Standard Contractual Clauses

*relating to the transfer of Personal Data outside the ADGM pursuant to
the Abu Dhabi Global Market Data Protection Regulations 2021*

[GUIDANCE:

(a) These Clauses (as defined in Clause 1 below) are intended to facilitate the lawful export of Personal Data under section 42(2) of the Abu Dhabi Global Market Data Protection Regulations 2021.

(b) 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.:

    a. Controller-to-Controller (Module One);

    b. Controller-to-Processor (Module Two);

    c. Processor-to-Processor (Module Three); or

    d. Processor-to-Controller (Module Four).

(c) Throughout these Clauses, certain provisions are marked as applying only to a certain Modules (see sub-paragraph (a) – (d) immediately above). Prior to entering into these Clauses, the Parties should remove any content marked as applicable to any Module other than the Module which applies to the transfer they are making.

(d) Where Personal Data is being transferred on a Controller-to-Processor basis, these Clauses are also sufficient to meet the requirements under section 26(3) of the DPR 2021. This means that it is not necessary to also enter into the SCCs relating to the Processing of Personal Data pursuant to section 26(3), (4) and (5) of the DPR 2021 or any other data processing agreement intended to meet the requirements of section 26(3).

(e) This Guidance should be removed prior to entering into these Clauses.]

SECTION I

Clause 1

Purpose and scope

1.1   The purpose of these standard contractual clauses is to ensure compliance with the requirements of the Abu Dhabi Global Market ("**ADGM**") Data Protection Regulations 2021 ("**DPR 2021**") relating to the transfer of Personal Data outside the ADGM.

1.2   The parties:

(a)   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

(b)   the entities in a jurisdiction outside of the ADGM receiving the Personal Data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in ANNEX I.A (the "**data importer**"),

((a) and (b) together the "**Parties**"),

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

1.3   These Clauses apply with respect to the transfer of Personal Data as specified in ANNEX I.B.

1.4   The Appendix to these Clauses containing the Annexes forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

2.1   These Clauses set out appropriate safeguards, including enforceable Data Subject rights and effective legal remedies, pursuant to section 42(1) and section 42(2) of the DPR 2021 and, with respect to data transfers from Controllers to Processors and Processors to Processors, standard contractual clauses pursuant to section 26(6) of the DPR 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 fundamental rights or freedoms of Data Subjects.

2.2   These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of the DPR 2021.

Clause 3

Third-party beneficiaries

3.1   Data Subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and data importer, with the following exceptions:

(a)   Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(b)   Clause 8 - Module One: Clause 8.5(e) and Clause 8.5(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);

(c)   Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(d)   Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(e)   Clause 13;

(f)   Clause 15.1(c), (d) and (e);

(g)   Clause 16(e);

(h)   Clause 18.

3.2   Paragraph 3.1 is without prejudice to rights of Data Subjects under the DPR 2021.

Clause 4
Interpretation

4.1   Where these Clauses use terms that are defined in the DPR 2021, those terms shall have the same meaning as in the DPR 2021.

4.2   These Clauses shall be read and interpreted in the light of the provisions of the DPR 2021.

4.3   These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in the DPR 2021.

Clause 5
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 will prevail.

Clause 6
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.

Clause 7 - Optional
Docking clause

7.1   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.

7.2   Once it has completed the Appendix and signed ANNEX I.A, the acceding entity will become 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.

7.3   The acceding entity will have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

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 Controller to Controller

8.1   Purpose limitation

The data importer will 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:

(a)   where it has obtained the Data Subject's prior consent;

(b)   where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(c)   where necessary in order to protect the vital interests of the Data Subject or of another natural person.

8.2   Transparency

(a)   In order to enable Data Subjects to effectively exercise their rights pursuant to Clause 10, the data importer will inform them, either directly or through the data exporter:

     (i)   of its identity and contact details;

     (ii)   of the categories of Personal Data Processed;

     (iii)   of the right to obtain a copy of these Clauses; and

     (iv)   where it intends to onward transfer the Personal Data to any third party/ies, 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.

(b)   Paragraph (a) will 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 will, to the extent possible, make the information publicly available.

(c)   On request, the Parties will 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 will 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 will provide the Data Subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

(d)   Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under sections 11 and 12 of the DPR 2021.

8.3   Accuracy and data minimisation

(a)   Each Party will ensure that the Personal Data is accurate and, where necessary, kept up to date. The data importer will take every reasonable step to ensure that Personal Data that is inaccurate, having regard to the purpose(s) of Processing, is erased or rectified without delay.

(b)   If one of the Parties becomes aware that the Personal Data it has transferred or received is inaccurate, or has become outdated, it will inform the other Party without undue delay.

(c)   The data importer will ensure that the Personal Data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of Processing.

8.4   Storage limitation

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

8.5   Security of Processing

(a)   The data importer and, during transmission, also the data exporter will implement appropriate technical and organisational measures to ensure the security of the Personal Data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter **"Personal Data Breach"**). In assessing the appropriate level of security, they will take due account of the State Of The Art, 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 will in particular consider having recourse to encryption or Pseudonymisation, including during transmission, where the purpose of Processing can be fulfilled in that manner.

(b)   The Parties have agreed on the technical and organisational measures set out in ANNEX II. The data importer will carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(c)   The data importer will ensure that persons authorised to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

---

[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.

(d)   In the event of a Personal Data Breach concerning Personal Data Processed by the data importer under these Clauses, the data importer will take appropriate measures to address the Personal Data Breach, including measures to mitigate its possible adverse effects.

(e)   In case of a Personal Data Breach that is likely to result in a risk to the rights of natural persons, the data importer will without undue delay notify both the data exporter and the ADGM Commissioner of Data Protection pursuant to Clause 13. Such notification will contain:

(i)   a description of the nature of the breach (including, where possible, categories and approximate number of Data Subjects and Personal Data records concerned);

(ii)   its likely consequences;

(iii)   the measures taken or proposed to address the breach; and

(iv)   the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

(f)   In case of a Personal Data Breach that is likely to result in a high risk to the rights of natural persons, the data importer will also notify without undue delay the Data Subjects concerned of the Personal Data Breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), sub-paragraphs (ii) to (iv), unless the data importer has implemented measures to significantly reduce the risk to the rights of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer will instead issue a public communication or take a similar measure to inform the public of the Personal Data Breach.

(g)   The data importer will document all relevant facts relating to the Personal Data Breach, including its effects and any remedial action taken, and keep a record thereof.

8.6   Special Category Personal Data

(a)   Where the transfer involves Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences or related security measures, the data importer will apply specific restrictions and additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the Personal Data, additional security measures (such as Pseudonymisation) and additional restrictions with respect to further disclosure.

8.7   Onward transfers

(a)   The data importer will not disclose the Personal Data to a third party located outside the ADGM (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:

(i)   it is to a jurisdiction benefitting from an adequacy decision pursuant to section 41 of the DPR 2021 that covers the Onward Transfer;

(ii)   the third party otherwise ensures appropriate safeguards pursuant to sections 42 or 43 the DPR 2021 with respect to the Processing in question;

(iii)   the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

(iv)   it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;

(v)   it is necessary in order to protect the vital interests of the Data Subject or of another natural person; or

(vi)   where none of the other conditions apply, the data importer has obtained the explicit consent of the Data Subject for an Onward Transfer in a specific situation, after having informed him or her of its purpose(s), the identity of the Recipient and the possible risks of such transfer to him or her due to the lack of appropriate data protection safeguards. In this case, the data importer will inform the data exporter and, at the request of the latter, will transmit to it a copy of the information provided to the Data Subject.

(b)   Any Onward Transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.8   Processing under the authority of the data importer

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

8.9   Documentation and compliance

(a)   Each Party will be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer will keep appropriate documentation of the Processing activities carried out under its responsibility.

(b)   The data importer will make such documentation available to the ADGM Commissioner of Data Protection on request.

MODULE TWO: Transfer Controller to Processor

8.1   Instructions

(a)   The data importer will 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.

(b)   The data importer will immediately inform the data exporter if it is unable to follow those instructions.

8.2   Purpose limitation

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

8.3 Transparency

On request, the data exporter will 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 will provide a meaningful summary where the Data Subject would otherwise not be able to understand the its content or exercise his or her rights. On request, the Parties will 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 sections 11 and 12 of the DPR 2021.

8.4 Accuracy

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

8.5 Duration of Processing and erasure or return of data

Processing by the data importer will only take place for the duration specified in ANNEX I.B. After the end of the provision of the Processing services, the data importer will, 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 data is deleted or returned, the data importer will 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 will continue to ensure compliance with these Clauses and will 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(b) 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 not in line with the requirements under Clause 14(a).

8.6 Security of Processing

(a)   The data importer and, during transmission, also the data exporter will implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter **"Personal Data Breach"**). In assessing the appropriate level of security, the Parties will take due account of the State Of The Art, 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 will in particular consider having recourse to encryption or Pseudonymisation, including during transmission, where the purpose of Processing can be fulfilled in that manner. In case of Pseudonymisation, the additional information for attributing the Personal Data to a specific Data Subject will, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer will at least implement the technical and organisational measures specified in ANNEX II. The data importer will carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b)   The data importer will 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 will ensure that persons authorised to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c)   In the event of a Personal Data Breach concerning Personal Data Processed by the data importer under these Clauses, the data importer will take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer will also notify the data exporter without undue delay after having become aware of the breach. Such notification will 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 will contain the information then available and further information will, as it becomes available, subsequently be provided without undue delay.

(d)   The data importer will cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under the DPR 2021, in particular to notify the ADGM Commissioner of Data Protection and the affected Data Subjects, taking into account the nature of Processing and the information available to the data importer.

8.7   Special Categories of Personal Data

Where the transfer involves Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences, the data importer will apply the specific restrictions and additional safeguards described in ANNEX I.B.

8.8   Onward transfers

(a)   The data importer will only disclose the Personal Data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the ADGM (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:

(i)   the Onward Transfer is to a jurisdiction benefitting from an adequacy decision pursuant to section 41 of the DPR 2021 that covers the Onward Transfer;

(ii)   the third party otherwise ensures appropriate safeguards pursuant to sections 42 or 43 of the DPR 2021 with respect to the Processing in question;

(iii)   the Onward Transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv)   the Onward Transfer is necessary in order to protect the vital interests of the Data Subject or of another natural person.

(b)   Any Onward Transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer will promptly and adequately deal with enquiries from the data exporter that relate to the Processing under these Clauses.

(b) The Parties will be able to demonstrate compliance with these Clauses. In particular, the data importer will keep appropriate documentation on the Processing activities carried out on behalf of the data exporter.

(c) The data importer will 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 non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) 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 will, where appropriate, be carried out with reasonable notice.

(e) The Parties will make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the ADGM Commissioner of Data Protection on request.

MODULE THREE: Transfer Processor to Processor

8.1 Instructions

(a) The data exporter has informed the data importer that it acts as Processor under the instructions of its Controller(s), which the data exporter will make available to the data importer prior to Processing.

(b) The data importer will Process the Personal Data only on documented instructions from the Controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions will not conflict with the instructions from the Controller. The Controller or data exporter may give further documented instructions regarding the data Processing throughout the duration of the contract.

(c) The data importer will 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 Controller, the data exporter will immediately notify the Controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract (or other legal act under any enactment or subordinate legislation applicable (i) in the ADGM; or (ii) under Abu Dhabi or Federal Law having application in ADGM and to which the Processor is subject ("**Applicable Law**") between the Controller and the data exporter.

8.2 Purpose limitation

The data importer will Process the Personal Data only for the specific purpose(s) of the transfer, as set out in ANNEX I.B., unless on further instructions from the Controller, as communicated to the data importer by the data exporter, or from the data exporter.

8.3 Transparency

On request, the data exporter will 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 will 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 will provide the Data Subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

8.4 Accuracy

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

8.5 Duration of Processing and erasure or return of data

Processing by the data importer will only take place for the duration specified in ANNEX I.B. After the end of the provision of the Processing services, the data importer will, at the choice of the data exporter, delete all Personal Data Processed on behalf of the 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 data is deleted or returned, the data importer will 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 will continue to ensure compliance with these Clauses and will 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(b) 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 not in line with the requirements under Clause 14(a).

8.6 Security of Processing

(a)   The data importer and, during transmission, also the data exporter will implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "Personal Data Breach"). In assessing the appropriate level of security, they will take due account of the State Of The Art, 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 will in particular consider having recourse to encryption or Pseudonymisation, including during transmission, where the purpose of Processing can be fulfilled in that manner. In case of Pseudonymisation, the additional information for attributing the Personal Data to a specific Data Subject will, where possible, remain under the exclusive control of the data exporter or the Controller. In complying with its obligations under this paragraph, the data importer will at least implement the technical and organisational measures specified in ANNEX II. The data importer will carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b)   The data importer will grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It will ensure that persons authorised to Process the Personal Data have

committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c)   In the event of a Personal Data Breach concerning Personal Data Processed by the data importer under these Clauses, the data importer will take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer will also notify, without undue delay, the data exporter and, where appropriate and feasible, the Controller after having become aware of the breach. Such notification will 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 will contain the information then available and further information will, as it becomes available, subsequently be provided without undue delay.

(d)   The data importer will cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under the DPR 2021, in particular to notify its Controller so that the latter may in turn notify the ADGM Commissioner of Data Protection and the affected Data Subjects, taking into account the nature of Processing and the information available to the data importer.

8.7   Special Category Personal Data

Where the transfer involves Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences, the data importer will apply the specific restrictions and additional safeguards set out in ANNEX I.B.

8.8   Onward transfers

(a)   The data importer will only disclose the Personal Data to a third party on documented instructions from the Controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the ADGM (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:

   (i)   the Onward Transfer is to a jurisdiction benefitting from an adequacy decision pursuant to section 41 of the DPR 2021 that covers the Onward Transfer;

   (ii)   the third party otherwise ensures appropriate safeguards pursuant to ections 42 or 43 of the DPR 2021;

   (iii)   the Onward Transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

   (iv)   the Onward Transfer is necessary in order to protect the vital interests of the Data Subject or of another natural person.

(b)   Any Onward Transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer will promptly and adequately deal with enquiries from the data exporter or the Controller that relate to the Processing under these Clauses.

(b) The Parties will be able to demonstrate compliance with these Clauses. In particular, the data importer will keep appropriate documentation on the Processing activities carried out on behalf of the Controller.

(c) The data importer will make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, and will provide it to the Controller.

(d) The data importer will 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 Controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the Controller, the data exporter will make the results available to the Controller.

(f) 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 will, where appropriate, be carried out with reasonable notice.

(g) The Parties will make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the ADGM Commissioner of Data Protection on request.

MODULE FOUR: Transfer Processor to Controller

8.1 Instructions

(a) The data exporter will Process the Personal Data only on documented instructions from the data importer acting as its Controller.

(b) The data exporter will immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe the DPR 2021.

(c) The data importer will refrain from any action that would prevent the data exporter from fulfilling its obligations under the DPR 2021, including in the context of sub-Processing or as regards cooperation with competent Supervisory Authorities.

(d) After the end of the provision of the Processing services, the data exporter will, 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.

8.2 Security of Processing

(a) The Parties will implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration,

unauthorised disclosure or access (hereinafter **"Personal Data Breach"**). In assessing the appropriate level of security, they will take due account of the State Of The Art, the costs of implementation, the nature of the Personal Data[2], 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 Pseudonymisation, including during transmission, where the purpose of Processing can be fulfilled in that manner.

(b)   The data exporter will assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a Personal Data Breach concerning the Personal Data Processed by the data exporter under these Clauses, the data exporter will notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.

(c)   The data exporter will ensure that persons authorised to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.3   Documentation and compliance

(a)   The Parties will be able to demonstrate compliance with these Clauses.

(b)   The data exporter will 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.

Clause 9

Use of sub-Processors

MODULE TWO: Transfer Controller to Processor

*[**EXPLANATORY NOTE**: Choose either OPTION 1 or OPTION 2 and remove the other option. For Modules 1 or 4, remove both OPTION 1 and OPTION 2 and add "Not used"]*

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

OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-Processor(s) from an agreed list. The data importer will specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-Processors at least [*Specify time period*] in advance, thereby giving the data exporter sufficient time

---

[2]   This includes whether the transfer and further Processing involves Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences.

to be able to object to such changes prior to the engagement of the sub-Processor(s). The data importer will provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b)   Where the data importer engages a sub-Processor to carry out specific Processing activities (on behalf of the data exporter), it will 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.[3] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 08.8. The data importer will ensure that the sub-Processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c)   The data importer will provide, at the data exporter's request, a copy of such a sub-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.

(d)   The data importer will remain fully responsible to the data exporter for the performance of the sub-Processor's obligations under its contract with the data importer. The data importer will notify the data exporter of any failure by the sub-Processor to fulfil its obligations under that contract.

(e)   The data importer will agree a third-party beneficiary clause with the sub-Processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter will have the right to terminate the sub-Processor contract and to instruct the sub-Processor to erase or return the Personal Data.

MODULE THREE: Transfer Processor to Processor

*[**EXPLANATORY NOTE**: Choose either OPTION 1 or OPTION 2 and remove the other option.. For Modules 1 or 4, remove both OPTION 1 and OPTION 2 and add "Not used"]*

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

OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the Controller's general authorisation for the engagement of sub-Processor(s) from an agreed list. The data importer will specifically inform the Controller in writing of any intended changes to that list through the addition or replacement of sub-Processors at least [*Specify time period*] in advance, thereby giving the Controller sufficient time to be able to object to such changes prior to the engagement of the sub-Processor(s).

---

[3] This requirement may be satisfied by the sub-Processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

The data importer will provide the Controller with the information necessary to enable the Controller to exercise its right to object. The data importer will inform the data exporter of the engagement of the sub-Processor(s).

(b)   Where the data importer engages a sub-Processor to carry out specific Processing activities (on behalf of the Controller), it will 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] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 0. The data importer will ensure that the sub-Processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c)   The data importer will provide, at the data exporter's or Controller's request, a copy of such a sub-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.

(d)   The data importer will remain fully responsible to the data exporter for the performance of the sub-Processor's obligations under its contract with the data importer. The data importer will notify the data exporter of any failure by the sub-Processor to fulfil its obligations under that contract.

(e)   The data importer will agree a third-party beneficiary clause with the sub-Processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter will have the right to terminate the sub-Processor contract and to instruct the sub-Processor to erase or return the Personal Data.

Clause 10

Data Subject rights

MODULE ONE: Transfer Controller to Controller

(a)   The data importer, where relevant with the assistance of the data exporter, will 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 two months of the receipt of the enquiry or request.[5] The data importer will take appropriate measures to facilitate such enquiries, requests and the exercise of Data Subject rights. Any information provided to the Data Subject will be in an intelligible and easily accessible form, using clear and plain language.

(b)   In particular, upon request by the data subject the data importer will, free of charge:

---

[4]   This requirement may be satisfied by the sub-Processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

[5]   Where necessary and that period may be extended by a maximum of 1 more month. Taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.

(i)   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 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 0; and provide information on the right to lodge a complaint with a Supervisory Authority in accordance with Clause 12(c)(i);

(ii)   rectify inaccurate or incomplete data concerning the Data Subject;

(iii)   erase Personal Data concerning the Data Subject if such 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.

(c)   Where the data importer Processes the Personal Data for direct marketing purposes, it will cease Processing for such purposes if the Data Subject objects to it.

(d)   The data importer will 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 country 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 will, where necessary in cooperation with the data exporter:

(i)   inform the Data Subject about the envisaged Automated Decision, the envisaged consequences and the logic involved; and

(ii)   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.

(e)   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.

(f)   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 section 21(1) of the DPR 2021.

(g)   If the data importer intends to refuse a Data Subject's request, it will inform the Data Subject of the reasons for the refusal and the possibility of lodging a complaint with the ADGM Commissioner of Data Protection and seeking judicial redress.

MODULE TWO: Transfer Controller to Processor

(a)   The data importer will promptly notify the data exporter of any request it has received from a Data Subject. It will not respond to that request itself unless it has been authorised to do so by the data exporter.

(b)   The data importer will assist the data exporter in fulfilling its obligations to respond to Data Subjects' requests for the exercise of their rights under the DPR 2021. In this regard, the Parties will set out in ANNEX II the appropriate technical and organisational measures, taking into account the nature of the Processing, by which the assistance will be provided, as well as the scope and the extent of the assistance required.

(c)   In fulfilling its obligations under paragraphs (a) and (b), the data importer will comply with the instructions from the data exporter.

MODULE THREE: Transfer Processor to Processor

(a)   The data importer will promptly notify the data exporter and, where appropriate, the 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 Controller.

(b)   The data importer will assist, where appropriate in cooperation with the data exporter, the Controller in fulfilling its obligations to respond to Data Subjects' requests for the exercise of their rights under the DPR 2021. In this regard, the Parties will set out in ANNEX II the appropriate technical and organisational measures, taking into account the nature of the Processing, by which the assistance will be provided, as well as the scope and the extent of the assistance required.

(c)   In fulfilling its obligations under paragraphs (a) and (b), the data importer will comply with the instructions from the Controller, as communicated by the data exporter.

MODULE FOUR: Transfer Processor to Controller

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

Clause 11

Redress

(a)   The data importer will 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 will deal promptly with any complaints it receives from a Data Subject.

*[**EXPLANATORY NOTE**: The wording immediately below 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[6] at no cost to the Data Subject. It will 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.]

---

[6]   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.

(b)   In case of a dispute between a Data Subject and one of the Parties as regards compliance with these Clauses, that Party will use its best efforts to resolve the issue amicably in a timely fashion. The Parties will keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c)   The data importer will abide by a decision that is binding under Applicable Law.

Clause 12

Liability

MODULE ONE: Transfer Controller to Controller

MODULE FOUR: Transfer Processor to Controller

(a)   Each Party will be liable to the any other Party for any damages it causes the other Party by any breach of these Clauses.

(b)   Each Party will be liable to the Data Subject, and the Data Subject will be 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 DPR 2021.

(c)   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 will be jointly and severally liable and the Data Subject is entitled to bring an action in court against any of these Parties.

(d)   The Parties agree that if one Party is held liable under paragraph (a), it will be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(e)   The data importer may not invoke the conduct of a Processor or sub-Processor to avoid its own liability.

MODULE TWO: Transfer Controller to Processor

MODULE THREE: Transfer Processor to Processor

(a)   Each Party will be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b)   The data importer will be liable to the Data Subject, and the Data Subject will be entitled to receive compensation, for any material or non-material damages the data importer or its sub-Processor causes the Data Subject by breaching the third-party beneficiary rights under these Clauses.

(c)   Notwithstanding paragraph (b), the data exporter will be liable to the Data Subject, and the Data Subject will be entitled to receive compensation, for any material or non-

material damages the data exporter or the data importer (or its sub-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 Processor acting on behalf of a Controller, to the liability of the Controller under Applicable Law.

(d)   The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-Processor), it will be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e)   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 will be jointly and severally liable and the Data Subject is entitled to bring an action in court against any of these Parties.

(f)   The Parties agree that if one Party is held liable under paragraph (e), it will be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g)   The data importer may not invoke the conduct of a sub-Processor to avoid its own liability.

Clause 13

Supervision

MODULE ONE: Transfer Controller to Controller

MODULE TWO: Transfer Controller to Processor

MODULE THREE: Transfer Processor to Processor

(a)   the data importer agrees to submit itself to the jurisdiction of and cooperate with the ADGM Commissioner of Data Protection 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 Supervisory Authority, including remedial and compensatory measures. it will provide the Supervisory Authority with written confirmation that the necessary actions have been taken.

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

Clause 14

Local laws and practices affecting compliance with the Clauses

MODULE ONE: Transfer Controller to Controller

MODULE TWO: Transfer Controller to Processor

MODULE FOUR: Transfer Processor to Controller (*where the Abu Dhabi Global Market Processor combines the Personal Data received from Controllers outside the ADGM with Personal Data collected by the Processor in the ADGM*)

(a)   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 fundamental rights and freedoms and do not exceed what is necessary and proportionate to safeguard one of the objectives listed in section 1 of the DPR 2021, are not in contradiction with these Clauses.

(b)   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 not in line with the requirements under paragraph (a), including following a change in the laws of the third country 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 will forward the notification to the Controller.]

(c)   Following a notification pursuant to paragraph (b), 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 will 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 Controller]. The data exporter will 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 Controller or] the ADGM Commissioner of Data Protection to do so. In this case, the data exporter will be 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) will apply.

Clause 15

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

MODULE ONE: Transfer Controller to Controller

MODULE TWO: Transfer Controller to Processor

MODULE THREE: Transfer Processor to Processor

MODULE FOUR: Transfer Processor to Controller (*where the ADGM Processor combines the Personal Data received from another jurisdiction with Personal Data collected by the Processor in the ADGM*)

15.1   Notification

(a) 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:

(i) 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 will include information about the Personal Data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to Personal Data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification will include all information available to the importer.

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

(b) If the data importer is prohibited from notifying the data exporter or the Data Subject under the laws of the country 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.

(c) 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 will forward the information to the Controller.]

(d) 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 ADGM Commissioner of Data Protection on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(b) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2   Review of legality and data minimisation

(a) 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 country of destination, applicable obligations under international law and principles of international comity. The data importer will, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer will seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It will 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(b).

(b) 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 country of destination, make the documentation available to the data exporter. It will also make it

available to the ADGM Commissioner of Data Protection on request. [For Module Three: The data exporter will make the assessment available to the Controller.]

(c)   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

Clause 16
Non-compliance with the Clauses and termination

(a)   The data importer will promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b)   In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter will 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(c).

(c)   The data exporter will be entitled to terminate the contract, insofar as it concerns the Processing of Personal Data under these Clauses, where:

    (i)   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 one month of suspension;

    (ii)   the data importer is in substantial or persistent breach of these Clauses; or

    (iii)   the data importer fails to comply with a binding decision of a competent court or Supervisory Authority regarding its obligations under these Clauses.

    In these cases, it will inform the ADGM Commissioner of Data Protection [for Module Three: and the Controller] of 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.

(d)   [For Modules One, Two and Three: Personal Data that has been transferred prior to the termination of the contract pursuant to paragraph (c) will at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same will apply to any copies of the data.] [For Module Four: Personal Data collected by the data exporter in the ADGM that has been transferred prior to the termination of the contract pursuant to paragraph (c) will immediately be deleted in its entirety, including any copy thereof.] The data importer will certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer will 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 will continue to ensure compliance with these Clauses and will only Process the data to the extent and for as long as required under that local law.

(e)   Either Party may revoke its agreement to be bound by these Clauses where the ADGM Commissioner of Data Protection adopts a decision pursuant to section 41(3) of the 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 DPR 2021.

Clause 17

Governing law

MODULE ONE: Transfer Controller to Controller

MODULE TWO: Transfer Controller to Processor

MODULE THREE: Transfer Processor to Processor

These Clauses shall be governed by the law of the Abu Dhabi Global Market.

MODULE FOUR: Transfer Processor to Controller

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of _____ *[specify country]*.

Clause 18

Choice of forum and jurisdiction

MODULE ONE: Transfer Controller to Controller

MODULE TWO: Transfer Controller to Processor

MODULE THREE: Transfer Processor to Processor

(a)   Any dispute arising from these Clauses shall be resolved by the courts of the Abu Dhabi Global Market.

(b)   The Parties agree to submit themselves to the jurisdiction of such courts.

MODULE FOUR: Transfer Processor to Controller

(a)   Any dispute arising from these Clauses shall be resolved by the courts of _____ *[specify country]*.

(b)   The Parties agree to submit themselves to the 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 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 Controller to Controller

MODULE TWO: Transfer Controller to Processor

MODULE THREE: Transfer Processor to Processor

MODULE FOUR: Transfer Processor to 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]*

1.   Name: *[Insert]*

     Address: *[Insert]*

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

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

     Signature and date: *[Insert]*

     Role (Controller/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]*

1.   Name: *[Insert]*

     Address: *[Insert]*

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

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

     Signature and date: *[Insert]*

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

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

B.   DESCRIPTION OF TRANSFER

MODULE ONE: Transfer Controller to Controller

MODULE TWO: Transfer Controller to Processor

MODULE THREE: Transfer Processor to Processor

MODULE FOUR: Transfer Processor to Controller

1.   Categories of Data Subjects whose Personal Data is transferred

*[**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 Controller's third party service providers.]*

2.   Categories of Personal Data transferred

[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 Special Category 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 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 data, restrictions for Onward Transfers or additional security measures.]

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

[Insert]

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

4.   Nature of the Processing

[Insert]

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

5.   Purpose(s) of the 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 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.]*

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

7.   **For transfers to (sub-) 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-) Processors.]*

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

MODULE ONE: Transfer Controller to Controller

MODULE TWO: Transfer Controller to Processor

MODULE THREE: Transfer Processor to 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 freedoms of natural persons.

[Insert]

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

- *Measures of Pseudonymisation 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 data during transmission*

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

[Insert]

ANNEX III- LIST OF SUB-PROCESSORS

MODULE TWO: Transfer Controller to Processor

MODULE THREE: Transfer Processor to Processor

*[**EXPLANATORY NOTE:** This Annex must be completed for Modules Two and Three, in case of the specific authorisation of sub-Processors (09(a), Option 1).]*

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

1.   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-Processors are authorised): *[Insert]*

2.   *[Insert additional information at (2), (3), (4) etc. if there is more than one sub-Processor granted specific authorisation pursuant to 09(a), Option 1).]*