Standard Contractual Clauses

relating to the Processing of Personal Data pursuant to
Section 26(3), (4) and (5) of the Abu Dhabi Global Market Data Protection Regulations 2021

*[**EXPLANATORY NOTE:** If entered into without any amendment, these Clauses meet the contractual requirements of section 26(3) of the DPR 2021, provided that the information inputted at Annexes I – IV is sufficiently detailed and accurate. Whilst it is not necessary for Controllers and Processors to use these Clauses in their unamended form in order to meet the requirements of section 26(3), (4) and (5) of the DPR 2021, it is the responsibility of the contracting parties to ensure that where any amendment is made (or, indeed, where an alternative agreement is used), that those requirements continue to be met.]*

SECTION I

INTRODUCTION

1. Purpose and scope

1.1. The purpose of these standard contractual clauses (the "**Clauses**") is to ensure compliance with Sections 26(3), (4) and (5) of the Abu Dhabi Global Market ("**ADGM**") Data Protection Regulations 2021 ("**DPR 2021**").

1.2. These Clauses are the standard contractual clauses referred to in section 26(6) of the DPR 2021.

1.3. The Controllers and Processors listed in Annex I (the "**Parties**") have agreed to these Clauses in order to ensure compliance with sections 26 (3), (4) and (5) of the DPR 2021.

1.4. These Clauses apply to the Processing of Personal Data as specified in Annex II.

1.5. Annexes I to IV are an integral part of the Clauses.

1.6. These Clauses are without prejudice to obligations to which the Controller is subject by virtue of the DPR 2021.

1.7. These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Part V of the DPR 2021.

2. Invariability of the Clauses

2.1. The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

2.2. This does not prevent the Parties from including the standard contractual clauses in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights of Data Subjects.

3. Interpretation

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

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

3.3. These Clauses shall not be interpreted in a way that is counter to the rights and obligations provided in the DPR 2021 or in a way that prejudices the fundamental rights of the Data Subjects.

4. **Hierarchy**

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

5. **Docking clause** ***[EXPLANATORY NOTE:*** *This Clause 5 is optional and may be deleted if you do not want other parties to accede to these Clauses.****]***

5.1. Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a Controller or a Processor by completing the Annexes and signing Annex I.

5.2. Once the Annexes to these Clauses are completed and Annex I has been signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a Controller or a Processor, in accordance with its designation in Annex I.

5.3. The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

SECTION II

OBLIGATIONS OF THE PARTIES

6. Description of Processing(s)

6.1. The details of the processing operations, in particular the categories of Personal Data and the purposes of Processing Personal Data on behalf of the Controller, are specified in Annex II.

7. **Obligations of the Parties**

7.1. Instructions

(a) The Processor will Process Personal Data only on documented instructions from the Controller, unless required to do so by 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"**). In this case, the Processor will inform the Controller of such legal requirement before Processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the Controller throughout the duration of the Processing of Personal Data. These instructions will always be documented.

(b) The Processor will immediately inform the Controller if, in the Processor's opinion, instructions given by the Controller infringe the DPR 2021 or other data protection provisions contained in Applicable Law.

7.2. Purpose limitation

(a) The Processor will Process the Personal Data only for the specific purpose(s) of the Processing, as set out in Annex II, unless it receives further instructions from the Controller.

7.3. Duration of the Processing of Personal Data

(a) Processing by the Processor will only take place for the duration specified in Annex II.

7.4. Security of Processing

(a) The Processor will at least implement the technical and organisational measures specified in Annex III to ensure the security of the Personal Data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data ("**Personal Data Breach**"). In assessing the appropriate level of security, the Parties will take account of the State Of The Art, the costs of implementation, the nature, scope, context and purposes of Processing and the risks involved for the Data Subjects.

(b) The Processor will grant access to the Personal Data undergoing Processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The Processor will ensure that persons authorised to Process the Personal Data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. Special Category Personal Data

(a) If the 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 and offences or related security measures, the Processor will apply specific restrictions and additional safeguards to be agreed by the Processor and Controller.

7.6. Documentation and compliance

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

(b) The Processor will deal promptly and adequately with inquiries from the Controller about the Processing of data in accordance with these Clauses.

(c) The Processor will make available to the Controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from the DPR 2021. At the Controller's request, the Processor will also permit 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 an audit, the Controller may take into account relevant certifications held by the Processor.

(d) The Controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

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

7.7. Use of sub-Processors

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

(a) OPTION 1: PRIOR SPECIFIC AUTHORISATION: The Processor will not subcontract any of its Processing operations performed on behalf of the Controller in accordance with these Clauses to a sub-Processor, without the Controller's prior specific written authorisation. The Processor 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. The list of sub-Processors authorised by the Controller can be found in Annex IV. The Parties shall keep Annex IV up to date.

OPTION 2: GENERAL WRITTEN AUTHORISATION: The Processor has the Controller's general authorisation for the engagement of sub-Processors from an agreed list. The Processor will specifically inform in writing the Controller of any intended changes of that list through the addition or replacement of sub-Processors at least [SPECIFY TIME PERIOD] in advance, giving the Controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-Processor(s). The Processor will provide the Controller with the information necessary to enable the Controller to exercise the right to object.

(b) Where the Processor engages a sub-Processor for carrying out specific Processing activities (on behalf of the Controller), it will do so by way of a contract which imposes on the sub-Processor, in substance, the same data protection obligations as the ones imposed on the Processor in accordance with these Clauses. The Processor will ensure that the sub-Processor complies with the obligations to which the Processor is subject pursuant to these Clauses and to the DPR 2021.

(c) At the Controller's request, the Processor will provide a copy of such a sub-Processor agreement and any subsequent amendments to the Controller. To the extent necessary to protect business secret or other confidential information, including Personal Data, the Processor may redact the text of the agreement prior to sharing the copy.

(d) The Processor will remain fully responsible to the Controller for the performance of the sub-Processor's obligations in accordance with its contract with the Processor. The Processor will notify the Controller of any failure by the sub-Processor to fulfil its contractual obligations.

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

7.8. International transfers

(a) Any transfer of data to a third country or an international organisation by the Processor will be done only on the basis of documented instructions from the Controller or in order to fulfil a specific requirement under applicable law to which the Processor is subject and shall take place in compliance with Part V of the DPR 2021.

(b) The Controller agrees that where the Processor engages a sub-Processor to carry out specific Processing activities (on behalf of the Controller) in accordance with Clause

7.7, and those Processing activities involve a transfer of Personal Data within the meaning of Part V of the DPR 2021, the Processor and the sub-Processor can ensure compliance with Part V of the DPR 2021 by using standard contractual clauses adopted by the ADGM Commissioner of Data Protection in accordance with section 42(3) of the DPR 2021, provided the conditions for the use of those standard contractual clauses are met.

8. Assistance to the Controller

8.1. The Processor will promptly notify the Controller of any request it has received from the Data Subject. It will not respond to the request itself, unless authorised to do so by the Controller.

8.2. The Processor will assist the Controller in fulfilling its obligations to respond to Data Subjects' requests to exercise their rights, taking into account the nature of the Processing. In fulfilling its obligations in accordance with Clause 8.1 and 8.2, the Processor will comply with the Controller's instructions.

8.3. In addition to the Processor's obligation to assist the Controller pursuant to Clause 8.2, the Processor will assist the Controller in ensuring compliance with the following obligations, taking into account the nature of the data Processing and the information available to the Processor:

(a) the obligation to carry out an assessment of the impact of the envisaged Processing operations on the protection of Personal Data (a "**Data Protection Impact Assessment**") where a type of Processing is likely to result in a high risk to the rights and freedoms of natural persons;

(b) the obligation to consult any competent Supervisory Authority prior to Processing where a Data Protection Impact Assessment indicates that the Processing would result in a high risk in the absence of measures taken by the Controller to mitigate the risk;

(c) the obligation to ensure that Personal Data is accurate and up to date, by informing the Controller without delay if the Processor becomes aware that the Personal Data it is Processing is inaccurate or has become outdated; and

(d) the obligations in section 30 of the DPR 2021.

8.4. The Parties will set out in Annex III the appropriate technical and organisational measures by which the Processor is required to assist the Controller in the application of this Clause as well as the scope and the extent of the assistance required.

9. Notification of Personal Data Breach

9.1. In the event of a Personal Data Breach, the Processor will cooperate with and assist the Controller to comply with its obligations under sections 32 and 33 of the DPR 2021, where applicable, taking into account the nature of Processing and the information available to the Processor.

Data breach concerning data Processed by the Controller

9.2. In the event of a Personal Data Breach concerning data Processed by the Controller, the Processor will assist the Controller:

(a) in notifying the Personal Data Breach to the ADGM Commissioner of Data Protection, without undue delay after the Controller has become aware of it, where relevant (unless the Personal Data Breach is unlikely to result in a risk to the rights of natural persons); and

(b) in obtaining the following information which, pursuant to section 32(3) of the DPR 2021, will be stated in the Controller's notification, and must at least include:

i. the nature of the Personal Data including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;

ii. the likely consequences of the Personal Data Breach; and

iii. the measures taken or proposed to be taken by the Controller to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where it is not possible to provide all of the information listed at Clause 9.2 (b) 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; and

(c) in complying, pursuant to section 33 of the DPR 2021, with the obligation to communicate without undue delay the Personal Data Breach to the Data Subject, when the Personal Data Breach is likely to result in a high risk to the rights of natural persons.

Data breach concerning data Processed by the Processor

9.3. In the event of a Personal Data Breach concerning data Processed by the Processor, the Processor will notify the Controller without undue delay after the Processor having become aware of the breach. Such notification will contain, at least:

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

(b) the details of a contact point where more information concerning the Personal Data Breach can be obtained; and

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

9.4. Where it is not possible to provide all of the information listed at Clause 9.3 (a) – (c) 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.

9.5. The Parties will set out in Annex III all other elements to be provided by the Processor when assisting the Controller in the compliance with the Controller's obligations under sections 32 and 33 of the DPR 2021.

SECTION III

FINAL PROVISIONS

10. Non-compliance with the Clauses and termination

10.1. Without prejudice to any provisions of the DPR 2021, in the event that the Processor is in breach of its obligations under these Clauses, the Controller may instruct the Processor to suspend the Processing of Personal Data until the Processor complies with these Clauses or the contract is terminated. The Processor will promptly inform the Controller in case it is unable to comply with these Clauses, for whatever reason.

10.2. The Controller will be entitled to terminate the contract if:

(a) the Processing of Personal Data by the Processor has been suspended by the Controller pursuant to Clause 10.1 and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(b) the Processor is in substantial or persistent breach of these Clauses or its obligations under the DPR 2021; and

(c) the Processor fails to comply with a binding decision of a competent court or the ADGM Commissioner of Data Protection regarding its obligations pursuant to these Clauses or to the DPR 2021

10.3. The Processor will be entitled to terminate the contract where, after having informed the Controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the Controller insists on compliance with the instructions.

10.4. Following termination of the contract, the Processor will, at the choice of the Controller, delete all Personal Data Processed on behalf of the Controller and certify to the Controller that it has done so, or, return all the Personal Data to the Controller and delete existing copies unless applicable law requires storage of the Personal Data. Until the data is deleted or returned, the Processor will continue to ensure compliance with these Clauses.

ANNEX I

List of Parties

Controller(s): *[**EXPLANATORY NOTE:** Please insert the identity and contact details of the Controller(s), and, where applicable, of the Controller's Data Protection Officer]*

1. Name: *[Insert]*

   Address: *[Insert]*

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

   Signature and accession date: *[Insert]*

2. *[Insert additional information if there is more than one Controller]*

Processor(s): *[**EXPLANATORY NOTE:** Please insert the identity and contact details of the Processor(s) and, where applicable, of the Processor's Data Protection Officer]*

1. Name: *[Insert]*

   Address: *[Insert]*

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

   Signature and accession date: *[Insert]*

2. *[**EXPLANATORY NOTE:** Insert additional information if there is more than one Processor]*

ANNEX II

Description of the Processing

1. Categories of Data Subjects whose Personal Data is Processed

[Insert]

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

2. Categories of Personal Data Processed

[Insert]

*[**EXPLANATORY NOTE:** List out the categories of Personal Data being Processed. 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).]*

3. Special Category Personal Data Processed (if applicable) and applied restrictions or safeguards

[Insert]

*[**EXPLANATORY NOTE**: The applied restrictions or safeguards must 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.]*

4. Nature of the Processing

[Insert]

*[**EXPLANATORY NOTE:** Describe how the Processor 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) for which the Personal Data is Processed on behalf of the Controller

[Insert]

*[**EXPLANATORY NOTE:** Describe the purpose for which the Processor is Processing the Personal Data. For example, the Processor 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. Duration of the Processing

[Insert]

*[**EXPLANATORY NOTE:** Describe for how long the Processor will continue to Process the Personal Data, or the criteria which would be used to determine that period. For example, if the Processor 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 Processing by (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 III

Technical and organisational measures to ensure the security of the data

*[**EXPLANATORY NOTE**: The technical and organisational measures used by your organisation must be described in this Annex III in a concrete and non-generic manner. 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.]*

1. **Description of the technical and organisational security measures implemented by the Processor(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the Processing, as well as 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]*

2. **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.**

   [Insert]

   ***[EXPLANATORY NOTE:** Please detail any measures which assist the Controller in enabling (sub-) Processors to fulfil Data Subject rights requests, as well as any measures which assist them to meet their obligations under sections 30 – 34 of the DPR 2021 (Security of Processing, cessation of Processing, notification of a Personal Data Breaches to the Commissioner and Data Subjects, Data Protection Impact Assessments.)]*

3. **Description of the specific technical and organisational measures to be taken by the Processor to be able to provide assistance to the Controller.**

   [Insert]

   ***[EXPLANATORY NOTE:** Please detail any measures which assist the Controller in enabling it to fulfil Data Subject rights requests, as well as any measures which assist it in meeting its obligations under sections 30 – 34 of the DPR 2021 (Security of Processing, cessation of Processing, notification of a Personal Data Breaches to the Commissioner and Data Subjects, Data Protection Impact Assessments.)]*

ANNEX IV

List of sub-Processors

*[**EXPLANATORY NOTE:** This Annex needs to be completed in case of specific authorisation of sub-Processors (Clause 7.7(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 the Processing (including a clear delimitation of responsibilities in case several sub-Processors are authorised): *[Insert]*

2. *[Insert additional information if there is more than one sub-Processor]*