Data Protection Regulations 2021

Factsheet

Data Protection Office
Qatar Financial Centre

Qatar Financial Centre Authority ● PO Box 23245 ● Doha, Qatar
T: +974 4496 7777 ● F: +974 4496 7676 ● info@qfc.qa ● qfc.qa

QFC Data Protection Regulations 2021

Factsheet

The QFC Data Protection Regulations 2021 (the 'Regulations') set out the principles and minimum requirements that all Data Controllers and Data Processors must comply with when Processing the Personal Data of staff, customers, suppliers, contractors, marketing information subscribers, etc.

More information on the Regulations, including guidance and helpful tools, can be found on the Data Protection Resources section which is accessible via the Data Protection Office page on the QFC website.

QFC Data Protection Commissioner

There are six core principles of the Regulations where Personal Data must be:

1 Processed lawfully, fairly & transparently

2 Processed only for specific, explicit and legitimate purposes

3 Adequate, relevant and limited to what is necessary for the purposes for which they are Processed

4 Accurate and kept up to date. Personal Data that are inaccurate must be erased or corrected without undue delay

5 Kept only for as long as is necessary for the purposes for which the data were Processed

6 Processed in a way that ensures that the data are appropriately secure

Key Definitions

Data Controller / Data Processor

Firms must determine if they are the Data Controller or Data Processor for a particular process.

Data Controller is any person (individual, organisation or corporate and unincorporated body) who determines the purpose (the why) and means (the how) of Personal Data Processing.

Data Processor is the person who Processes Personal Data on behalf of the Data Controller. Data Processors act only on direct, clear instructions of the Data Controller.

For employee data the firm will most likely be the Data Controller.

Firms will need to carefully consider if they are the Data Controller or the Data Processor when Processing Personal Data. Where the firm is the Data Controller, all the obligations under the Regulations will apply.

Personal Data / Sensitive Personal Data

Personal Data and Sensitive Personal Data are the data collected and Processed regarding staff, customers, suppliers, contractors, marketing information subscribers, etc.

Personal Data includes first and surnames, postal addresses, email address, ID card numbers, location data, IP addresses, cookie IDs, loyalty card numbers, etc.

- **Personal data** is information relating to a living individual who can be identified, directly or indirectly, from those data.
- **Sensitive Personal Data** is a subset of Personal Data. It includes information related to race, ethnic origin, political opinions, religious or philosophical beliefs, trade union memberships and health of an individual.

Qatar Financial Centre Authority ● PO Box 23245 ● Doha, Qatar
T: +974 4496 7777 ● F: +974 4496 7676 ● info@qfc.qa ● qfc.qa

Key Requirements

Lawfulness of Processing

Article 10 of the Regulations requires a lawful basis in order to Process Personal Data, these may include:

- **Consent**
- **Contractual necessity**
- **Legal obligation**
- **Vital interests of the Data Subjects**
- **Public interest or interest of the QFC**
- **Legitimate interest of controller/ 3rd parties**

Note: Personal Data might be used in more than one Process, in these cases a separate lawful basis might be appropriate for each Process.

Consent

Article 11 of the Regulations concern the use of Consent as a lawful basis. Consent gives Data Subjects real choice and control over how their Personal Data are used by a Data Controller.

For consent to be deemed a valid lawful basis to Process Personal Data is must be:

- **freely given**
- **specific**
- **informed**
- **an unambiguous indication of agreement**
- **as easy to withdraw as it was to provide**

Information provided to Data Subjects

Transparent communications with Data Subjects is required under Articles 14 and 15 of the Regulations and subject to Article 13 and Rule 3. Data Subjects must be given information as to the nature of the Personal Data, the Processing performed, to whom their Personal Data might be shared, and what their rights are concerning it.

A **Data Subject** is the person to whom the Personal Data relates. It includes staff, customers, suppliers, contractors, marketing information subscribers, etc.

A record of Processing operations

Article 30 of the Regulations require Data Controllers have in place a record of all Processes that use Personal Data.

- **Processing** includes collecting, recording, organising, storing, adapting or altering, retrieving, consulting, using, disclosing, disseminating or otherwise making available, aligning or combining, blocking, erasing or destroying.

This record must include all Processes that involve employee data as well as customer and supplier data.

Data Processors must also maintain a record of Processing for all activities they undertake for a Data Controller.

Data Transfers out of the QFC

Articles 23 and 24 refer to transfers of Personal Data out of the QFC. Personal Data **can only be transferred to a jurisdiction outside the QFC which offers an adequate level of protection.**

The list of adequate jurisdictions is available on Data Protection Resources page of the QFC website.

Person Data transfers to jurisdictions which are not on this list are permitted only when:

- appropriate safeguards are in place, such as the use of our Standard Contractual Clauses;
- specific derogations apply such as explicit consent;
- in limited circumstances e.g., a once off transfer; or
- a permit has been obtained from the DPO.

Data Subject Rights

Data Subjects have several rights per the Regulations, these are:

- **Access** (Article 16)
- **Rectification** (Article 17)
- **Erasure** (Article 18)
- **Objection** (Article 19)
- **Restriction** (Article 20)
- **Portability** (Article 21)
- **Automated decisions & profiling** (Article 22)

Firms must be able to recognise Data Subject rights requests when they are received and be able to act upon them in a timely manner.

Data Protection by Design / Default & Data Protection Impact Assessments

Article 26 requires firms to implement Data Protection by Design and Default.

By design: firms must consider data protection at the start of any project, this includes when designing and when carrying out Processing.

By default: ensuring systems and applications adopt a "privacy-first" approach i.e. configuring privacy settings in the strictest most privacy focused mode as standard.

Data Protection Impact Assessment (DPIA) (Article 27) must be carried out before doing any high risk Processing, i.e., Processing that could impact the rights and legitimate interests of Data Subjects.

Personal Data Breaches

Article 31 requires firms inform the DPO of any Personal Data Breaches without undue delay and **within 72 hours of becoming aware of such a breach**.

If a firm determines that a Personal Data Breach is not likely to harm the rights and legitimate interests of the Data Subjects whose data were exposed, then they are not required to report the breach

Firms must have a process in place to identify, assess and report Personal Data Breaches within this time limit.

Data Security

Article 29 specifies that Data Controllers must have the appropriate technical and organisational measures in place to protect Personal Data. The nature of the Personal Data and the level of potential harm to the Data Subject, should there be a breach, are among the considerations when assessing an appropriate level of protection.

- **Technical measures:** Access control, network security including vulnerability assessment, anonymisation and de-identification, data transfer controls, etc.
- **Organisation measures:** Risk assessments, data protection and information security policies and procedures, incident management, business resilience, training, audits and system logs, etc.

Where a firm outsources any Personal Data Processing to a third party, the firm must ensure the third party offers a level of protection that is sufficient to the risk.

Data Controller & Data Processors Obligations

Data Controllers must implement *appropriate and effective technical and organisational measures to ensure and to be able to demonstrate* that Processing is performed in accordance with the Regulations (Article 25).

Data Processors must (Article 28)**:**

- Process Personal Data only based on a written contract;
- need written approval to appoint a sub-processor; and
- must notify the Controller of any Personal Data breaches without undue delay.

Data Processors must also implement technical and organisational measures to comply with these Regulations and ensure that Data Subjects' rights are protected.