# Standard Contractual Clauses

*relating to the transfer of Personal Data outside the QFC pursuant to*

*the QFC Data Protection Regulations 2021 (“****QFC DPR 2021****”)*

*[GUIDANCE:*

1. *The following Guidance should be removed prior to entering into these Clauses.*
2. *These Clauses (as defined in Clause 1 below) are intended to facilitate the lawful export of Personal Data under Article 24(2) of the QFC DPR 2021.*
3. *Prior to entering into these Clauses, the Parties (as defined in Clause 1 below) must establish the basis upon which the transfer of Personal Data is being made, i.e.:*
   1. *Data Controller-to-Data Controller (Module One);*
   2. *Data Controller-to- Data Processor (Module Two);*
   3. *Data Processor-to- Data Processor (Module Three); or*
   4. *Data Processor-to- Data Controller (Module Four).*
4. *Throughout these Clauses, certain provisions are marked as applying only to a certain Modules (see sub-paragraph (c) a. – d. immediately above). Prior to entering into these Clauses, the Parties should remove any content marked as applicable to any Module that does not apply to the transfer they are making.*
5. *The Clauses for the transfer of Personal Data on a Data Controller-to-Data Processor basis are also sufficient to meet the requirements under Article 28(3) of the QFC DPR 2021* *and Rule 7 of the QFC Data Protection Rules Version 2 2021 (“QFC DP Rules 2021”). This means that if these Clauses are used for such transfer on a Data Controller-to-Data Processor basis, then it is not necessary to also enter into a separate agreement relating to the Processing of Personal Data pursuant to Article 28(3) of the QFC DPR 2021 and Rule 7 of the QFC DP Rules 2021]*

**SECTION** I

## Purpose, scope and definitions

* 1. The purpose of these standard contractual clauses is to ensure compliance with the requirements of the Qatar Financial Centre (“**QFC**”) Data Protection Regulations 2021 (“**QFC DPR 2021**”) relating to the transfer of Personal Data outside the QFC.

* 1. The parties:
     1. the natural or legal persons, public authorities, agencies or other bodies transferring the Personal Data, as listed in ANNEX I.A. (the “**data exporter**”), and
     2. the entities in a jurisdiction outside of the QFC receiving the Personal Data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in in ANNEX I.A. (the “**data importer**”),

((a) and (b) together the “**Parties**”),

have agreed to these standard contractual clauses (the “**Clauses**”).

* 1. These Clauses apply with respect to the transfer of Personal Data as specified in ANNEX I.B.
  2. The appendix to these Clauses containing the Annexes (the “Appendix“) forms an integral part of these Clauses.

## Effect and invariability of the Clauses

* 1. These Clauses set out appropriate safeguards, including enforceable Data Subject rights and effective legal remedies, pursuant to Articles 24(1) and 24(2) of the QFC DPR 2021 and, with respect to Personal Data transfers from Data Controllers to Data Processors and Data Processors to Data Processors, standard contractual clauses pursuant to Article 28(3) of the QFC DPR 2021 and Section 7 of the QFC DP Rules 2021, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the rights or legitimate interests of Data Subjects.
  2. These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of the QFC DPR 2021.

## Third-party beneficiaries

* 1. Data Subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and data importer, with the following exceptions:
     1. ‎Clause 1, ‎Clause 2, ‎Clause 3, ‎Clause 6, ‎Clause 7;
     2. ‎Clause 8 - Module One: Clause ‎8.5(e) and Clause ‎8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1(b) and Clause 8.3(b);
     3. Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);
     4. Clause 12 - Module One: ‎Clause 12(a) and ‎(d); Modules Two and Three: Clause 12(a), (d) and (f);
     5. Clause 13;
     6. Clause 15.1(c), (d) and (e);
     7. Clause 16(e);
     8. Clause 18.
  2. Paragraph 3.1 is without prejudice to rights of Data Subjects under the QFC DPR 2021.

## Interpretation

* 1. Where these Clauses use capitalised terms that are defined in the QFC DPR 2021, those terms have the same meaning as in the QFC DPR 2021.
  2. These Clauses must be read and interpreted in the light of the provisions of the QFC DPR 2021.
  3. These Clauses must not be interpreted in a way that conflicts with rights and obligations provided for in the QFC DPR 2021.

## Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into after, these Clauses prevail.

# 

## Description of the transfer(s)

The details of the transfer(s), and in particular the categories of Personal Data that are transferred and the purpose(s) for which they are transferred, are specified in ANNEX I.B.

# [Optional]

## Docking clause

* 1. An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing ANNEX I.A.
  2. Once it has completed the Appendix and signed ANNEX I.A, the acceding entity becomes a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in ANNEX I.A.
  3. The acceding entity has no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

## Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

MODULE ONE: Transfer Data Controller to Data Controller

* 1. Purpose limitation

The data importer must Process the Personal Data only for the specific purpose(s) of the transfer, as set out in ANNEX I.B. It may only Process the Personal Data for another purpose:

* + 1. where it has obtained the Data Subject’s prior consent;
    2. where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
    3. where necessary in order to protect the vital interests of the Data Subject or of another natural person.
  1. Transparency
     1. In order to enable Data Subjects to effectively exercise their rights pursuant to Clause 10, the data importer must inform them, either directly or through the data exporter:
        1. of its identity and contact details;
        2. of the categories of Personal Data Processed;
        3. of the right to obtain a copy of these Clauses; and
        4. where it intends to onward transfer the Personal Data, of details of the Recipient or categories of Recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.
     2. Paragraph (a) must not apply where the Data Subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer must, to the extent possible, make the information publicly available.
     3. On request, the Parties must make a copy of these Clauses, including the Appendix as completed by them, available to the Data Subject free of charge. To the extent necessary to protect business secrets or other confidential information, including Personal Data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but must provide a meaningful summary where the Data Subject would otherwise not be able to understand its content or exercise his or her rights. On request, the Parties must provide the Data Subject with the reasons for the redactions, to the extent possible without revealing the redacted information.
     4. Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 14 and 15 of the QFC DPR 2021.
  2. Accuracy and data minimisation
     1. Each Party must ensure that the Personal Data is accurate and, where necessary, kept up to date. The data importer must take every reasonable step to ensure that Personal Data that is inaccurate, having regard to the purpose(s) of Processing, is erased or corrected without delay.
     2. If one of the Parties becomes aware that the Personal Data it has transferred or received is inaccurate, or has become outdated, it must inform the other Party without undue delay.
     3. The data importer must ensure that the Personal Data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of Processing.
  3. Storage limitation

The data importer must retain the Personal Data for no longer than necessary for the purpose(s) for which it is Processed (hereafter **“Retention Period”**). It must put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation[[1]](#footnote-1) of the Personal Data and all back-ups at the end of the Retention Period.

* 1. Security of Processing
     1. The data importer and the data exporter must implement appropriate technical and organisational measures to ensure the security of the Personal Data, including during transmission from data exporter to data importer, and protection against a Personal Data Breach. In assessing the appropriate level of security, the Parties must take due account of the available technology, the costs of implementation, the nature, scope, context and purpose(s) of Processing and the risks involved in the Processing for the Data Subject. The Parties must in particular consider having recourse to encryption or De-identification, including during transmission, where the purpose of Processing can be fulfilled in that manner.
     2. The Parties have agreed on the technical and organisational measures set out in ANNEX II. The data importer must carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
     3. The data importer must ensure that persons authorised to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
     4. In the event of a Personal Data Breach concerning Personal Data Processed by the data importer under these Clauses, the data importer must take appropriate measures to address the Personal Data Breach, including measures to mitigate its possible adverse effects.
     5. In case of a Personal Data Breach that is likely to result in a risk to the rights and legitimate interests of Data Subjects, the data importer must without undue delay and, where feasible, not later than 72 hours after having become aware of the Personal Data Breach, notify both the data exporter and the QFC Data Protection Office pursuant to Clause 13. Such notification must:
        1. describe the nature of the Personal Data Breach including:
           1. the categories of Data Subjects affected;
           2. the approximate number of Data Subjects affected;
           3. the categories and approximate number of Personal Data records affected;
        2. give the name and contact details of a person from whom more information can be obtained;
        3. describe the likely consequences of the Personal Data Breach;
        4. describe the measures that the data importer 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;
        5. if the notification is not made within 72 hours after the data importer becoming aware of the Personal Data Breach, give reasons for the delay.
     6. In case of a Personal Data Breach, the data importer must consider notifying any Personal Data Breaches to affected Data Subjects, taking into account the risk to their rights and legitimate interests, if necessary in cooperation with the data exporter. If such a notification is given it must use clear and plain language and must contain at least:
        1. the nature of the Personal Data Breach;
        2. the likely consequences of the Personal Data Breach; and
        3. a description of the measures taken or proposed to be taken by the data importer to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.
     7. The data importer must document all relevant facts relating to the Personal Data Breach, including its effects and any remedial action taken, and keep a record thereof.
  2. Sensitive Personal Data

Where the transfer involves Sensitive Personal Data, the data importer must apply specific restrictions and additional safeguards adapted to the specific nature of the Personal Data described in ANNEX I.B, and the risks involved. This may include restricting the personnel permitted to access the Sensitive Personal Data, additional security measures (such as De-identification) and additional restrictions with respect to further disclosure.

* 1. Onward transfers
     1. The data importer must not disclose the Personal Data to a third party located outside the QFC (in the same jurisdiction as the data importer or in another jurisdiction, “Onward Transfer”) unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an Onward Transfer by the data importer may only take place if:
        1. it is to a jurisdiction benefitting from an adequacy decision pursuant to Article 23 of the QFC DPR 2021 that covers the Onward Transfer; or
        2. the third party otherwise ensures appropriate safeguards pursuant to Article 24 of the QFC DPR 2021 with respect to the Processing in question.
     2. Any Onward Transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

* 1. Processing under the authority of the data importer

The data importer must ensure that any person acting under its authority, including a Data Processor, Processes the Personal Data only on its instructions.

* 1. Documentation and compliance
     1. Each Party must be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer must keep appropriate documentation of the Processing activities carried out under its responsibility.
     2. The data importer must make such documentation available to the QFC Data Protection Office on request.

MODULE TWO: Transfer Data Controller to Data Processor

* 1. Instructions
     1. The data importer must Process the Personal Data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
     2. The data importer must immediately inform the data exporter if it is unable to follow those instructions.
  2. Purpose limitation

The data importer must Process the Personal Data only for the specific purpose(s) of the transfer, as set out in ANNEX I.B, unless on further written instructions from the data exporter.

* 1. Transparency

On request, the data exporter must make a copy of these Clauses, including the Appendix as completed by the Parties, available to the Data Subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in ANNEX II and Personal Data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but must provide a meaningful summary where the Data Subject would, due to such redactions, otherwise not be able to understand its content or exercise his or her rights. On request, the Parties must provide the Data Subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 14 and 15 of the QFC DPR 2021.

* 1. Accuracy

If the data importer becomes aware that the Personal Data it has received is inaccurate, or has become outdated, it must inform the data exporter without undue delay. In this case, the data importer must cooperate with the data exporter to erase or rectify the Personal Data.

* 1. Duration of Processing and erasure or return of Personal Data

Processing by the data importer must only take place for the duration specified in ANNEX I.B. After the end of the provision of the Processing services, the data importer must, at the choice of the data exporter, delete all Personal Data Processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all Personal Data Processed on its behalf and delete existing copies. Until the Personal Data is deleted or returned, the data importer must continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the Personal Data, the data importer warrants that it must continue to ensure compliance with these Clauses and must only Process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices that would cause it not to be able to comply with the requirements under Clause 14(a).

* 1. Security of Processing
     1. The data importer and the data exporter must implement appropriate technical and organisational measures to ensure the security of the Personal Data, including during transmission from data exporter to data importer, and protection against a Personal Data Breach. In assessing the appropriate level of security, the Parties must take due account of the available technology, the costs of implementation, the nature, scope, context and purpose(s) of Processing and the risks involved in the Processing for the Data Subjects. The Parties must in particular consider having recourse to encryption or De-identification, including during transmission, where the purpose of Processing can be fulfilled in that manner. In case of De-identification, the additional information for attributing the Personal Data to a specific Data Subject must, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer must at least implement the technical and organisational measures specified in ANNEX II. The data importer must carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
     2. The data importer must grant access to the Personal Data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It must ensure that persons authorised to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
     3. In the event of a Personal Data Breach concerning Personal Data Processed by the data importer under these Clauses, the data importer must take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer must also notify the data exporter without undue delay after having become aware of the breach. Such notification must contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of Data Subjects and Personal Data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification must contain the information then available and further information must, as it becomes available, subsequently be provided without undue delay.
     4. The data importer must cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under the QFC DPR 2021, in particular to notify the QFC Data Protection Office and the affected Data Subjects, if deemed necessary by the Data Controller, taking into account the nature of Processing and the information available to the data importer.
  2. Sensitive Personal Data

Where the transfer involves Sensitive Personal Data, the data importer must apply the specific restrictions and additional safeguards described in ANNEX I.B.

* 1. Onward transfers
     1. The data importer must only disclose the Personal Data to a third party on documented instructions from the data exporter. In addition, the Personal Data may only be disclosed to a third party located outside the QFC (in the same jurisdiction as the data importer or in another jurisdiction, hereinafter “Onward Transfer”) if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:
        1. the Onward Transfer is to a jurisdiction benefitting from an adequacy decision pursuant to Article 23 of the QFC DPR 2021 that covers the Onward Transfer; or
        2. the third party otherwise ensures appropriate safeguards pursuant to Article 24 of the QFC DPR 2021 with respect to the Processing in question.
     2. Any Onward Transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.
  2. Documentation and compliance
     1. The data importer must promptly and adequately deal with enquiries from the data exporter that relate to the Processing under these Clauses.
     2. The Parties must be able to demonstrate compliance with these Clauses. In particular, the data importer must keep appropriate documentation on the Processing activities carried out on behalf of the data exporter.
     3. The data importer must make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter’s request, allow for and contribute to audits of the Processing activities covered by these Clauses, at reasonable intervals or if there are indications of non­compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.
     4. The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and must, where appropriate, be carried out with reasonable notice.
     5. The Parties must make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the QFC Data Protection Office on request.

MODULE THREE: Transfer Data Processor to Data Processor

* 1. Instructions
     1. The data exporter has informed the data importer that it acts as Data Processor under the instructions of its Data Controller(s), which the data exporter must make available to the data importer prior to Processing.
     2. The data importer must Process the Personal Data only on written instructions from the Data Controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions must not conflict with the instructions from the Data Controller. The Data Controller or data exporter may give further documented instructions regarding the Personal Data Processing throughout the duration of the contract.
     3. The data importer must immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the Data Controller, the data exporter must immediately notify the Data Controller.
     4. The data exporter warrants that it has imposed the same Personal Data protection obligations on the data importer[[2]](#footnote-2):
        1. as set out in the contract the data exporter has with the Data Controller for the provision of Processing services; or
        2. which are imposed upon the data exporter pursuant to any other legal act under any enactment or subordinate legislation applicable in the QFC by which the data exporter is subject to comply for the purpose of providing its service to, or conduct Processing for, the Data Controller.
  2. Purpose limitation

The data importer must Process the Personal Data only for the specific purpose(s) of the transfer, as set out in ANNEX I.B, unless on further written instructions from the data exporter.

* 1. Transparency

On request, the data exporter must make a copy of these Clauses, including the Appendix as completed by the Parties, available to the Data Subject free of charge. To the extent necessary to protect business secrets or other confidential information, including Personal Data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but must provide a meaningful summary where the Data Subject would otherwise not be able to understand its content or exercise his or her rights. On request, the Parties must provide the Data Subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

* 1. Accuracy

If the data importer becomes aware that the Personal Data it has received is inaccurate, or has become outdated, it must inform the data exporter without undue delay. In this case, the data importer must cooperate with the data exporter to rectify or erase the Personal Data.

* 1. Duration of Processing and erasure or return of Personal Data

Processing by the data importer must only take place for the duration specified in ANNEX I.B. After the end of the provision of the Processing services, the data importer must, at the choice of the data exporter, delete all Personal Data Processed on behalf of the Data Controller and certify to the data exporter that it has done so, or return to the data exporter all Personal Data Processed on its behalf and delete existing copies. Until the Personal Data is deleted or returned, the data importer must continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the Personal Data, the data importer warrants that it must continue to ensure compliance with these Clauses and must only Process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices that would cause it not to be able to comply with the requirements under Clause 14(a).

* 1. Security of Processing
     1. The data importer and the data exporter must implement appropriate technical and organisational measures to ensure the security of the Personal Data, including during transmission from data exporter and data importer, and protection against a Personal Data Breach. In assessing the appropriate level of security, the Parties must take due account of the available technology, the costs of implementation, the nature, scope, context and purpose(s) of Processing and the risks involved in the Processing for the Data Subject(s). The Parties must in particular consider having recourse to encryption or De-identification, including during transmission, where the purpose of Processing can be fulfilled in that manner. In case of De-identification, the additional information for attributing the Personal Data to a specific Data Subject must, where possible, remain under the exclusive control of the data exporter or the Data Controller. In complying with its obligations under this paragraph, the data importer must at least implement the technical and organisational measures specified in ANNEX II. The data importer must carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
     2. The data importer must grant access to the Personal Data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It must ensure that persons authorised to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
     3. In the event of a Personal Data Breach concerning Personal Data Processed by the data importer under these Clauses, the data importer must take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer must also notify, without undue delay, the data exporter and, where appropriate and feasible, the Data Controller after having become aware of the breach. Such notification must contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of Data Subjects and Personal Data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification must contain the information then available and further information must, as it becomes available, subsequently be provided without undue delay.
     4. The data importer must cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under the QFC DPR 2021, in particular to notify its Data Controller so that the latter may in turn notify the QFC Data Protection Office and the affected Data Subjects, taking into account the nature of Processing and the information available to the data importer.
  2. Sensitive Personal Data

Where the transfer involves Sensitive Personal Data, the data importer must apply the specific restrictions and additional safeguards set out in ANNEX I.B.

* 1. Onward transfers
     1. The data importer must only disclose the Personal Data to a third party on documented instructions from the Data Controller, as communicated to the data importer by the data exporter. In addition, the Personal Data may only be disclosed to a third party located outside the QFC (in the same jurisdiction as the data importer or in another jurisdiction, the “Onward Transfer”) if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:
        1. the Onward Transfer is to a jurisdiction benefitting from an adequacy decision pursuant to Article 23 of the QFC DPR 2021 that covers the Onward Transfer; or
        2. the third party otherwise ensures appropriate safeguards pursuant to Article 24 of the QFC DPR 2021.
     2. Any Onward Transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.
  2. Documentation and compliance
     1. The data importer must promptly and adequately deal with enquiries from the data exporter or the Data Controller that relate to the Processing under these Clauses.
     2. The Parties must be able to demonstrate compliance with these Clauses. In particular, the data importer must keep appropriate documentation on the Processing activities carried out on behalf of the Data Controller.
     3. The data importer must make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, and must provide it to the Data Controller.
     4. The data importer must allow for and contribute to audits by the data exporter of the Processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same applies where the data exporter requests an audit on instructions of the Data Controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.
     5. Where the audit is carried out on the instructions of the Data Controller, the data exporter must make the results available to the Data Controller.
     6. The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and must, where appropriate, be carried out with reasonable notice.
     7. The Parties must make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the QFC Data Protection Office on request.

MODULE FOUR: Transfer Data Processor to Data Controller

* 1. Instructions
     1. The data exporter must Process the Personal Data only on documented instructions from the data importer acting as its Data Controller.
     2. The data exporter must immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe the QFC DPR 2021.
     3. The data importer must refrain from any action that would prevent the data exporter from fulfilling its obligations under the QFC DPR 2021, including in the context of sub-Processing or as regards cooperation with competent Supervisory Authorities.
     4. After the end of the provision of the Processing services, the data exporter must, at the choice of the data importer, delete all Personal Data Processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all Personal Data Processed on its behalf and delete existing copies.
  2. Security of Processing
     1. The Parties must implement appropriate technical and organisational measures to ensure the security of the Personal Data, including during transmission, and protection against a Personal Data Breach. In assessing the appropriate level of security, the Parties must take due account of the available technology, the costs of implementation, the nature of the Personal Data[[3]](#footnote-3), the nature, scope, context and purpose(s) of Processing and the risks involved in the Processing for the Data Subjects, and in particular consider having recourse to encryption or De-identification, including during transmission, where the purpose of Processing can be fulfilled in that manner.
     2. The data exporter must assist the data importer in ensuring appropriate security of the data in accordance with paragraph 8.2(a). In case of a Personal Data Breach concerning the Personal Data Processed by the data exporter under these Clauses, the data exporter must notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.
     3. The data exporter must ensure that persons authorised to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
  3. Documentation and compliance
     1. The Parties must be able to demonstrate compliance with these Clauses.
     2. The data exporter must make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

# 

## Use of sub-Data Processors

[**EXPLANATORY NOTE:** This clause is not relevant to Modules 1 and 4. Where using these Clauses only for Modules 1 or 4 then remove Modules 2 and 3 below and language underneath those modules and replace the following language with “Clause 9 not used”.]

MODULE TWO: Transfer Data Controller to Data Processor

[**EXPLANATORY NOTE**: Choose either OPTION 1 or OPTION 2 and remove the other option.]

* + 1. [OPTION 1] SPECIFIC PRIOR AUTHORISATION The data importer must not sub­contract any of its Processing activities performed on behalf of the data exporter under these Clauses to a sub-Data Processor without the data exporter’s prior specific written authorisation. The data importer must submit the request for specific authorisation at least [*Specify time period*] prior to the engagement of the sub-Data Processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-Data Processors already authorised by the data exporter can be found in ANNEX III. The Parties must keep ANNEX III up to date.

[OR]

* + 1. [OPTION 2] GENERAL WRITTEN AUTHORISATION The data importer has the data exporter’s general authorisation for the engagement of sub-Data Processor(s) from an agreed list. The data importer must specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-Data Processors at least [*Specify time period*] in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-Data Processor(s). The data importer must provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.
    2. Where the data importer engages a sub-Data Processor to carry out specific Processing activities (on behalf of the data exporter), it must do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for Data Subjects.[[4]](#footnote-4) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer must ensure that the sub-Data Processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
    3. The data importer must provide, at the data exporter’s request, a copy of such a sub-Data Processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including Personal Data, the data importer may redact the text of the agreement prior to sharing a copy with the data exporter.
    4. The data importer remains fully responsible to the data exporter for the performance of the sub-Data Processor’s obligations under its contract with the data importer. The data importer must notify the data exporter of any failure by the sub-Data Processor to fulfil its obligations under that contract.
    5. The data importer must agree a third-party beneficiary clause with the sub-Data Processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter must have the right to terminate the sub-Data Processor contract and to instruct the sub-Data Processor to erase or return the Personal Data.

MODULE THREE: Transfer Data Processor to Data Processor

[**EXPLANATORY NOTE**: Choose either OPTION 1 or OPTION 2 and remove the other option.]

* + 1. [OPTION 1] SPECIFIC PRIOR AUTHORISATION The data importer must not sub­contract any of its Processing activities performed on behalf of the data exporter under these Clauses to a sub-Data Processor without the prior specific written authorisation of the Data Controller. The data importer must submit the request for specific authorisation to the Data Controller at least [*Specify time period*] prior to the engagement of the sub-Data Processor, together with the information necessary to enable the Data Controller to decide on the authorisation. It must inform the data exporter of such engagement. The list of sub-Data Processors already authorised by the Data Controller can be found in ANNEX III. The Parties must keep ANNEX III up to date.

[OR]

* + 1. [OPTION 2] GENERAL WRITTEN AUTHORISATION The data importer has the Data Controller’s general authorisation for the engagement of sub-Data Processor(s) from an agreed list. The data importer must specifically inform the Data Controller in writing of any intended changes to that list through the addition or replacement of sub-Data Processors at least *[Specify time period*] in advance, thereby giving the Data Controller sufficient time to be able to object to such changes prior to the engagement of the sub-Data Processor(s). The data importer must provide the Data Controller with the information necessary to enable the Data Controller to exercise its right to object. The data importer must inform the data exporter of the engagement of the sub-Data Processor(s).
    2. Where the data importer engages a sub-Processor to carry out specific Processing activities (on behalf of the Data Controller), it must do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for Data Subjects.[[5]](#footnote-5) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer must ensure that the sub-Data Processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
    3. The data importer must provide, at the data exporter’s or Data Controller’s request, a copy of such a sub-Data Processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including Personal Data, the data importer may redact the text of the agreement prior to sharing a copy.
    4. The data importer remains fully responsible to the data exporter for the performance of the sub-Data Processor’s obligations under its contract with the data importer. The data importer must notify the data exporter of any failure by the sub-Data Processor to fulfil its obligations under that contract.
    5. The data importer must agree a third-party beneficiary clause with the sub-Data Processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter must have the right to terminate the sub-Data Processor contract and to instruct the sub-Data Processor to erase or return the Personal Data.

## Data Subject rights

MODULE ONE: Transfer Data Controller to Data Controller

* + 1. The data importer, where relevant with the assistance of the data exporter, must deal with any enquiries and requests it receives from a Data Subject relating to the Processing of his or her Personal Data and the exercise of his or her rights under these Clauses without undue delay and at the latest within 30 days of the receipt of the enquiry or request.[[6]](#footnote-6) The data importer must take appropriate measures to facilitate such enquiries, requests and the exercise of Data Subject rights. Any information provided to the Data Subject must be in an intelligible and easily accessible form, using clear and plain language.
    2. In particular, upon request by the Data Subject the data importer must, free of charge:
       1. provide confirmation to the Data Subject as to whether Personal Data concerning him or her is being Processed and, where this is the case, a copy of the Personal Data relating to him or her and the information in ANNEX I; if Personal Data has been or will be Onward Transferred, provide information on Recipients or categories of Recipients (as appropriate with a view to providing meaningful information) to which the Personal Data has been or will be Onward Transferred, the purpose of such Onward Transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with the QFC Data Protection Office in accordance with Clause 11(c)(i);
       2. rectify inaccurate or incomplete Personal Data concerning the Data Subject;
       3. erase Personal Data concerning the Data Subject if such Personal Data is being or has been Processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the Data Subject withdraws the Consent on which the Processing is based.
    3. Where the data importer Processes the Personal Data for direct marketing purposes, it must cease Processing for such purposes if the Data Subject objects to it.
    4. The data importer must not make a decision based solely on the automated Processing of the Personal Data transferred (hereinafter “Automated Decision”), which would produce legal effects concerning the Data Subject or similarly significantly affect him or her, unless with the explicit Consent of the Data Subject or if authorised to do so under the laws of the jurisdiction of destination, provided that such laws lays down suitable measures to safeguard the Data Subject’s rights and legitimate interests. In this case, the data importer must, where necessary in cooperation with the data exporter:
       1. inform the Data Subject about the envisaged Automated Decision, the envisaged consequences and the logic involved; and
       2. implement suitable safeguards, at least by enabling the Data Subject to contest the decision, express his or her point of view and obtain review by a human being.
    5. Where requests from a Data Subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.
    6. The data importer may refuse a Data Subject’s request if such refusal is allowed under the laws of the jurisdiction of destination and is necessary and proportionate to protect one of the objectives listed in Annex IV.
    7. If the data importer intends to refuse a Data Subject’s request, it must inform the Data Subject of the reasons for the refusal and the possibility of lodging a complaint with the QFC Data Protection Office and seeking judicial redress.

MODULE TWO: Transfer Data Controller to Data Processor

* + 1. The data importer must promptly notify the data exporter of any request it has received from a Data Subject. It must not respond to that request itself unless it has been authorised to do so by the data exporter.
    2. The data importer must assist the data exporter in fulfilling its obligations to respond to Data Subjects’ requests for the exercise of their rights under the QFC DPR 2021. In this regard, the Parties must set out in ANNEX II the appropriate technical and organisational measures, taking into account the nature of the Processing, by which the assistance must be provided, as well as the scope and the extent of the assistance required.
    3. In fulfilling its obligations under paragraphs (a) and (b), the data importer must comply with the instructions from the data exporter.

MODULE THREE: Transfer Data Processor to Data Processor

* + 1. The data importer must promptly notify the data exporter and, where appropriate, the Data Controller of any request it has received from a Data Subject, without responding to that request unless it has been authorised to do so by the Data Controller.
    2. The data importer must assist, and where appropriate or necessary in cooperation with the data exporter, the Data Controller in fulfilling its obligations to respond to Data Subjects’ requests for the exercise of their rights under the QFC DPR 2021. In this regard, the Parties must set out in ANNEX II the appropriate technical and organisational measures, taking into account the nature of the Processing, by which the assistance must be provided, as well as the scope and the extent of the assistance required.
    3. In fulfilling its obligations under paragraphs (a) and (b), the data importer must comply with the instructions from the Data Controller, as communicated by the data exporter.

MODULE FOUR: Transfer Data Processor to Data Controller

The Parties must assist each other in responding to enquiries and requests made by Data Subjects under the local law applicable to the data importer or, for Personal Data Processing by the data exporter in the QFC, under the QFC DPR 2021.

## Redress

* + 1. The data importer must inform Data Subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It must deal promptly with any complaints it receives from a Data Subject.

[**EXPLANATORY NOTE**: The wording immediately below in [square brackets] is optional only and can be removed.]

[The data importer agrees that Data Subjects may also lodge a complaint with an independent dispute resolution body[[7]](#footnote-7) at no cost to the Data Subject. It must inform the Data Subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

MODULE ONE: Transfer Controller to Controller

MODULE TWO: Transfer Controller to Processor

MODULE THREE: Transfer Processor to Processor

* + 1. In case of a dispute between a Data Subject and one of the Parties as regards compliance with these Clauses, that Party must use its best efforts to resolve the issue amicably in a timely fashion. The Parties must keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
    2. Where the Data Subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer must accept the decision of the Data Subject to:
       1. lodge a complaint with the QFC Data Protection Office pursuant to Clause 13;
       2. refer the dispute to the competent courts within the meaning of Clause 18.
    3. The data importer must abide by a decision that is binding under applicable law.
    4. The data importer agrees that the choice made by the Data Subject in Clause 11(c) must not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable law.

## Liability

MODULE ONE: Transfer Data Controller to Data Controller

MODULE FOUR: Transfer Data Processor to Data Controller

* + 1. Each Party is liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
    2. Each Party is liable to the Data Subject, and the Data Subject is entitled to receive compensation, for any material or non-material damages that the Party causes the Data Subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under the QFC DPR 2021.
    3. Where more than one Party is responsible for any damage caused to the Data Subject as a result of a breach of these Clauses, all responsible Parties are jointly and severally liable and the Data Subject is entitled to bring an action in court against any of these Parties.
    4. The Parties agree that if one Party is held liable under paragraph (a), it is entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.
    5. The data importer may not invoke the conduct of a Data Processor or sub-Data Processor to avoid its own liability.

MODULE TWO: Transfer Data Controller to Data Processor

MODULE THREE: Transfer Data Processor to Data Processor

* + 1. Each Party is liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
    2. The data importer is liable to the Data Subject, and the Data Subject is entitled to receive compensation, for any material or non-material damages the data importer or its sub-Data Processor causes the Data Subject by breaching the third-party beneficiary rights under these Clauses.
    3. Notwithstanding paragraph (b), the data exporter is liable to the Data Subject, and the Data Subject is entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-Data Processor) causes the Data Subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a Data Processor acting on behalf of a Data Controller, to the liability of the Data Controller under applicable law.
    4. The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-Data Processor), it is entitled to claim back from the data importer that part of the compensation corresponding to the data importer’s responsibility for the damage.
    5. Where more than one Party is responsible for any damage caused to the Data Subject as a result of a breach of these Clauses, all responsible Parties are jointly and severally liable and the Data Subject is entitled to bring an action in court against any of these Parties.
    6. The Parties agree that if one Party is held liable under paragraph (e), it is entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.
    7. The data importer may not invoke the conduct of a sub-Data Processor to avoid its own liability.

# 

## Supervision

The data importer agrees to submit itself to the jurisdiction of and cooperate with the QFC Data Protection Office in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the QFC Data Protection Office, including remedial and compensatory measures. The data importer must provide the QFC Data Protection Office with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

# 

## Local laws and practices affecting compliance with the Clauses

MODULE ONE: Transfer Data Controller to Data Controller

MODULE TWO: Transfer Data Controller to Data Processor

MODULE THREE: Transfer Data Processor to Data Processor

MODULE FOUR: Transfer Data Processor to Data Controller (where the QFC Data Processor combines the Personal Data received from Data Controllers outside the QFC with Personal Data collected by the Data Processor in the QFC)

* + 1. The Parties warrant that they have no reason to believe that the laws and practices in the jurisdiction of destination applicable to the Processing of the Personal Data by the data importer, including any requirements to disclose Personal Data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the rights and legitimate interests of Data Subjects and do not exceed what is necessary and proportionate to safeguard one of the objectives listed in Annex IV, are not in contradiction with these Clauses.
    2. The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
       1. the specific circumstances of the transfer, including the length of the Processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of Processing; the categories and format of the transferred Personal Data; the economic sector in which the transfer occurs; the storage location of the Personal Data transferred;
       2. the laws and practices of the jurisdiction of destination – including those requiring the disclosure of Personal Data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[[8]](#footnote-8);
       3. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the Processing of the Personal Data in the jurisdiction of destination.
    3. The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it must continue to cooperate with the data exporter in ensuring compliance with these Clauses.
    4. The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
    5. The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices that would cause it not to be able to comply with the requirements under paragraph (a), including following a change in the laws of the jurisdiction of destination or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). [For Module Three: The data exporter must forward the notification to the Data Controller.]
    6. Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter must promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and data importer to address the situation [for Module Three: , if appropriate in consultation with the Data Controller]. The data exporter must suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the Data Controller or] the QFC Data Protection Office to do so. In this case, the data exporter is entitled to terminate the contract, insofar as it concerns the Processing of Personal Data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where these Clauses are terminated pursuant to this Clause, Clause 16(d) and Clause 16(e) must apply.

## Obligations of the data importer in case of access by public authorities

MODULE ONE: Transfer Data Controller to Data Controller

MODULE TWO: Transfer Data Controller to Data Processor

MODULE THREE: Transfer Data Processor to Data Processor

MODULE FOUR: Transfer Data Processor to Data Controller (where the QFC Data Processor combines the Personal Data received from Data Controllers outside the QFC with Personal Data collected by the Data Processor in the QFC)

* 1. Notification
     1. The data importer agrees to notify the data exporter and, where possible, the Data Subject promptly (if necessary with the help of the data exporter) if it:
        1. receives a legally binding request from a public authority, including judicial authorities, under the laws of the jurisdiction of destination for the disclosure of Personal Data transferred pursuant to these Clauses; such notification must include information about the Personal Data requested, the requesting authority, the legal basis for the request and the response provided; or
        2. becomes aware of any direct access by public authorities to Personal Data transferred pursuant to these Clauses in accordance with the laws of the jurisdiction of destination; such notification must include all information available to the importer.

[For Module Three: The data exporter must forward the notification to the Data Controller.]

* + 1. If the data importer is prohibited from notifying the data exporter or the Data Subject under the laws of the jurisdiction of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
    2. Where permissible under the laws of the jurisdiction of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authorities, whether requests have been challenged and the outcome of such challenges, etc.). [For Module Three: The data exporter must forward the information to the Data Controller.]
    3. The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the QFC Data Protection Office on request.
    4. Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.
  1. Review of legality and data minimisation
     1. The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the jurisdiction of destination, applicable obligations under international law and principles of international comity. The data importer must, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer must seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It must not disclose the Personal Data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).
     2. The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the jurisdiction of destination, make the documentation available to the data exporter. It must also make it available to the QFC Data Protection Office on request. [For Module Three: The data exporter must make the assessment available to the Data Controller.]
     3. The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

# SECTION IV – FINAL PROVISIONS

# 

## Non-compliance with the Clauses and termination

* + 1. The data importer must promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
    2. In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter must suspend the transfer of Personal Data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
    3. The data exporter is entitled to terminate the contract, insofar as it concerns the Processing of Personal Data under these Clauses, where:
       1. the data exporter has suspended the transfer of Personal Data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within 30 days of suspension;
       2. the data importer is in substantial or persistent breach of these Clauses; or
       3. the data importer fails to comply with a binding decision of a competent court or authority regarding its obligations under these Clauses.

In these cases, it must inform the QFC Data Protection Office [for Module Three: and the Data Controller] of termination caused by such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

* + 1. [For Modules One, Two and Three: Personal Data that has been transferred prior to the termination of the contract pursuant to paragraph (c) must at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same must apply to any copies of the Personal Data.] [For Module Four: Personal Data collected by the data exporter in the QFC that has been transferred prior to the termination of the contract pursuant to paragraph (c) must immediately be deleted in its entirety, including any copy thereof.] The data importer must certify the deletion of the Personal Data to the data exporter. Until the Personal Data is deleted or returned, the data importer must continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred Personal Data, the data importer warrants that it must continue to ensure compliance with these Clauses and must only Process the Personal Data to the extent and for as long as required under that local law.
    2. Either Party may revoke its agreement to be bound by these Clauses where the QFC Data Protection Office adopts a decision pursuant to Article 23(1) of the QFC DPR 2021 that covers the transfer of Personal Data to which these Clauses apply. This is without prejudice to other obligations applying to the Processing in question under the QFC DPR 2021.

## Governing law

MODULE ONE: Transfer Data Controller to Data Controller

MODULE TWO: Transfer Data Controller to Data Processor

MODULE THREE: Transfer Data Processor to Data Processor

These Clauses are governed by the laws of the Qatar Financial Centre.

MODULE FOUR: Transfer Data Processor to Data Controller

These Clauses are governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this is the law of \_\_\_\_\_\_\_ [*specify country*].

# 

## Choice of forum and jurisdiction

MODULE ONE: Transfer Data Controller to Data Controller

MODULE TWO: Transfer Data Controller to Data Processor

MODULE THREE: Transfer Data Processor to Data Processor

* + 1. Any dispute arising from these Clauses must be resolved by the courts of the Qatar Financial Centre.
    2. The Parties agree to submit themselves to the exclusive jurisdiction of such courts and must abide by any binding decision of the courts.

MODULE FOUR: Transfer Data Processor to Data Controller

* + 1. Any dispute arising from these Clauses must be resolved by the courts of \_\_\_\_\_ [specify country].
    2. The Parties agree to submit themselves to the exclusive jurisdiction of such courts.

APPENDIX

[**EXPLANATORY NOTE:** It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers or contractual relationship, where this transparency can be achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.]

ANNEX I

**A** - LIST OF PARTIES

MODULE ONE: Transfer Data Controller to Data Controller

MODULE TWO: Transfer Data Controller to Data Processor

MODULE THREE: Transfer Data Processor to Data Processor

MODULE FOUR: Transfer Data Processor to Data Controller

Data exporter(s):[**EXPLANATORY NOTE**: Please insert the identity and contact details of the data exporter(s) and, where applicable, of its/their Data Protection Officer]

Name: [*Insert*]

Address: [*Insert*]

Contact person’s name, position and contact details: [*Insert*]

Activities relevant to the Personal Data transferred under these Clauses: [*Insert*]

Signature and date: [*Insert*]

Role (Data Controller/Data Processor): [*Insert*]

[**EXPLANATORY NOTE:** Insert additional information if there is more than one data exporter]

Data importer(s):[**EXPLANATORY NOTE**: Please insert the identity and contact details of the data importer(s), including any contact person with responsibility for data protection]

Name: [Insert]

Address: [Insert]

Contact person’s name, position and contact details: [Insert]

Activities relevant to the Personal Data transferred under these Clauses: [Insert]

Signature and date: [Insert]

Role (Data Controller/Data Processor): [Insert]

[Insert additional information if there is more than one data importer]

**B** - DESCRIPTION OF TRANSFER

MODULE ONE: Transfer Data Controller to Data Controller

MODULE TWO: Transfer Data Controller to Data Processor

MODULE THREE: Transfer Data Processor to Data Processor

MODULE FOUR: Transfer Data Processor to Data Controller

**Categories of Data Subjects whose Personal Data is transferred**

[Insert]

[**EXPLANATORY NOTE:** List out the categories of Data Subjects whose Personal Data is being transferred. By way of example, these may include (but are not limited to): (i) the exporter’s employees; (ii) the exporter’s customers; and / or (iii) target customers, employees or representatives of the Data Controller’s third party service providers.]

**Categories of Personal Data transferred (including, if relevant, Sensitive Personal Data)**

[Insert]

[**EXPLANATORY NOTE:** List out the categories of Personal Data being transferred. By way of example only, these may include (but are not limited to): (i) contact details (name, email address, phone number, etc.); (ii) employment information (references, educational history, CV); (iii) financial information (banking details, credit history, payroll records).]

If any Sensitive Personal Data is transferred that must be set out clearly. It is also necessary to set out any applied restrictions or safeguards that fully take into consideration the nature of the Personal Data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the Personal Data, restrictions for Onward Transfers or additional security measures.]

**The frequency of the transfer (e.g. whether the Personal Data is transferred on a one-off or continuous basis).**

[Insert]

[**EXPLANATORY NOTE:** Describe how the data importer will receive, use, store and delete the Personal Data in scope. Provide details of any systems which will be used (both internal and third party).]

**Nature of the Processing**

[Insert]

[**EXPLANATORY NOTE:** Describe how the data importer will receive, use, store and delete the Personal Data in scope. Provide details of any systems which will be used (both internal and third party).]

**Purpose(s) of the Personal Data transfer and further Processing**

[Insert]

[**EXPLANATORY NOTE:** Describe the purpose for which the data importer is importing the Personal Data. For example, the data importer may be providing a service to the Data Controller which necessitates the Processing of Personal Data. If that is the case, details of the service being provided should be included underneath this sub-heading.]

**The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period**

[Insert]

[**EXPLANATORY NOTE:** Describe for how long the data importer must continue to Process the Personal Data, or the criteria which would be used to determine that period. For example, if the data importer must Process Personal Data for the duration for which certain services are being provided by the Data Processor to the Data Controller under a separate services agreement, the Term of that Services Agreement could be referenced here (subject to any provisions regarding extension).]

**For transfers to (sub-) Data Processors, also specify subject matter, nature and duration of the Processing**

[Insert]

[**EXPLANATORY NOTE:** The information set out at (1) – (6) above must also be provided with respect to any Processing by (sub-) Data Processors.]

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE ONE: Transfer Data Controller to Data Controller

MODULE TWO: Transfer Data Controller to Data Processor

MODULE THREE: Transfer Data Processor to Data Processor

*[****EXPLANATORY NOTE:*** *The technical and organisational measures used by your organisation must be described in specific (and not generic) terms in Annex II. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers. Alternatively, you can fulfil the requirement to describe technical and organisational measures by attaching your organisation’s data security policy or other similar document provided that the controls described are relevant to the Processing carried out under this agreement.]*

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the Processing, and the risks for the rights and legitimate interests of natural persons.

[Insert]

[**EXPLANATORY NOTE:** Examples of possible measures:

* Measures of De-identification and encryption of Personal Data
* Measures for ensuring ongoing confidentiality, integrity, availability and resilience of Processing systems and services
* Measures for ensuring the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident
* Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the Processing
* Measures for user identification and authorisation
* Measures for the protection of Personal Data during transmission
* Measures for the protection of Personal Data during storage
* Measures for ensuring physical security of locations at which Personal Data are Processed
* Measures for ensuring events logging
* Measures for ensuring system configuration, including default configuration
* Measures for internal IT and IT security governance and management
* Measures for certification/assurance of processes and products
* Measures for ensuring data minimisation
* Measures for ensuring data quality
* Measures for ensuring limited data retention
* Measures for ensuring accountability
* Measures for allowing data portability and ensuring erasure]

For transfers to (sub-) Data Processors, also describe the specific technical and organisational measures to be taken by the (sub-) Data Processor to be able to provide assistance to the Data Controller and, for transfers from a Data Processor to a sub-Data Processor, to the data exporter.

[Insert]

ANNEX III - LIST OF SUB-DATA PROCESSORS

MODULE TWO: Transfer Data Controller to Data Processor

MODULE THREE: Transfer Data Processor to Data Processor

[**EXPLANATORY NOTE:** This Annex must be completed for Modules Two and Three, in case of the specific authorisation of sub-Data Processors (Clause 9(a), Option 1).]

The Data Controller has authorised the use of the following sub-Data Processors:

Name: [Insert]

Address: [Insert]

Contact person’s name, position and contact details: [Insert]

Description of Processing (including a clear delimitation of responsibilities in case several sub-Data Processors are authorised): [Insert]

[Insert additional information at (2), (3), (4) etc. if there is more than one sub-Data Processor granted specific authorisation pursuant to Clause 9(a), Option 1).]

ANNEX IV - LIST OF SAFEGUARDS

List of safeguards per Clause 10 and Clause 14:

* national security, defence and public security;
* important objectives of general public interest in particular economic or financial interest such as monetary, budgetary and taxation matters, public health and social security;
* the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;
* public bodies or authorities, only to the extent that compliance would be likely to prejudice the proper discharge of their powers and functions as set out in law;
* the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
* Courts, judicial bodies or other individuals acting in a judicial or quasi-judicial capacity for the purposes of assessing a person’s suitability for judicial office or where the application of those provisions would be likely to prejudice their judicial independence or judicial proceedings;
* the protection of the Data Subject or the rights and legitimate interests of others;
* the enforcement of civil law claims.

1. This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone and that this process is irreversible. [↑](#footnote-ref-1)
2. See article 28(7) QFC DPR 2021, which states “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) [of article 28] must be imposed on that other Data Processor by a written contract.” [↑](#footnote-ref-2)
3. This includes whether the transfer and further Processing involves Sensitive Personal Data. [↑](#footnote-ref-3)
4. This requirement may be satisfied by the sub-Data Processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7 [↑](#footnote-ref-4)
5. This requirement may be satisfied by the sub-Data Processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7. [↑](#footnote-ref-5)
6. That period may be extended by a maximum of 60 days where necessary, taking into account the complexity and number of requests. The data importer must duly and promptly inform the Data Subject of any such extension. [↑](#footnote-ref-6)
7. The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards. [↑](#footnote-ref-7)
8. As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer must not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies. [↑](#footnote-ref-8)