit from the QFCA

Finally, where none of the other options for a data transfer are appropriate, the firm can apply to the Data Protection Office for a permit to transfer the data. The permit application process is available on the Client Portal and further information about the permit application is available in Rule 5.

Approved transfer mechanism

The Regulations allow for transfers to take place via an approved transfer mechanism, including via a set of Binding Corporate Rules ("BCRs") approved by the Data Protection Office.

BCRs are Personal Data protection policies which are adhered to by a Data Controller or Data Processor for transfers or a set of transfers of Personal Data to a Data Controller or Data Processor within a Group. In other words, BCRs are strict privacy policies followed by a firm when transferring Personal Data within its own group of companies. These rules ensure that Personal Data is protected and managed consistently across all entities within the group.

For a Firm to rely on BCRs as a valid transfer mechanism, these must first be approved by the Data Protection Office prior to any Personal Data transfers taking place. Rule 5.2 set outs what must be included in an application to the Data Protection Office for approval of BCRs. Key aspects of the BCR application process include providing information on:

- Transparency requirements, including informing Data Subjects of their rights and how they can enforce them;
- Monitoring compliance with the Binding Corporate Rules, and how the results of this monitoring are presented to the Board of parent company and to the Data Protection Office, on request;
- That there is a procedure in place to allow Data Subjects to raise complaints on how their data are Processed; and
- Ensuring personnel permanent or regular access to Personal Data are adequately trained.

The Data Protection Office also has the power to approve additional transfer mechanisms. Firms should continue to check QFC/resource-centre/data-protection for more information on approved mechanisms for international transfers of Personal Data.

If a firm would like to apply for approval of its binding corporate rules, they could contact the Data Protection Office at dataprotection@qfc.qa.

Part 5

Data Controller and Data Processor Obligations

Part 5 of the Regulations provides detail on the responsibilities placed on both Data Controllers and Data Processors when Processing Personal Data.

This part of the guidance covers Rules 6-9 and the following Articles of the Regulations:

- Article 25 – Responsibility of the Data Controller;
- Article 26 – Data protection by Design and by Default;
- Article 27 – Data protection impact assessment;
- Article 28 – Data Processors;
- Article 29 – Security of Processing;
- Article 30 – Record of Processing operations;
- Article 31 – Notification of Personal Data Breaches.

Article 25 – Responsibility of the Data Controller

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.

This Article places responsibility on Data Controllers to put in place the systems and controls necessary to demonstrate compliance with the Regulations. This obligation, along with Article 9, is often referred to as 'accountability' and mandates that firms must put in place appropriate and effective, and technical and organisational, measures to be able to demonstrate compliance with the Regulations.

Appropriate and effective

'Appropriate' means the measures must be the right measures to be able to demonstrate compliance with Regulations.

'Effective' is focused on the actual outcome of the measure and their ability to comply with the Regulations.

Example

A firm puts in place a policy, supported by procedures, to ensure that Data Subjects who no longer wish to receive marketing information are removed from the marketing list without undue delay. If correctly performed the procedure will ensure no Data Subject who withdraws their consent will receive marketing information. However, upon checking the effectiveness of this process, the firm discovers that withdrawal requests sent to 'info@' mailbox are not being actioned, per the policy.

In this case, the process is adequate and would ensure the Regulations are complied with; however, it is ineffective as the process is not functioning as designed.

Technical and organisational

Firms are required to include both technical and organisational measures to demonstrate compliance with the Regulations.

Technical measures include:

- Access control;
- Network security, including vulnerability assessments;
- Encryption;
- Anonymisation and de-identification;
- Data transfer controls, etc.

Organisational measures include:

- Risk assessments;
- Data protection and information security policies and procedures;
- Incident management;
- Business resilience;
- Training;
- Audits and system logs, etc.

Testing and Reporting

Measures to demonstrate the effectiveness of the technical and organisational measures must be in place. Firms can achieve this through a clear testing and reporting framework.

Testing processes to ensure they are achieving the desired outcome will not only ensure firms are demonstrating compliance with the Regulations but also help them identify efficiencies within processes.

Reporting the results of testing to senior management and the board demonstrates that compliance with the Regulations is important to the firm and allows management to take corrective actions where necessary.

Cross-reference

See Article 26 for information on data protection by design and by default and Article 27 for information on data protection impact assessments. By complying with both of these Articles, firms will have gone a long way to demonstrating compliance with the Regulations.

Article 26 – Data Protection by Design and by Default

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: are not made accessible (without the Data Subject's intervention) to an indefinite number of Recipients; and

(A) Are made accessible only to individuals who, for their role, function or task, need to Process those Personal Data.

(B) Are made accessible only to individuals who, for their role, function or task, need to Process those Personal Data.

Data protection by design and by default are essential requirements to ensure firms are implementing adequate and effective organisational and technical measures to:

- Comply with the Regulations;
- Comply with the Principles;
- Ensure the Personal Data are protected against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access; and
- Protect the Personal Data from other forms of unlawful Processing.

Data protection by design

The Regulations require firms to consider data protection at both the time of determining the means for Processing and the time of the Processing itself. This is not a new concept in data protection, but with the 2021 Regulations, it is now an explicit requirement for firms. It is linked to the accountability principle and obligations in the Regulations.

When firms start to design and develop new processes, products and services which Process Personal Data, they need to ensure data are protected and these Regulations are considered from the start. This includes ensuring they have appropriate and effective organisational and technical controls to ensure compliance with the Regulations and that Personal Data are held securely and protected against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access. Firms should integrate data protection and the requirements under the Regulations into their Processing activities and business practices, from the design stage of any system, service, product or process and throughout the lifecycle.

Although not a definitive list, data protection by design applies to:

- New products offerings or variations;
- Using Personal Data for new purposes;
- New services or ways of Processing Personal Data, such as data sharing initiatives;
- Developing organisational policies and strategies that may have privacy implications; or
- New technology that involve the Processing of Personal Data such as:
    - New IT platforms;
    - New online portals or mobile applications'
    - Cloud migration.

It is important firms not only focus on the IT elements but consider all aspects of the Processing, whether electronic or physical.

Finally, data protection by design goes further than just processes and should be something that becomes part of the culture of the firm. When privacy is considered at all stages of the firm's Personal Data Processing lifecycle demonstrating compliance with the Regulations and ensuring the Personal Data are protected is more straightforward.

Data protection by default

This part of the Article focuses on ensuring only Personal Data necessary for each specific purpose are Processed. This is linked to Principle 2 on specific purpose and Principle 3 on data minimisation in Article 8.

This provision ensures firms adopt the appropriate data protection standards suitable to the Processing. These measures must ensure that by default, Personal Data are:

- Only accessible to those who need access for their roles; and
- Not accessible by everyone without some form of intervention by the Data Subject.

Firms must understand what data are required for a role and limit access only to the required data.

For example, firms may consider:

- Providing individuals with sufficient controls and options to exercise their rights;
- Ensuring systems and applications adopt a "privacy-first" approach by default (i.e. configuring the privacy settings in the strictest mode); and
- Not Processing additional data or sharing such data with new third parties unless the Data Subject has consented.

Cross-reference

Firms should consider this Article in light of:

- *Article 9 for responsibility for compliance with the Regulations;*
- *Article 25 for the responsibility of the Data Controller;*
- *Article 26 for information on the data protection by design and by default,*
- *Article 27 for information on data protection impact assessment and*
- *Article 29 for security of Processing.*

By complying with these Articles, firms will have gone a long way to demonstrating compliance with the Regulations.

Article 27 – Data protection impact assessment

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

(3) 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.

(4) The Data Protection Office may establish and make public a non-exhaustive list of the Processing operations which require a data protection impact assessment.

(5) A single assessment may address a set of similar Processing operations that present similar risks.

(6) 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.

QFC Data Protection Rules

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.

The Regulations require firms to undertake a data protection impact assessment ("DPIA") for any 'high risk' Processing.

The goal of the assessment is to:

- Understand the purpose of the Processing;
- Ensure the Personal Data used is compliant with the Principles in Article 8;
- Ensure there is appropriate security in place to protect the data against accidental or unlawful destruction, loss, Alteration, unauthorised disclosure of, or access; and
- Understand the risks to the rights and legitimate interest of the Data Subject due to the Processing, and ensure those risks are sufficiently mitigated.

The DPIA is a living document about a Processing operation and should be reviewed regularly to ensure it is still reflective of the Processing.

When is a DPIA Required?

High risk Processing

A DPIA is required when the Personal Data Processing presents a high risk to the rights and legitimate interests of Data Subjects.

As a first step, firms must have a way to assess the risk of their proposed Processing on those whose data they will be Processing.

This might involve assessing if the Personal Data Processing:

- Is on a large scale, taking into account:
  - The number of Data Subjects involved or projected to be involved;
  - The categories and amount of Personal Data captured;
  - The time frame to retain data; and
  - The geographical scope of processing;
- Evaluates or scores individuals, including profiling and predicting behaviour;
- Involves systematic monitoring e.g. using technology to observe, monitor or control data subjects;
- Matches or combines datasets, especially when the purpose of the datasets was different;
- Concerns vulnerable data subjects, such as children;
- Involves innovative use or applying new technological or organisational solutions;
- Prevents data subjects from exercising a right or using a service or a contract;
- Is based on specific lawful basis e.g. based on consent or legitimate interest;
- Lead to a Personal Data Breach, what would be the potential effect on Data Subjects?

Before Processing

Firms must complete the DPIA before the Processing takes place. This is to ensure the rights and legitimate interests of Data Subjects are managed sufficiently. It also aligns with the privacy by design requirements in Article 26.

This Article requires firms to ensure they integrate necessary safeguards into the Processing to meet the requirements of these Regulations. These safeguards are required when the means for Processing are determined and at the time of the Processing itself.

Firms may not have all the information or designed all procedures for a process before its commencement. This should not be seen as a reason to delay completing the DPIA, and the firm should complete it with all available information before Processing has commenced. Firms should review the Processing when it commences to either fill in any gaps in the original DPIA or affirm it is operating as expected.

Finally, the DPIA should be reviewed at regular intervals or after certain trigger events to ensure Processing is still carried out as envisaged and no new risks to the rights and legitimate interests of Data Subjects have materialised.

Cross-reference

This should be read in conjunction with Articles 8, 9 and 26 of the Regulations.

Article 27(2) provides examples when a processing operation is considered “high risk Processing”. Note that the words “in particular” in the introductory sentence of this Article 27(2) indicate that this is not an exhaustive list. Firms therefore should assess the risks involving their proposed Processing and determine whether it could be considered as “high risk Processing”.

Automated Processing, including Profiling, which leads to decisions that significantly affect the Data Subject

The focus on this type of Processing is around the words ‘which leads to decisions that significantly affect the Data Subject’. Therefore, the DPIA is required only when the automated Processing significantly affects the Data Subject. Firms should consider whether the decision made by the automated Processing significantly affects the circumstances, behaviour or choices of the Data Subjects; whether it would have a prolonged or permanent impact on the Data Subject; or whether it could lead to exclusion or discrimination of the Data Subjects. Decisions may “significant” where they: (i) affect someone’s financial circumstances; or (ii) deny someone an employment opportunity or put them in a serious disadvantage.

Examples of automated Processing that may significantly affect Data Subjects include: the automatic refusal of an online credit application, determining a job applicant’s suitability for a role by way of automated recruitment tests (i.e.

e-recruiting practices without any human intervention), or an online evaluation of an employee's performance without human intervention.

Cross-reference

See Article 39 for the definition of Sensitive Personal Data.

Large scale Processing of Sensitive Personal Data

Processing on a large scale that involves Sensitive Personal Data requires a DPIA. This is because of the special nature of this data and that accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Sensitive Personal Data could harm the Data Subject.

When determining whether the processing is carried out on a large scale, firms should consider the following factors:

- The number of Data Subjects concerned;
- The volume of Sensitive Personal Data being processed; and
- The duration of the Processing activity.

Cross-reference

See Article 39 for the definition of Sensitive Personal Data.

Systematic monitoring of a publicly accessible area on a large scale

This applies to large scale monitoring of public spaces by, for example, CCTV. Given the amount of Personal Data captured by this type of monitoring, it is very intrusive and requires a DPIA. This type of Processing may involve collecting Personal Data from individuals who are not aware they are being monitored or how that data will be used.

As prescribed by the Data Protection Office

Per under Article 27(3), the Data Protection Office has determined, and published, that the following Processing activities require a Data Controller to undertake a DPIA prior to Processing:

1. Evaluation or scoring, including Profiling and predicting: This includes various applications, such as assessing credit references, using health questionnaires for insurance evaluations, and creating behavioural marketing profiles based on user attributes and browsing history.

2. Biometric Data Processing: The Processing of biometric data for the purpose of uniquely identifying an individual, in particular when combined with any other Processing Activity listed here.

3. Genetic Data Processing: Any Processing of genetic data, other than that Processed by doctor or health professional for the provision of health care direct to the Data Subject.

4. Combining or matching Datasets: Combining, comparing or matching Personal Data obtained from multiple sources, particularly those combined where the purpose of the original collection is different or where the Data Subject would not expect them to be combined.

5. Processing the Personal Data of vulnerable Data Subjects or children: Processing involving vulnerable segments of the population requiring special protection, including, by way of example, children and elderly people, those with certain medical conditions, and those who are socioeconomically disadvantaged. This includes the Processing of children's data, and in particular automated decisions, profiling and marketing to children.

6. Processing using innovative technological or existing technologies in a new way: Processing of Personal Data using innovative technologies or using existing technologies in a new way. This includes the use of Distributed Ledger Technologies, Artificial Intelligence, Machine Learning, Large Language Models or other such technology.

7. Tracking including geolocation: Processing which involves tracking an individual's geolocation or behaviour, including in the online environment.

8. Invisible Processing: Where the Personal Data are not sourced directly from the Data Subject and where transparency requirements are not being met, including when relying on exemptions based on impossibility or disproportionate effort.

9. Risk of physical harm: where the Processing is of such a nature that a personal data breach could jeopardise the [physical] health or safety of individuals.

The list has been made available to via the QFC website.

Firms should carefully examine any new or updates to existing Processing activities to see if they fit into any of these categories or where they pose a High Risk to the rights and legitimate interests of Data Subjects.

What should be included in the DPIA?

Rule 6 provides a list of the criteria that must be included in the DPIA. However, firms are advised to consider all impacts affecting Data Subjects.

A systematic description of the envisaged Processing operations and the purposes of the Processing

1. Firms must provide a systematic description of the Processing and its purpose.

The purpose of the processes is a description of the 'why' of the Processing. This should focus on the Processing outcomes and what they are designed to achieve.

The systematic description of the Processing is a description of the 'how' of the Processing operation. This should be an operational description and provide a high-level understanding of the Processing.

2. When Processing is based on legitimate interest or consent as the lawful basis.

Legitimate Interest – where this is the lawful basis, the rationale as to why the firm believes their interest does not override the rights and legitimate interests of the Data Subject needs to be stated. This is referred to as the 'balancing test' and more information can be found in Article 10(1)(F) and guidance on the same above.

Consent - where this is the lawful basis, the DPIA must include:

- How the firm has ensured that the consent obtained is valid per Article 11;
- What the impact, if any, might be on the Data Subject if they withdraw consent; and
- How the firm ensures the Data Subject can easily withdraw their consent.

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

This requirement ties directly back to Principle 3 described in Article 8. Firms must demonstrate how the Personal Data they are collecting meet these three criteria of adequate, relevant and limited to what is necessary. This means:

- Adequate – the data collected should be sufficient to meet the purpose of the Processing;
- Relevant – the data has a direct link to that purpose; and
- Limited to what is necessary – the data collected should not exceed the minimum needed to meet the stated purpose.

An assessment of the risks to the rights and legitimate interests of Data Subjects

This is a more general description of all the risks to the rights and legitimate interest associated with the Processing and not just focused on legitimate interest. All Processing of Personal Data will present some risks to the Data Subject; firms must demonstrate they have identified and considered these risks as part of the DPIA.

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

Finally, firms must show how the risks identified are mitigated and any residual risks to the Data Subject have taken into account their rights and legitimate interests. Here firms should consider the security measures, both technical and organisational, they are putting in place and their ability to secure the data when assessing the residual risk to Data Subjects.

Example

Title: *Payroll Processing*

Description of the Processing*: Calculating and paying working time, overtime, bonus and commissions payments. The data are taken from the time management system, overtime forms, and sales entered into the sales system. The data are transferred to a third party (i.e. designated bank) to make the payment.*

Description of the Purpose of Processing: *Payment of benefits, grants and loans administration.*

Adequate, relevant and limited to what is necessary: *Only up-to-date mandatory data from the time management system, overtime forms and the sales system are Processed for this purpose. No other data is collected or processed.*

Risks of Processing: *Payment data of employees / contractors may be viewed as sensitive to Data Subjects, particularly if breached and exposed to third parties or to other employees within the firm. If the payment data is used for the wrong purpose or subject to a breach caused, for example, by the third party Processing the payments (i.e. the bank), this could expose important financial information about the Data Subjects and lead to misuse of their data.*

Risk mitigation options: *Limiting access to the payment data on a need-to-know basis; entering into a data processing agreement with the third party payment processor; and implementing robust security measures such as encryption and firewalls.*

Cross-reference

See Article 8 for information on the six principles of data protection.

See Article 10(1)(F) for information on the lawful basis of legitimate interest and the requirement for a 'balancing test'.

See Article 11 for information on the valid use of consent as a lawful basis.

See Article 30 for information on the record of processing as this information will be similar, if not the same, as the information in this record.

Good practices

Firms should have a robust process in place for completing the DPIA. This should include:

- Clear policies and procedures to carry out the DPIA, including the creation, sign-off, review and testing of the DPIA;
- Defined roles and responsibilities, including who signs off on the DPIA when they are completed;
- The role Data Processors play in contributing to the completion of the DPIA; and
- How and when the firm might consult with different stakeholders, including customers, employees, industry bodies and the Data Protection Office.

A DPIA may cover a single Processing operation or a group of similar Processing operations that present similar risks. This may be the case, for example, where similar technology is used to collect the same data for the same purpose.

Example

A firm has multiple premises and uses the same video surveillance systems for all its premises. The firm can conduct one DPIA for the use of the video surveillance system for all its premises.

Article 28 – Data Processors

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.

QFC Data Protection Rules

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.

The Regulations have placed specific requirements on Data Processors directly and on Data Controllers when engaging a Data Processor.

A mandatory requirement under the Regulations is to have a written contract in place between the Data Controller and the Data Processor, often referred to as a data processing agreement. Having a contract in place demonstrates compliance with the Regulations and serves as a clear instruction and description of what is expected by both parties.

Example

A firm hires a hosting service provider to store encrypted data on the provider's servers. The provider only stores the Personal Data on its servers: it does not determine what data to host nor how to process the data. The firm provides instructions to the provider on what data to store on the servers and the technical and organisational security measures that are required. The firm enters into a data processing agreement with the provider which includes the minimum obligations set out in Rule 7, including assisting the firm in ensuring that the necessary security measures are taken and notifying the firm in case of a breach to the servers that affects the personal data (i.e. a Personal Data Breach).

Responsibilities of the Data Controller when engaging a Data Processor

When a Data Controller is engaging a Data Processor to Process Personal Data on their behalf, they must:

- Choose a Data Processor who can provide sufficient guarantees to implement technical and organisational measures to comply with these Regulations; and
- Enter into a written contract with the Data Processor.

A Data Controller can demonstrate that the Data Processor provides sufficient guarantees through a combination of due diligence undertaken on the Data Processor, for example:

- By conducting a data protection impact assessment;
- By including the necessary clauses in the data processing agreement; and
- Through ongoing monitoring of the contract and the Data Processor's compliance with the obligations set out in the contract.

The key here is that the Data Controller is satisfied that the Data Processor can and does protect the Personal Data and complies with the Regulations.

What must be included in the contract between Data Controller and Data Processor

Rule 7 specifies what, at a minimum, must be included in the contract between the Data Controller and the Data Processor; these are:

- The subject matter and duration of the Processing;
- The nature and purpose of the Processing;
- The type of Personal Data and categories of Data Subjects;
- The obligations and rights of the Data Controller.

The contract must also set out that the Data Processor 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;
- Ensure only persons authorised to Process the data have undertaken to maintain its confidentiality or are under an appropriate statutory obligation of confidentiality;
- Take all the security measures required by Article 29 (Security of Processing) of the Regulations. See the guidance on Article 29 and the relevant section below for more information on this requirement;
- Not engage a sub-processor without the Data Controllers' written approval;
- Inform the Data Controller if an instruction will breach the Regulations;
- Assist the Data Controller to fulfil their obligations when responding to Data Subject rights requests;
- Assist the Data Controller to comply with the Data Controller's obligations under:
    - Article 27 – Data protection impact assessment;
    - Article 29 – Security of Processing; and
    - Article 31 – Notification of Personal Data Breaches.

The contract must include measures that compel Data Processors to delete or return Personal Data relating to the service per the Data Controllers› instructions. In addition, the Data Processor should retain no Personal Data relating to the service unless compelled by law.

Data Processors must make all information available to the Data Controller to show the Data Processor has complied with the obligations laid down in the Regulations. This might include security standards to protect data and any related internal or external audit results.

Finally, Data Processors must allow for and assist with audits and inspections by the Data Controller or an auditor appointed by the Data Controller.

Security of Processing

The contract between the Data Controller and Data Processor must include a requirement for the Data Processor to comply with Article 29 of the Regulations (Security of Processing).

Responsibilities of the Data Processor

The Regulations place specific obligations on Data Processors, given their important role in Processing Personal Data on behalf of Data Controllers. This mirrors the obligations required for the contract between the Data Controller and the Data Processor.

These obligations mean if a Data Processor were to breach one or more of the provisions, they would be liable both to the Data Controller via the contract and to the QFC under the Regulations.

The responsibilities of Data Processors are:

- They must not Process Personal Data except where:
  - Instructed to do so by a Data Controller with whom they have a written contract;
  - They must do so under a law or regulation which applies to the data and they have informed the Data Controller before doing so; or
  - Where they are instructed to do so by the Data Protection Office;
- They must notify the Data Controller if their instructions contravene the Regulations or any other legal requirement; and
- They have written authorisation to engage a sub-processor. Where authorisation is provided, the Data Processor must have a written contract in place with the sub-processor and must include the same responsibilities on the sub-processor as the Data Controller placed on them. In this case, the lead Data Processor remains fully liable to the Data Controller for the performance of the sub-processor's obligations.

Data Processors should be careful to ensure they are only acting as a Data Processor and not determining the purpose and means of the Processing. The Regulations make it clear if a Data Processor determines the purpose of means of Processing, they will be held to be a Data Controller for that Processing. Where this is the case, they will be responsible for ensuring full compliance with the Regulations for such Processing as a Data Controller.

Data Processors and Article 30 Records of Processing Operations

In addition to the requirement set forth in this Article, Data Processor must have in place and maintain a record of processing operations for those processes they undertake for a Data Controller.

This record should clarify who is the Data Controller for the Processing operations. This is important when the Data Processor processes Personal Data on behalf of a number of different Data Controllers.

Much, if not all, of the information required to meet this obligation will be included in the data processing agreement (contract) between the Data Controller and the Data Processor.

As noted in the guidance for Article 30 below, firms that are Data Processors for a Data Controller may be a Data Controller with respect to their internal processes, such as those in Finance, Human Relations (i.e. the Data Processor will Process the Personal Data of its employees as a Data Controller) and Marketing.

Cross-reference

See Article 25 for more information on determining the purpose and means of Processing and Data Controllers obligations.

See Article 30(2) for more information on what must be included in a record of processing operations.

Article 29 – Security of 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.

Keeping Personal Data secure is critical when complying with the Regulations, particularly Principle 6 regarding the integrity and confidentiality of Processing, and building trust with customers, employees and other stakeholders. Depending on the type of Personal Data Processed by a firm, Data Subjects are exposed to various risks, including, at the high end: identity theft, targeted fraud, intimidation and blackmail; and at the lower end of the scale: embracement or inconvenience.

This Article makes it mandatory for firms to implement technical and organisational measures to ensure that an appropriate level of security for the Personal Data they Process is maintained. This applies when a Data Controller uses a Data Processor as part of their Processing.

When the appropriate level of security is mentioned, this means appropriate to ensure Personal Data are protected from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data. To decide on an appropriate level of security, firms will need to understand the data they Process and the risks inherent in that Processing to Data Subjects.

Measures to ensure an appropriate level of security

The measure described below should be read in conjunction with Article 29(2), which is explained in more detail below. When deciding which measures to put in place, firms can consider the available technology at the time and the cost of implementation of such technology. This means the measures should be suitable to manage the risk whilst weighted against what is available and what it costs to secure the data.

De-identification of the Personal Data

De-identification is defined by the Regulations as

> *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.*

This means where data can identify an individual, those elements which can easily identify the individual, such as name, are replaced by a reference, dummy or holding data. The resulting data becomes comprised of information that no longer directly identifies the individual. However, it does not mean it is impossible to combine the data with other information to identify the individual, so it is still classified as Personal Data under the Regulations.

De-identification is the same practice as 'pseudonymisation' within other international data protection legislation such as the EU's GDPR.

Encryption of the Personal Data

Encryption is the Processing of encoding data using a mathematical formula so only authorised users have access to it. Without the ability to unencrypt the data, it is essentially useless to any unauthorised users who might gain access to it. However, encrypted data remains Personal Data under the Regulations.

The encryption of Personal Data is seen as a key tool to ensuring the confidentiality of the data is maintained. Therefore, firms are encouraged to encrypt Personal Data throughout the data cycle, including data at rest and in transit.

Confidentiality, integrity, availability and resilience of Processing systems and services

Firms must employ measures that ensure Processing systems and services are maintained to ensure their confidentiality, integrity, availability and resilience.

Confidentiality focuses on making sure data are safe from unauthorised access. Firms should ensure only authorised individuals have access to the data.

Integrity focuses on the accuracy and completeness of data. Therefore, firms must ensure data are not modified or deleted without authorisation. This applies to both data in transit and data at rest.

Availability focuses on making sure data are available to be used when needed. Firms must ensure systems are up and running and are accessible when employees and customers need the data.

Resilience is focused on the system's ability to withstand, adapt and recover from all forms of disruption, threats and other events. This may include incident response plans, crisis management plans and tried and tested business continuity and disaster recovery processes.

Restore availability and access

Firms must be able to restore access to and the availability of Personal Data promptly following an incident. There is crossover here with the requirements for availability and resilience. The ability to promptly restore the availability of and access to Personal Data are critical following a physical or technical incident.

Testing, assessing and evaluating

Firms must not only focus on putting measures in place to ensure the security of the data, but they must also check the effectiveness of these measures. This is done through a program of regularly testing, assessing and evaluating the effectiveness of the measures. This might include vulnerability scans, network penetration testing, and network stress testing to ensure resilient systems.

How to assess an appropriate level of security

When assessing the appropriate level of security, firms should understand, for example:

- *The categories and quantity of Personal Data collected;*

Firms should consider the categories and the quantity of Personal Data they Process. Are there multiple data points for each Data Subject? Do they collect Sensitive Personal Data, and if so, what types? Firms should also consider the number of Data Subjects involved.

- *The categories of Data Subjects;*

Firms should be aware of the categories of Data Subjects, such as customers, employees, visitors etc. when accessing which security measures are appropriate. Special consideration should be given to the data of vulnerable individuals such as children.

- *The risks to Data Subjects should the data be compromised;*

Firms should consider the impact on Data Subjects should there be a Personal Data Breach. For example, based on the categories of Personal Data and the categories of Data Subject, could a breach lead to unfavourable outcomes such as identity theft or embarrassment.

- *How are the data collected?*

Is the Personal Data collected electronically, if so, is it transferred using end-to-end encryption? Is the Personal data collected via a paper form(s), if so, are they collected face-to-face or posted/couriered to the firm?

- *Where are the data stored?*

Are the Personal Data stored electronically on servers held on the firm's premises or remotely on the cloud? Are paper files held on-site for a period and then transferred to an off-site location? What security measures are in place for entry and exit into the firm's premises where the data are held?

- *Who has access to the data?*

Who has access to the data, and is it controlled and monitored? Are there audit trails for electronic data to indicate who might have accessed, viewed/altered, printed, or deleted them? This also applies to physical data files.

- *How are the data Processed?*

Is the data Processed manually or electronically using a workflow? Do employees routinely print documents for Processing and then dispose of them? How are physical files destroyed, are they shredded in-house or by a third-party service provider?

- *What technology is available to protect the data?*

Technology is ever-advancing, and do firms know what solutions are in the market to protect the data? For example, firms might have to decide between using either two-factor authentication or multi-factor authentication to allow users access to their network. Which technology protects the data best and at what cost, both financial and user experience?

- *What is the cost of that technology?*

Firms can consider the cost of the technology that protects their data. Not all firms have vast sums of money to protect their data, so firms can weigh the cost against the risk to Data Subjects and the goal of protecting the data.

What are technical and organisational measures?

Technical measures

Firms must consider the available technology and take into account the cost of implementation. Where the cost of implementation is high and the risk to the Data Subject is low, firms can consider this when deciding to proceed with the measure.

- Physical Security – includes access to buildings, offices, file rooms and server rooms. Access should be restricted to those employees who require it for their roles and might include an audit trail in case of any issues.
- Device security – how are devices protected against unauthorised access, and how secure is the network access from mobile and other devices outside of the network?

- Data security – this is focused on the data level security and may include logical access controls and ensuring data and databases are encrypted in transit and at rest.
- System security – how secure is the network as a whole and specifically where Personal Data are Processed? Firms may consider perimeter security to prevent unauthorised access and data loss prevention tools to protect against data exfiltration.
- Online security – how does the firm protect applications that are open to the public, such as websites and mobile applications?

Organisational measures

- Risk assessment – how well the firm understands the level of risk associated with the Processing of Personal Data and the risks to the Data Subject. The level of risk should be a key driver for the level of control needed to mitigate the risk.
- Roles and responsibilities and accountability – having the right people responsible and accountable to ensure Personal Data are adequately protected.
- Policies and procedures – how has the firm articulated how it will manage the Processing, particularly the security, of Personal Data? This is a requirement under Article 29(4) of the Regulations.
- Testing and reporting – ongoing testing on how well the controls in place are working to protect the Personal Data and to whom in the firm the results are reported.

What can be taken into account when deciding on what is an appropriate level of security?

Not every firm is the same, and not all Processing of Personal Data presents the same risks to the Data Subject. As such, firms can, when deciding what the appropriate level of security is, take into account the following:

- The available technology;
- The costs of implementation;
- The likelihood and severity of risks to the rights and legitimate interests of individuals;
- The nature, scope, context and purposes of the Processing; and
- The risks of accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data that are presented by Processing.

When a firm decides to use or not use either an organisational or technical measure, they should document the rationale to demonstrate their approach is in line with the Regulations.

The requirement for appropriate data protection policies

Article 29(4) requires firms to implement appropriate data protection policies that cover the technical and organisational measures the firm has put in place to ensure an appropriate level of security in the Processing of Personal Data. The policies should cover the considerations taken into account when deciding on those measure, namely:

- The available technology;
- The costs of implementation;
- The nature, scope, context and purposes of the Processing; and
- The likelihood and severity of risks to the rights and legitimate interests of individuals.

It would be considered best practice to have policies in place that cover all aspects of a firms' data protection programme.

Cross-reference

See Article 8 for more information on the Principles, including Principle 6 relating to integrity and confidentiality of Processing.

See Article 25 for the information on the accountability principle and the requirement to implement the appropriate technical and organisational measures to demonstrate compliance with the Regulations.

See Article 26 for information on data protection by design and by default, including implementing the appropriate technical and organisational measures to ensure data are protected.

See Article 27 for information on data protection impact assessments required for high risk Processing and will help identify the appropriate level of security required for the Processing.

See Article 28 for information on the requirements when engaging Data Processors and their responsibilities under the Regulations.

Article 30 – Record of Processing operations

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.

QFC Data Protection Rules

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.

The Article 30 record of Processing operations is a critical component of a firm's compliance framework. The record, when completed correctly, significantly helps meet several other provisions of the Regulations, including meeting the transparency requirements under Articles 14 and 15 and the accountability obligations under Articles 9 and 25.

Data Controllers

All Data Controllers must complete the record of Processing operations for all Personal Data Processing the firm undertakes.

The record of Processing operations should be sufficiently granular to provide enough information for a Processing operation. The record of Processing operations is not a procedural document and does not need to include each procedural step in a process but be written so the purpose of the Processing is clear to the reader.

Data Processors

Data Processors must maintain a record of Processing operations for all Personal Data Processing they undertake on behalf of a Data Controller, per Article 30(2).

This record should clarify who is the Data Controller for the Processing. This is important when the Data Processor processes Personal Data on behalf of many Data Controllers.

Much, if not all, of the information required to meet this obligation will be included in the data processing agreement (contract) between the Data Controller and the Data Processor, required under Article 28.

Firms that are Data Processors for a Data Controller will be the Data Controller for a number of their own processes, such as those in Finance, Human Relations and Marketing.

Cross-reference

This should be read in conjunction with Article 28 of the Regulations and Rule 7(B).

See Article 28 for information on the Data Processor obligations, including the requirement to have a contract (data processing agreement) between the Data Controller and the Data Processor.

What is included in the record of Processing operations?

The record of Processing operations must include the following information:

The identity and contact details of the Data Controller.

This would typically include the name, address, contact name and number/email address of the legal entity that controls the data. Remember, the Data Controller may not be the legal entity undertaking the Processing and, particularly in a group setting, this may be a parent or other entity in a group.

Cross-reference

This information must be included in the transparency notices as required by Articles 14 & 15 of the Regulations and Rule 3(A).

The purpose of the Processing.

The purpose of the Processing is the main objective of the Processing. Therefore, this description should be sufficiently descriptive so the reader can understand what the Processing is trying to achieve.

Cross-reference

This information must be included in the transparency notices as required by Articles 14 & 15 of the Regulations and Rule 3(B).

The lawful basis, per Article 10 of the Regulations, for the Processing.

The lawful basis is intrinsically linked to the purpose of the Processing. Article 10 of the Regulations provides several lawful bases upon which Processing can be based. See also the additional bases for processing Sensitive Personal Data under Article 12.

Cross-reference

This information must be included in the transparency notices as required by Articles 14 & 15 of the Regulations and Rule 3(B).

Descriptions of the categories of Data Subjects and the categories of Personal Data.

The categories of Data Subjects refer to the types of Data Subject whose data are being Processed. Typical categories of Data Subject include:

- Employees, including agents, temporary and casual workers;
- Clients and customers;
- Suppliers;
- Members;
- Complainants, correspondents, and enquirers;
- Relatives and associates of the Data Subject; and
- Advisors, consultants, and other professional experts.

The categories of Personal Data refer to the types of Personal Data being Processed. Typical categories of Personal Data include:

- Name, surname and/or date of birth;
- Contact details (phone no, email address, postal address);
- Official identification data (QID, Passport, National ID);
- Access/ID information (username, password, reference number);
- Social media profiles;
- Economic and financial data;
- Official documents (originals or copies);
- Location data e.g. GPS (not including address info);
- Photo, video or audio records or recording; and
- Communication data.

Cross-reference

This information must be included in the transparency notices as required by Articles 14 & 15 of the Regulations and Rule 3(D).

The categories of Recipients to whom the Personal Data have been or will be disclosed.

When sharing Personal Data externally, a firm must know with whom it is sharing the Personal Data and list it in the record of Processing operations. Typical Recipients are:

- Individuals or organisations in a direct relationship with the Controller;
- Other private enterprises;
- Public services;
- Courts and law enforcement;

- Government offices;
- Banks and insurance companies; and
- Personal data or direct marketing brokers.

Cross-reference

This information must be included in the transparency notices as required by Articles 14 & 15 of the Regulations and Rule 3(E).

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.

This is linked to the previous requirement to include the category of Recipient of Personal Data. If a Recipient is located outside the QFC then the record of Processing operations must include:

- The name of the jurisdiction to which the Personal Data are transferred;
- The basis of the transfer; and
- Information on any other suitable safeguards in place if the transfer is to a jurisdiction not on the Data Protection Office's approved adequacy list. See further guidance on Articles 23 and 24 above.

Cross-reference

This information must be included in the transparency notices as required by Articles 14 & 15 of the Regulations and Rule 3(F).

The envisaged time limits for retention of the different categories of Personal Data.

One of the core data protection principles in Article 8 is Principle 5: the storage limitation. This Principle states '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'.

Firms must determine the length of time Personal Data will be retained. This might include reference to other laws or regulations requiring Personal Data to be held for a minimum time. See further information on the storage limitation Principle in the guidance on Article 8 above.

Cross-reference

This information must be included in the transparency notices as required by Articles 14 & 15 of the Regulations and Rule 3(H).

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

The record of Processing operations must include an overview of the technical and the organisational measures which have been put in place to ensure an appropriate level of security for the Personal Data.

Firms should include a general overview of the technical measures in place and may include:

- Encryption (or other forms of de-identification);
- 2-factor authentication;
- Logical access;
- Back-up and recovery solutions;
- Data loss identification and prevention tools, etc.
  It is important to focus on the technical and organisational measures firms have in place. These might include:
- Risk assessments;
- Data protection and information security policies and procedures;

- Incident management;
- Business resilience procedures;
- Audit and other internal control reviews, etc.

This does not need to be a detailed replica of all the technical and organizational measures the firm has in place but an overview. For example, where the firm has a detailed information security policy or related policy, it can be cross-referenced here.

To whom does the record of Processing operations need to be made available?

If requested, the record of Processing operations must be made available to the QFC Data Protection Office. In addition, firms must keep the record up-to-date for any changes in Personal Data Processing the firm undertakes.

Keeping the record of Processing operations up-to-date

The Regulations do not specify a review cycle for the record of Processing operations; however, firms should consider a review cycle in line with their business. In addition, firms should include a trigger to review or update the record of Processing operations as part of internal control test, internal audit review, and as part of the data protection impact assessment process as described in Article 27.

A Record of Processing Template can be downloaded from QFC/resource-centre/data-protection.

Article 31 – Notification of Personal Data Breaches

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.

QFC Data Protection Rules

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.

The Regulations require all firms to report Personal Data Breaches ("Breaches") to the Data Protection Office, without undue delay, and within 72 hours of becoming aware of them.

A Breach is defined "as 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".

This definition is very broad and focuses not only on the loss of data but also on access, alteration, and destruction. In addition, this definition includes deliberate, malicious, and accidental breaches.

Example

An employee of a firm provides a notice of resignation to HR. While serving the applicable notice period, the employee downloads and sends a large amount of documents obtained via the firm's database to his personal email account. The documents contain Personal Data of the firm's clients. The employee only had authorisation to access the data to fulfil his job tasks. After leaving the job, the employee uses the information obtained from the documents to contact the clients of the firm to entice them to his new business.

The employee has breached the firm's security by obtaining unauthorised access to the Personal Data.

Example

A financial institution suffers a cyber-attack against its website. Due to a vulnerability of the website, some information regarding Data Subjects (i.e. name, surname, gender, date of birth, bank account information and user identification codes) are leaked to the attacker. This leak affects 200,000 Data Subjects. The cyber-attack has caused a breach in the financial institution's security leading to the unauthorised disclosure of Personal Data of Data Subjects to the attacker.

Breach Identification

Firms must have an appropriate process in place to identify when Breaches occur. Firms may have both organisational and technological solutions to help identify when and if a Breach has occurred. Organisational controls such as training are an important tool to ensure employees understand what a Breach is and how to escalate it appropriately within the firm. Technological controls also play an important role, e.g. data leak identification and detection tools which automatically identify when specified data are compromised.

Assessment and Exclusion to Reporting

Once the firm has established a Breach has occurred, the next step is to assess the breach to determine if it is likely to result in a risk to Data Subjects' rights and legitimate interests.

The reporting obligation within the Regulations is not absolute; firms do not need to report Breaches that are unlikely to result in a risk to Data Subjects' rights and legitimate interests. Therefore assessing the potential impact of a breach is an important step in the process.

When assessing the impact on Data Subjects of a Breach, firms should consider the following outcomes the Data Subject could face, including:

- Loss of control over their Personal Data or limitation of their rights;
- Discrimination;
- Identity theft or fraud;
- Financial loss;
- Unauthorised reversal of de-identified data;
- Damage to reputation;
- Loss of confidentiality of Personal Data protected by professional secrecy; or
- Any other significant economic or social disadvantage to the natural person concerned.

When undertaking the assessment, firms should consider:

- The nature of Personal Data involved in the breach. Does the Breach involve contact information, governmental or banking data, Sensitive Personal Data etc.?;
- The volume of Personal Data involved. Is it limited to one piece or multiple pieces of Personal Data per Data Subject?
- The nature of the Breach itself. Did the Breach involve the loss of control of Personal Data or did an authorised third party gain access to the data; was data changed; or did the Breach involved a loss of access to the data?

The result of the assessment will determine if the Breach is reportable to the Data Protection Office.

Where a firm has determined the Breach is not reportable, they should document their conclusion as this must be made available to the Data Protection Office if requested.

Not later than 72 hours after having become aware of it

Firms should be aware that the test of when it becomes aware of a Personal Data Breach is an objective one. Once the firm has enough information to conclude that a Personal Data Breach has occurred, as defined by the Regulations, the 72-hour reporting period starts. Firms cannot delay reporting by simply ignoring or not responding to a Personal Data Breach.

During the 72-hour reporting period, a firm may conclude that the exclusion is Article 31(2) applies; however, this does not affect the initial notice period's timeline.

Example

When sending an external email, an employee accidentally enters the wrong email address and sends a report which contains medial information of staff to an unauthorised individual outside of the firm.

The unintended recipient immediately called the employee to let the firm know they have sent the information to the wrong recipient.

The firm became aware of the personal data breach when the employee, realising the error after the call, checked the sent email and confirmed it was addressed incorrectly. It is at this date and time that the 72-hour notification period commences.

The combination of the requirement to notify the Data Protection Office in Article 31(1) of the Regulations and Article 31(2) means that the threshold for notification of a Personal Data Breach to the Data Protection Office is a low threshold. This means that unless a firm can confidently determine that the breach will not impact data subjects adversely, it must proceed with the notification, thus ensuring a broad scope for reporting and a low bar for activation of the notification requirement.

Firms should establish internal processes to promptly assess potential breaches and initiate the 72-hour notification to ensure compliance with these requirements.

Example

An employee notices – due to a faulty setting on the firm's systems – she is able to access sensitive information relating to employees of the firm (e.g. sick leave and medical information) that she is not authorised to access as per her job function. She immediately notifies her manager, who in turn contacts the firm's IT department to rectify the problem. The employee did not review or use the data and signs a written statement to that effect. While a breach may have occurred, there was no loss of control nor access or use of the Sensitive Personal Data. An analysis of the breach by IT indicates that there is no likelihood of it resulting in a risk to the employees' rights and legitimate interests.

Reporting to the Data Protection Office

Rule 9 provides information on what must be included in a report to the Data Protection Office:

- The nature of the Breach;
- The categories of Data Subjects affected, such as customers, employees, etc.;
- The approximate number of Data Subjects affected;
- The categories and approximate number of Personal Data records affected;
- The name and contact details of someone in the firm who can be contacted regarding the Breach;
- A description of the likely consequences of the Breach;
- What has or is planned to be done to rectify the Breach and to mitigate any adverse effects on Data Subjects; and
- Where the notification is not made within 72 hours, the reason why it was not made within this time period.

Firms can notify Personal Data Breaches to the Data Protection Office by completing and submitting the QFC Data Protection Breach Report that can be downloaded from QFC/resource-centre/data-protection.

Example

The nature of the Breach might be the loss of control of Personal Data due to an email containing Personal Data of customers being accidentally disclosed to a third party. In this example, the Personal Data of 100 customers, which included contact information such as email and telephone numbers and their full names, was included in the file; this means 300 records were lost.

Notifying the Data Subject following a Breach

The Regulations do not make notifying Data Subjects of a Breach mandatory; however, firms must consider whether notification is required. The assessment as to whether or not to notify a Data Subject can take place at the same time as assessing whether the Breach is reportable to the Data Protection Office, as it will involve a similar process and data set.

The conclusion of this assessment must be clear and made available to the Data Protection Office if required.

The Data Protection Office may order the firm to notify Data Subjects following a Breach if deemed necessary.

Rectification and Mitigation of the Breach

Firms must provide information on how they have rectified or mitigated the risks to Data Subjects following the Breach. Firms must provide this information to the Data Protection Office for all reportable events per Rule 9.

Rectification and mitigation will vary depending on the nature and scale of the event. Examples of rectification and mitigating actions might include:

- Changes in Processing to remove manual steps;
- Contacting unauthorised Recipients and requesting deletion of data;
- Contacting Data Subjects, informing them of the event and suggesting they change passwords and monitor their accounts; and
- Monitoring client accounts for any unusual or suspicious behaviour.

Where firms are unsure about how to mitigate a particular event, please contact the Data Protection Office.

Example

An incident occurs where client details, including name, email address and telephone number, were accidentally emailed to the wrong Recipient as part of a regular Processing for marketing purposes. In response to this event and to ensure it does not happen again, the firm reviewed the process and decided to use a secure online platform where the marketing firm can log in and collect the file and thus eliminating the need to send it via email.

Data Processors role in notifying Data Controllers of a Personal Data Breach

Where a Data Processor becomes aware of a Personal Data Breach it has an obligation under Article 31(7) to notify the Data Controller 'without undue delay'. Where the Data Processor delays notification to the Firm, this does not absolve the Data Controller of its responsibilities under the Regulations. As the key decision-maker in Processing activities, the Data Controller determines the purposes and means of Processing, while the Data Processor acts on its behalf according to instructions. Therefore, the Data Processor cannot be used as a means to evade compliance with the Regulations.

The following Articles are of key importance in understanding the responsibility of Data Controllers and Data Processors when it comes to the reporting of Personal Data Breaches:

- Article 25 requires Data Controllers to implement appropriate technical and organisational measures to ensure, and to be able to demonstrate, that Processing is performed in accordance with the Regulations.
- Article 26 requires Data Controllers to, both at the time of the determination of the means for Processing and at the time of the Processing itself, implement technical and organisational measures to integrate the necessary safeguards into the Processing to meet the requirements of the Regulations.
- Article 28 (1) states that 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 to (a) implement technical organisational measures to comply with these Regulations, and (b) ensure that Data Subjects' rights are protected.
- Article 28 (3) requires the Data Controller and the Data Processor to enter into a written contract that sets out, at a minimum, the information contained in the Data Protection Rules.
- Article 31 (1) requires Data Controllers to notify Personal Data Breaches to the Data Protection Office without undue delay and, where feasible, no later than 72 hours after having become aware of it.
- Article 31 (7) requires a Data Processor to notify the Data Controller concerned without undue delay after becoming aware of a Personal Data Breach.
- Rule 7(J) of the Rules outlines that for the purpose of Article 28 of the Regulations, a contract between a Data Controller and a Data Processor must set out, at a minimum, the requirement for the Data Processor to assist the Data Controller to comply with the Data Controller's obligations under Article 27, 29 and 31 of the Regulations, taking into account the nature of the Processing and the information available to the Data Processor.

When read together, the Regulations and Rules provide that:

(a) Data Controllers must implement technical and organisational measures to comply with the Regulations and ensure that Data Processors, acting on behalf of Data Controllers, also have appropriate measures in place.

(b) Ensuring compliance with the Regulations includes the express requirement to ensure Data Controllers are able to notify the Data Protection Office of a Personal Data Breach without undue delay and by no later than 72 hours after having become aware of it.

(c) To enable Data Controllers to meet this obligation, there is also an obligation to ensure a proper process is in place for Data Processors to notify Data Controllers of a Personal Data Breach upon becoming aware of the same.

(d) Article 31(7) places an obligation on the Data Processor to notify the Data Controller without undue delay after becoming aware of a Personal Data Breach. This provision does not amount to a shift in responsibility from the Data Controller to the Data Processor for notifying the Data Protection Office, rather, it sets the minimum expectation of obligations a Data Controller is required to impose on a Data Processor, when entrusting it with its Processing activities.

Accordingly, the Data Controller's obligation under Article 31(1) remains fully applicable even when it has outsourced processing activities to a Data Processor who fails to notify the Data Controller promptly of a Personal Data Breach. The Data Controller remains fully responsible for compliance with the regulations, and such a failure still results in a breach of the Regulations. Non-compliance due to inadequate processes or a failure to adhere to established procedures does not absolve the Data Controller from its legal obligations.

Record Keeping

Keeping the appropriate records of Breaches will demonstrate how firms have identified, assessed, rectified, and mitigated any Breach should they occur.

Firms can decide how they would like to record Breaches, but it is suggested such records should include all the information required per Rule 9 and, in addition, may include:

- The date the Breach occurred and the date it was discovered, if different;
- The type of Breach such as human error, system failure, etc.;
- The conclusion of the assessment of the impact of the Breach on Data Subjects; and
- The conclusion of the assessment as to whether to notify Data Subjects of the Breach.

Part 6

The Data Protection Office

Article 32 – Establishment of the Data Protection Office and the Data Protection Commissioner

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) In performing its functions and exercising its powers, the objectives of the Data Protection Office are as follows:

(A) To monitor, ensure and enforce compliance with these Regulations;

(B) To promote good practices and compliance with the requirements of these Regulations by Data Controllers or Data Processors;

(C) To promote greater awareness and public understanding of data protection and the requirements of these Regulations in the QFC.

(4) The Data Protection Office is to be managed by the Data Protection Commissioner (the "Commissioner") who will determine its procedures and management.

(5) 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; and

(B) Ensure that the Data Protection Office uses its resources in accordance with its objectives.

(6) The QFC Authority may make rules and issue guidance 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.

(7) The independence of the Data Protection Office is not affected by the financial or other controls and reporting obligations to which it may be subject as an Institution of the QFC.

Article 32 details the creation of the Data Protection Office as an independent institution of the QFC and the creation of the role of Data Protection Commissioner (the "Commissioner").

Paragraph (3) sets out the objective of the Data Protection Office which include:

- to monitor, ensure and enforce compliance with these Regulations;
- to promote good practices and compliance with the requirements of these Regulations by Data Controllers or Data Processors;
- to promote greater awareness and public understanding of data protection and the requirements of these Regulations in the QFC.

The Data Protection Office is charged with administering the Regulations and should be read in conjunction with Article 33.

Article 32A – The Data Protection Commissioner

ARTICLE 32A – THE DATA PROTECTION COMMISSIONER

(1) The QFC Authority must appoint a person to be the Commissioner who is appropriately experienced and qualified.

(2) The Commissioner is to be appointed for a specified period of time not exceeding 5 years, and may be re-appointed for 1 or more further periods, but no such period may extend beyond the day when the Commissioner turns 65 years of age.

(3) The Commissioner may be removed from office by written notice issued by QFC Authority for reasons of inability, incapacity or misbehaviour, including:

(A) Accepting or giving bribes or any illegal gratification or any solicitation therefore;

(B) Defrauding or attempting to defraud the QFCA including forgery of documents;

(C) Committing on QFCA premises an offence in breach of State Criminal Law;

(D) Committing on QFCA premises inappropriate behaviour including indulging in any kind of sexual or physical behaviour;

(E) Being under the influence of alcohol or drugs while on duty;

(F) Possession of weapons at work.

(4) The Commissioner may at any time resign by giving 3 months written notice addressed to the QFC Authority.

(5) The Commissioner must act with complete independence in performing its duties and exercising its powers and functions in accordance with these Regulations. The independence of the Data Protection Commissioner is not affected by the financial or other controls and reporting obligations to which it may be subject.

(6) In performing its duties and exercising its powers and functions the Commissioner must:

(A) Remain free from external influence, whether direct or indirect, and neither seek nor take instructions from anybody;

(B) Refrain from any action incompatible with their duties; and

(C) Not engage in any occupation, remunerated or not, that is incompatible with the role of the Commissioner.

(7) Officers and staff appointed to the DPO will be, and remain, subject to the exclusive direction and authority of the Commissioner.

(8) The Commissioner may delegate any of its functions, duties or powers to be carried out by its officers or staff provided that the Commissioner remains ultimately responsible for how they are carried out.

This Article sets out the role of the Commissioner.

The QFCA appoints a Commissioner who is suitably experienced and qualified, for a term not exceeding five years, with eligibility for reappointment. The Commissioner can be removed for reasons such as accepting bribes, fraud, inappropriate behaviour, as set out in paragraph (3). The Commissioner may resign with three months› notice and must operate independently, avoiding external influences, incompatible actions, or occupations that conflict with their role.

Article 33 – Powers

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:

(A) To issue, on its own initiative or on request, opinions, interpretations, 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 approve Binding Corporate Rules, or other internationally acceptable transfer mechanisms for the purposes of Article 24;

(D) 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.

This Article outlines the powers of the Data Protection Office, which are broken down into three general categories as follows:

- Investigative powers;
- Corrective powers; and
- Authorisation and advisory powers.

The powers of the Data Protection Office are far-reaching and have specific objectives; for example, the power to order compliance with a Data Subject rights request and to ensure firms are not ignoring their obligations to Data Subjects. Whereas the power to impose a financial penalty, although a last resort, is there to punish a firm for wilful or negligent breaches of the Regulations.

Investigatory Powers

The investigatory powers in Article 33(1) include the power to:

- Order a Data Controller to provide any information requested;
- Carry out investigations, including data protection audits;
- Notify a Data Controller or Data Processor of an alleged infringement; and
- Obtain access to any premises of a Data Controller or Data Processor and includes access to equipment.

Corrective Powers

The corrective powers in Article 33(2) include the power to:

- Issue warnings to Data Controllers or Data Processors that they might infringe the Regulations;
- Issue reprimands or orders to rectify any identified infringements;
- Order compliance with a Data Subjects Rights requests;
- Carry out Processing in a specified manner;
- Notify a Data Subject of a Personal Data Breach;
- Impose a temporary or permanent limitation or ban on Processing;
- Order the rectification or erasure Personal Data;
- Impose a financial penalty (See Article 36);
- Order the suspension of data transfers to a Recipient outside the QFC; and
- Order a Data Controller to undertake a data protection impact assessment.

Authorisation and Advisory Powers

The authorisation and advisory powers in Article 33(2) include the power to:

- Issue opinions, interpretations, and training;
- Publish a list of adequate jurisdictions in accordance with Article 23;
- Approve a firms application to BCRs for the transfer of Personal Data;
- Approve other internationally acceptable transfer mechanisms for the transfer of Personal Data; and
- Grant permits for the Processing of Sensitive Personal Data and transfers of Personal Data per Articles 12 and 24.

Non-compliance with an order of the Data Protection Office

Where a firm does not comply with a determination, decision or order of the Data Protection Office made according to Article 33 or 36, the Data Protection Office can bring the matter directly to the Civil and Commercial Court to obtain an order:

- Directing the Data Controller or Data Processor to comply with such an order; and
- Directing the Data Controller or Data Processor to pay any costs incurred by the Data Protection Office.

Appeals to the Regulatory Tribunal

Firms may appeal any determination, decision or order made by the Data Protection Office to the Regulatory Tribunal within 60 days, per QFC Law.

Part 7

Remedies

PART 7 – Remedies

Part 7 of the Regulations focuses on the remedies available to Data Subjects should a firm breach its obligations under the Regulations and Rules.

The remedies available to Data Subjects under the Regulations are administrative and judicial in nature. The administrative remedies are actioned via the Data Protection Office and primarily focus on responding to complaints. The judicial remedies available to Data Subjects involve taking a case directly against the firm to the QFC Civil and Commercial Court. In addition, the Regulations now provide for material and non-material damages for breaches of the Regulations.

Article 34 – Right to Lodge a Complaint with the Data Protection Office

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.

QFC Data Protection Rules

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.

Any person, body, organisation or association can lodge a complaint with the Data Protection Office where they believe a firm has breached the Regulations. Complaints tend to be made by Data Subjects directly and usually when a firm is not Processing their Personal Data in accordance with the Regulations, or they have not responded to a Data Subject rights request in the correct manner, specifically:

- Personal Data being Processed without a clear lawful basis;
- Data Subjects were not adequately informed about how their data are Processed;
- Personal Data being transferred outside the QFC without the appropriate safeguards;
- Data Subject access request was denied or not all Personal Data provided to the Data Subject;
- Data Subject rights request not being Processed promptly; or
- Data Subjects being charged for a rights request without a suitable basis.

Data Subjects do not need to go through an internal complaint handling process with the firm before lodging a complaint, but it is advisable to do so as this can often resolve issues quickly and efficiently.

What must be included in the complaint?

Rule 10 outlines what must be included in a complaint and includes:

- The complainant's full name and address;
- The full name and address of the Data Controller;
- Compensate details on the complainant;
- What outcome the complainant is seeking;
- A declaration the information provided is accurate; and
- Any other information the Data Subject deems important to the complaint.

It is important to note that the Data Protection Office cannot award compensation to the Data Subject in the event of a complaint being upheld. Therefore, where complaints are made to fulfil a Data Subject rights request, the goal will be to ensure the rights request is fulfilled promptly.

Data Subjects can lodge a complaint by completing and submitting the QFC Data Protection Office Data Subject Complaint Form, which is available online at QFC/resource-centre/data-protection.

Assessment, Investigation and Resolution of Complaints

The Data Protection Office reviews all complaints received and determines whether to investigate the complaint or refuse to act on it; see below for more information on refusing to act on a complaint.

When investigating a complaint, the Data Protection Office will keep the complainant updated on its status and outcome.

The aim when investigating a complaint is to ensure that infringements of the Regulations are rectified as efficiently as possible. For example, where the complaint is related to a non-completion or unnecessary delay in responding to a Data Subject rights request, the aim will be to ensure the rights request is actioned without additional delay.

Following an investigation and where a complaint is upheld, the Data Protection Office may rely on its powers under Article 33, including issuing warnings, reprimands or orders to act or cease acting.

Refusing to act on a Complaint

The Data Protection Office may refuse to accept, review or investigate a complaint or may suspend or postpone any such activity where:

- It determines the Regulations do not apply to the complaint;
- There is not enough evidence to prove the complaint;
- A previously related decision has been made by the Data Protection Office, the Civil and Commercial Court, or the Regulatory Tribunal on the complaint;
- The complainant did not engage with or assist the Data Protection Office in facilitating the handling, resolution or investigation of the complaint;
- The dispute that caused the complaint is resolved; or
- The complaint is frivolous, vexatious, trivial or not made in good faith.

When the Data Protection Office refuses to act on a complaint, it will inform the complainant without undue delay of that decision.

Decisions of the Data Protection Office to refuse to act on a complaint can be challenged by the Regulatory Tribunal within 60 days of such a decision.

Charging for Complaints

The Data Protection Office will not generally charge for handling complaints, however in exceptional cases, the Data Protection Office may charge but only where the complaint is assessed to be manifestly unfounded or excessive. For example, this could be due to the repetitive character of the complaint.

Any costs must be reasonable regarding the administrative costs incurred by the Data Protection Office.

Article 35 – Right to Compensation and Liability

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).

Along with the right to lodge a complaint with the Data Protection Office, the right to compensation and liability are key remedies for Data Subjects under the Regulations.

This Article provides Data Subjects with the right to claim compensation from a Data Controller or a Data Processor for damage, material or non-material, suffered due to Processing which infringes the Regulations.

Claims must be taken directly with the Civil and Commercial Court and do not need to go through the Data Protection Office or the complaints process prior to being lodged with the Court.

Material or Non-Material Damage

Material damage is where the Data Subject has a tangible loss, such as loss of money. Non-material damage is wider and covers loss due to pain, suffering, and distress.

The Data Protection Office cannot award compensation for breaches of the Regulations, even when a complaint is upheld.

Liability of Data Controllers and Data Processors

As the party who decided on the purpose and means of data Processing, Data Controllers are liable for any damage caused by Processing that breaches the Regulations.

Data Processors are liable for damage caused by Processing where they have acted without the lawful instruction of the Data Controller or against such lawful instruction or where they have failed to comply with provisions of the Regulations directly related to Data Processors.

Where the Data Controller or Data Processor can show they were not responsible for the event giving rise to the damage, they may not be liable for the damage.

Both Data Controllers and Data Processors should seek appropriate legal advice should a case be taken against them at the Civil and Commercial Court.

Lodging a case with the Civil and Commercial Court

Data Subjects who wish to take a case at the Civil and Commercial Court can do so by visiting www.qicdrc.gov.qa or by obtaining independent legal advice.

Article 36 – General Conditions for Imposing Penalties

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 USD1,500,000.

Article 33(2)(H) of the Regulations now gives the Data Protection Office the power to administer a financial penalty for infringements of the Regulations. This Article provides information on the considerations which the Data Protection Office will take into account when deciding to impose a financial penalty and the amount of that penalty.

The Article sets the maximum fine that can be applied: namely USD1,500,000 per provision infringed. This means the total maximum fine is based on the number and nature of the provisions infringed. Where a firm breaches more than one provision, each provision carries a maximum penalty of USD1,500,000.

Purpose of financial penalties

The main purpose of having the power to impose a financial penalty is to dissuade firms from non-compliance and persuade them to comply with the Regulations.

When deciding to issue a fine, the Data Protection Office will consider:

- The scale and severity of the non-compliance;
- The firm's openness and engagement with the Data Protection Office; and
- The firm's willingness to rectify the infringement and a commitment to ongoing compliance.

Maximum Fine

The maximum fine is $1,500,000 per provision infringed. This is the maximum fine and an individual fine may be less than this amount.

When setting an acceptable amount, the Data Protection Office will take into account:

- The nature, gravity and duration of the infringement, considering:
  - The nature, scope or purpose of the Processing concerned;
  - The number of Data Subjects affected; and
  - The level of damage suffered or potentially suffered by them;
- The categories and amount of Personal Data affected by the infringement (for example, did it include Sensitive Personal Data?);
- Whether the infringement occurred through the intentional or negligent character or actions of the firm;
- Actions taken by the Data Controller or Data Processor to mitigate or limit damage suffered by Data Subjects;
- The number, seriousness and relevance of other infringements of the Data Controller or Data Processor;
- The degree of cooperation with the Data Protection Office in fixing and mitigating the effects of the infringement on Data Subjects;
- How the Data Protection Office became aware of the infringement (for example, did the Data Controller or Data Processor report the incident themselves or was it through a Data Subject complaint?);
- If the Data Protection Office has previously made an order against the Data Controller or Data Processor for the same infringement and the extent of compliance with that order; and
- 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.

Example

A firm has not completed its Article 30 records of processing, and they have not provided Data Subjects with a transparent privacy notice per Articles 14 and 15. As a result, as well being in breach of their obligations under Articles 14, 15 and 30, they may have breached the lawfulness, fairness and transparency principle under Article 8. In this case, the maximum total penalty imposed could be up to $4,500,000.00 as they are potentially in breach of three provisions of the Regulations.

Appeal of penalties issued by the Data Protection Office

Firms retain the right to challenge any determination, decision or order made by the Data Protection Office regarding a financial penalty imposed on them to the QFC Regulatory Tribunal within 60 days of such a determination, decision or order.

Part 8

Final Provisions

Article 37 – General Exemptions

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.

(D) A Data Controller, to the extent that compliance with those Articles would be likely to prejudice:

(i) National security, defence and public security;

(ii) The prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and preventing threats to public security;

(iii) The prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

(iv) The protection of Data Subjects or the rights and legitimate interests of others

(v) The enforcement of civil law claims.

Article 37 provides two general classes of exemption from either the whole Regulations or aspects of it.

The Household Exemption

There is a general exemption for natural persons Processing Personal Data for purely household activities. In this case, the Regulations are exempt only when the Processing is for household activities such as protecting personal property using a CCTV camera. However, if the Processing steps into the public domain (e.g. the CCTV camera monitors the public pathway outside the property), then the exemption may no longer apply.

It is important to note that given the nature and scope of the QFC and the licenced activities permitted, it is unlikely this exclusion would apply to any QFC firms in the course of their business.

Exemption for QFC bodies

There is a limited exemption for specific QFC bodies when discharging their powers and functions, if by complying with the Regulations this would interfere with the proper discharge and intentions of those powers and function. This is fundamentally a limited exemption and only:

(a) Applies to the following articles:

(a) Articles 14 & 15 information to be provided to Data Subjects;

(b) Article 16, 17, 18, 19, 20 and 21 regarding the Data Subject rights to access, rectification, erasure, object, restrict Processing and portability;

(c) Article 22 the rights around automated individual decision-making including profiling; and

(d) Article 23 & 24 regarding data transfers outside the QFC.

(b) Applies:

(a) To the QFC Authority, the QFC Regulatory Authority, or a QFC Institution;

(b) In their capacity as a Data Controller; and

(c) Only to the extent that compliance with those Articles would likely prejudice the proper discharge of their powers and functions.

Where one of the listed bodies wishes to rely on this exemption, they must be able to:

- Identify the power or function which they are relying on for the exemption; and
- Assess whether fulfilling that specific power or function would prejudice its discharge. This can be on a case-by-case basis or potentially for a Processing activity as a whole.

In line with the Accountability provisions in Article 9 and Article 25, the relevant body would need to document the power or function that is being relied upon and why it would be prejudiced by complying with the relevant provision.

Example

When investigating an individual for a potential infringement of QFC Regulations and Rules, the QFC Authority may determine that providing Personal Data obtained via the investigation as part of a Data Subject access request may tip off the individual to the investigation and compromise the objective of the process. In this case, all other Personal Data held by the QFC Authority is provided to the individual except information that would prejudice the proper discharge of the investigations. The reliance on the exemption, the relevant Regulations and provisions applicable and why it would prejudice the investigation are noted on the relevant file.

Exemption for QFC Civil and Commercial Court and Regulatory Tribunal

When the Civil and Commercial Court and Regulatory Tribunal is acting in a judicial or quasi-judicial capacity to assess someone for judicial office or if applying the provisions would impede their judicial independence or proceedings, the provision of Articles 14 to 24 does not apply.

Limited additional exemptions for Data Controllers

Article 37(1)(D) provides Data Controllers with an exemption for complying Articles 14, 15, 16, 17, 18, 19, 20, 21, 22, 23 and 24, but only when the Processing is in relation to the following one of the activities listed in (D)(i) to (v).

Given the specific nature of these activities, the firm should be clear that their Processing in done in in relation to these directly and should adequately document their use of this exemption.

Cross-reference

See Article 9 and 25 for information on the accountability requirements of the Regulations.

Article 38 – Interpretation

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.

This Article provides clarity on how specific words or dates are to be interpreted when reading the Regulations.

Where there is uncertainty on how a word or date should be interpreted the firm should review this Article before proceeding.

Article 39 – Definitions

This Article clarifies the meaning of specific words and phrases used throughout the Regulations and Rules. These words and phrases are capitalised and have the meaning described below.

A word or phrase is not defined will have its ordinary meaning.

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

Binding Corporate Rules	Personal Data protection policies which are adhered to by a Data Controller or Data Processor for transfers or a set of transfers of Personal Data to a Data Controller or Data Processor within a Group.
Body Corporate	Has the meaning set out in the Companies Regulations 2005.
Child	An individual who is under the age of 18 years.
Civil and Commercial Court	The Civil and Commercial Court of the QFC established under Article 8 of the QFC Law.
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 or another Data Processor.
Data Protection Commissioner	The individual appointed in accordance with Article 32 who determines the procedures and management of the Data Protection Office.
Data Protection Office	The QFC Institution established by Article 32.
Data Subject	A natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the Data Subject.
De-identification	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.
Filing System	Any structured set of Personal Data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.
Minister	The Minister as defined in the QFC Law.
Permitted Activity	The activities listed in Schedule 3 or designated by the Council of Ministers under Article (1)10 of the QFC Law.
Personal Data	Any information relating to a Data Subject.
Personal Data Breach	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.
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.
QFC	The Qatar Financial Centre.
QFC Authority or QFCA	The Qatar Financial Centre Authority established under Article 3 of the QFC Law.
QFC Institution	An institution established pursuant to Article 6 of the QFC Law.

QFC Law	Law No. (7) of 2005 of the State of Qatar.
Recipient	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.
Regulations	Regulations enacted by the Minister in accordance with Article 9 of the QFC Law.
Regulatory Authority	The Regulatory Authority of the QFC established under Article 8 of the QFC Law.
Rules	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.
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.
State	The State of Qatar.
Regulatory Tribunal	The Qatar Financial Centre Regulatory Tribunal, established under Article 8 of the QFC Law.

Qatar Financial Centre Authority • PO Box 23245 • Doha, Qatar
T: +974 4496 7777 • F: +974 4496 7676 • info@qfc.qa • qfc.qa