



ABU DHABI GLOBAL MARKET
سوق أبوظبي العالمي

DATA PROTECTION REGULATIONS 2015

DATA PROTECTION REGULATIONS 2015

Part 1 General Rules on the Processing of Personal Data	1
Part 2 Rights of Data Subjects	7
Part 3 Notifications to the Registrar	7
Part 4 The Registrar	8
Part 5 The Board	9
Part 6 Remedies, Liability and Sanctions	9
Part 7 General Exemptions	12
SCHEDULE 1 DATA TRANSFER AGREEMENT (Data Controller to Data Controller transfers)	16
SCHEDULE 2 DATA TRANSFER AGREEMENT (Data Controller to Data Processor transfers)	25
SCHEDULE 3 JURISDICTIONS WITH AN ADEQUATE LEVEL OF PROTECTION	35
SCHEDULE 4 FEES	37

DATA PROTECTION REGULATIONS 2015

Regulations to make provision for the protection of personal data within the Abu Dhabi Global Market and for connected purposes.

Date of Enactment: **4 October 2015**

The Board of Directors of the Abu Dhabi Global Market, in exercise of its powers under Article 6(1) of Law No. 4 of 2013 concerning the Abu Dhabi Global Market issued by His Highness the Ruler of the Emirate of Abu Dhabi, hereby enacts the following Regulations –

Part 1 General Rules on the Processing of Personal Data

1. General requirements

- (1) Data Controllers shall ensure that Personal Data which they Process are–
- (a) Processed fairly, lawfully and securely;
 - (b) Processed for specified, explicit and legitimate purposes in accordance with the Data Subject's rights and not further Processed in a way incompatible with those purposes or rights;
 - (c) adequate, relevant and not excessive in relation to the purposes for which they are collected or further Processed;
 - (d) accurate and, where necessary, kept up to date; and
 - (e) kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data were collected or for which they are further Processed.
- (2) Every reasonable step shall be taken by Data Controllers to ensure that Personal Data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further Processed, are erased or rectified.

2. Requirements for legitimate Processing

Personal Data may only be Processed if–

- (a) the Data Subject has given his written consent to the Processing of that Personal Data;
- (b) Processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract;
- (c) Processing is necessary for compliance with any regulatory or legal obligation to which the Data Controller is subject;
- (d) Processing is necessary in order to protect the vital interests of the Data Subject;

- (e) Processing is necessary for the performance of a task carried out in the interests of the Abu Dhabi Global Market or in the exercise of the Board's, the Court's, the Registrar's or the Regulator's functions or powers vested in the Data Controller or in a Third Party to whom the Personal Data are disclosed; or
- (f) Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by the Third Party to whom the Personal Data are disclosed, except where such interests are overridden by compelling legitimate interests of the Data Subject relating to the Data Subject's particular situation.

3. **Processing of Sensitive Personal Data**

(1) Sensitive Personal Data shall not be Processed unless–

- (a) the Data Subject has given an additional written consent to the Processing of this kind of Personal Data;
- (b) Processing is necessary for the purposes of carrying out the obligations and specific rights of the Data Controller;
- (c) Processing is necessary to protect the vital interests of the Data Subject or of another person where the Data Subject is physically or legally incapable of giving his consent;
- (d) Processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body on condition that the Processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the Personal Data are not disclosed to a Third Party without the consent of the Data Subjects;
- (e) the Processing relates to Personal Data which are manifestly made public by the Data Subject, or is necessary for the establishment, exercise or defence of legal claims;
- (f) Processing is necessary for compliance with any regulatory or legal obligation to which the Data Controller is subject;
- (g) Processing is necessary to uphold the legitimate interests of the Data Controller recognised in the international financial markets, provided the Processing is undertaken in accordance with applicable standards and except where such interests are overridden by compelling legitimate interests of the Data Subject relating to the Data Subject's particular situation;
- (h) Processing is necessary to comply with any regulatory, auditing, accounting, anti-money laundering or counter terrorist financing obligations that apply to a Data Controller or for the prevention or detection of any crime; or
- (i) Processing is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of healthcare services, and where those Personal Data are Processed by a health professional subject under law or rules established by competent bodies to the obligation of confidence or by another person subject to an equivalent obligation.

- (2) Subsection (1) shall not apply if–
- (a) a permit has been obtained from the Registrar to Process Sensitive Personal Data; and
 - (b) the Data Controller applies adequate safeguards with respect to the Processing of the Personal Data.

4. Transfers out of the Abu Dhabi Global Market: adequate level of protection

- (1) Except as set out in section 5, a transfer of Personal Data to a Recipient located in a jurisdiction outside the Abu Dhabi Global Market may take place only if the jurisdiction is listed in Schedule 3 or has been designated by the Registrar under subsection (3).
- (2) The adequacy of the level of protection ensured by laws to which the Recipient is subject, as referred to in subsection (1), shall be assessed in the light of all the circumstances surrounding a Personal Data transfer operation or set of Personal Data transfer operations, including, but not limited to–
- (a) the nature of the Personal Data;
 - (b) the purpose and duration of the proposed Processing operation or operations;
 - (c) if the Personal Data do not emanate from the Abu Dhabi Global Market, the country of origin and country of final destination of the Personal Data; and
 - (d) any relevant laws to which the Recipient is subject, including professional rules and security measures.
- (3) Certain jurisdictions are hereby designated as providing an adequate level of protection for Personal Data for the purposes of subsection (1). These are listed in Schedule 3 to these Regulations. Additional jurisdictions may be designated by the Registrar from time to time to the list of jurisdictions considered to fall under subsection (1) which shall be deemed to be part of Schedule 3 by a publication to such effect on the Registrar's website.
- (4) The Registrar may also, by publication to such effect on the Registrar's website, withdraw a designation from a jurisdiction designated under subsection (3) or listed in Schedule 3 if the Registrar considers that: (a) the relevant jurisdiction no longer provides an adequate level of protection for Personal Data for the purposes of subsection (1); and (b) such removal is warranted in order to further the protection of Personal Data.

5. Transfers out of the Abu Dhabi Global Market in the absence of an adequate level of protection

- (1) A transfer or a set of transfers of Personal Data to a Recipient which is not subject to laws which ensure an adequate level of protection within the meaning of section 4(1) may take place on condition that–
- (a) the Registrar has granted a permit for the transfer or the set of transfers and the Data Controller applies adequate safeguards with respect to the protection of such Personal Data;
 - (b) the Data Subject has given his written consent to the proposed transfer;

- (c) the transfer is necessary for the performance of a contract between the Data Subject and the Data Controller or the implementation of pre-contractual measures taken in response to the Data Subject's request;
- (d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the Data Controller and a Third Party;
- (e) the transfer is necessary for the establishment, exercise or defence of legal claims;
- (f) the transfer is necessary in order to protect the vital interests of the Data Subject;
- (g) the transfer is necessary in the interests of the Abu Dhabi Global Market;
- (h) the transfer is made at the request of a regulator, the police or other government agency;
- (i) the transfer is made from a register which according to law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case;
- (j) the transfer is necessary for compliance with any regulatory or legal obligation to which the Data Controller is subject;
- (k) the transfer is necessary to uphold the legitimate interests of the Data Controller recognised in the international financial markets, provided that the transfer is carried out in accordance with applicable standards and except where such interests are overridden by legitimate interests of the Data Subject relating to the Data Subject's particular situation;
- (l) the transfer is necessary to comply with any regulatory, auditing, accounting, anti-money laundering or counter terrorist financing obligations that apply to a Data Controller which is established in the Abu Dhabi Global Market, or for the prevention or detection of any crime;
- (m) the transfer is made to a person established outside the Abu Dhabi Global Market who would be a Data Controller (if established in the Abu Dhabi Global Market) or who is a Data Processor, if, prior to the transfer, a legally binding agreement in the form set out in Schedule 1 or Schedule 2 respectively to these Regulations has been entered into between the transferor and Recipient; or
- (n) the transfer is made between one or more members of a Group of Companies in accordance with a global data protection compliance policy of that Group, under which all the members of such Group that are or will be transferring or receiving the Personal Data are bound to comply with all the provisions of these Regulations containing restrictions on the use of Personal Data and Sensitive Personal Data in the same way as if they would be if established in the Abu Dhabi Global Market.

- (2) A transfer or set of transfers of Personal Data to a Recipient which is not subject to laws which ensure an adequate level of protection within the meaning of section 4(1) shall still be regarded as having been made pursuant to subsection 5(1)(m) if–
- (a) a legally binding agreement had been entered into between the transferor and Recipient prior to the date of commencement of the Data Protection (Amendment) Regulations 2018 (being 1 February 2018); and
 - (b) the agreement mentioned in subsection (a) above is in the form previously contained in Schedule 1 or 2 of the Data Protection Regulations 2015 prior to the amendments made by the Data Protection (Amendment) Regulations 2018,
- regardless of whether such transfer occurs prior to or after the effective date of the Data Protection (Amendment) Regulations 2018 (being 1 February 2018).

6. Providing information where Personal Data have been obtained from the Data Subject

- (1) Data Controllers shall provide a Data Subject whose Personal Data it collects from the Data Subject with at least the following information as soon as possible upon commencing to collect Personal Data in respect of that Data Subject–
- (a) the identity of the Data Controller;
 - (b) the purposes of the Processing for which the Personal Data are intended; and
 - (c) any further information in so far as such is necessary, having regard to the specific circumstances in which the Personal Data are collected, to guarantee fair Processing in respect of the Data Subject, such as–
 - (i) the Recipients or categories of Recipients of the Personal Data;
 - (ii) whether replies to questions are obligatory or voluntary, as well as the possible consequences of failure to reply;
 - (iii) the existence of the right of access to and the right to rectify the Personal Data concerning him;
 - (iv) whether the Personal Data will be used for direct marketing purposes; and
 - (v) whether the Personal Data will be Processed on the basis of section 3(1)(g) or section 5(1)(k).
- (2) A Data Controller need not provide that information otherwise required by subsection (1)(c)(i) to the Data Subject if the Data Controller reasonably expects that the Data Subject is already aware of that information.

7. Providing information where Personal Data have not been obtained from the Data Subject

- (1) Where Personal Data have not been obtained from the Data Subject, a Data Controller or his representative shall at the time of undertaking the Processing of Personal Data or if a disclosure to a Third Party is envisaged, no later than the time when the Personal Data are first Processed or disclosed, provide the Data Subject with at least the following information–
- (a) the identity of the Data Controller;

- (b) the purposes of the Processing;
 - (c) any further information in so far as such further information is necessary, having regard to the specific circumstances in which the Personal Data are Processed, to guarantee fair Processing in respect of the Data Subject, such as–
 - (i) the categories of Personal Data concerned;
 - (ii) the Recipients or categories of Recipients;
 - (iii) the existence of the right of access to and the right to rectify the Personal Data concerning him;
 - (iv) whether the Personal Data will be used for direct marketing purposes; and
 - (v) whether the Personal Data will be Processed on the basis of section 3(1)(g) or section 5(1)(k).
- (2) Subsection (1) shall not apply to require–
- (a) the Data Controller to provide information which the Data Controller reasonably expects the Data Subject to possess; or
 - (b) the provision of such information if it is reasonably impracticable or would involve a disproportionate effort.

8. Confidentiality

Any person acting under a Data Controller or a Data Processor, including the Data Processor himself, who has access to Personal Data shall not Process them except on instructions from the Data Controller, unless he is required to do so by law.

9. Security of Processing

- (1) The Data Controller shall implement appropriate technical and organisational measures to protect Personal Data against unauthorised or unlawful Processing and against accidental loss or destruction of, or damage to, such Personal Data.
- (2) Having regard to the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the Processing and the nature of the Personal Data to be protected.
- (3) The Data Controller shall, where Processing is carried out on its behalf, choose a Data Processor providing sufficient guarantees in respect of the technical security measures and organisational measures governing the Processing to be carried out, and shall ensure compliance with those measures.
- (4) In the event of an unauthorised intrusion (including any loss of devices containing Personal Data or unauthorised disclosures) whether physical, electronic or otherwise, to any Personal Data held by a Data Processor, the Data Processor shall inform the Data Controller of the incident as soon as reasonably practicable.

- (5) In the event of an unauthorised intrusion (including any loss of devices containing Personal Data or unauthorised disclosures) whether physical, electronic or otherwise, to any Personal Data, including by any of its Data Processors, the Data Controller shall inform the Registrar of the incident without undue delay, and where feasible, not later than 72 hours after becoming aware of it.

Part 2 Rights of Data Subjects

10. Right to access to and rectification, erasure or blocking of Personal Data

A Data Subject has the right to require and obtain from the Data Controller upon request, at reasonable intervals and without excessive delay or expense—

- (a) confirmation in writing as to whether or not Personal Data relating to him are being Processed and information at least as to the purposes of the Processing, the categories of Personal Data concerned, and the Recipients or categories of Recipients to whom the Personal Data are disclosed;
- (b) communication to him in an intelligible form of the Personal Data undergoing Processing and of any available information as to their source; and
- (c) as appropriate, the rectification, erasure or blocking of Personal Data the Processing of which does not comply with the provisions of these Regulations.

11. Right to object to Processing

- (1) A Data Subject has the right—
- (a) to object, at any time on reasonable grounds relating to his particular situation, to the Processing of Personal Data relating to him; and
 - (b) to be informed before Personal Data are disclosed for the first time to Third Parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object to such disclosures or uses.
- (2) Where there is a justified objection, the Processing instigated by the Data Controller shall no longer include those Personal Data.

Part 3 Notifications to the Registrar

12. Requirement to notify the Registrar

- (1) In order to be entitled to operate in such a capacity, a Data Controller must first be registered as a Data Controller with the Registrar. A Data Controller shall notify the Registrar of its intention to become a Data Controller in the required form. A Data Controller shall establish and maintain records of any Personal Data Processing operations or set of such operations intended to secure a single purpose or several related purposes.
- (2) The Registrar may by written notification prescribe
- (a) the information in relation to Personal Data Processing operations that shall be recorded for the purposes of subsection (1);
 - (b) the circumstances in which a Data Controller shall notify the Registrar of any

- operations referred to in subsection (1); and
- (c) the content of any such notification.
- (3) A Data Controller must also notify the Registrar of—
- (a) the appointment of a Data Processor, within one month of the appointment;
- (b) the cessation of a Data Processor, within one month of the cessation;
- (c) any change in the particulars of any appointed Data Processor within one month of the change; and
- (d) any change in its business contact details, within one month of the change.
- (4) The notifications required by subsections 12(1) and 12(3)(a) must be submitted to the Registrar on an annual basis where the Personal Data Processing is to continue in the subsequent year.
- (5) The annual notification in subsection 12(4) must be submitted to the Registrar, with payment of such fee(s) as prescribed by Schedule 4 of these Regulations, within one month of the previous annual notification expiring.
- (6) Natural persons acting in their capacity as staff for a Data Controller or Data Processor are not subject to any personal obligations to register or make notifications under these Regulations.

13. Register of notifications

The Registrar shall keep a register of Personal Data Processing operations and other information notified in accordance with section 12 available for inspection during normal business hours by any person.

Part 4 The Registrar

14. General Powers of the Registrar

- (1) The Registrar has such functions and powers as may be conferred on it by or under these Regulations and any other enactment.
- (2) The Registrar shall administer these Regulations and enforce its provisions.
- (3) Without limiting the generality of subsection (1), such powers and functions of the Registrar include the powers and functions, so far as are reasonably practicable, to—
- (a) access Personal Data Processed by Data Controllers or Data Processors;
- (b) collect all the information necessary for the performance of its supervisory duties;
- (c) prescribe forms to be used for any of the purposes of these Regulations;
- (d) issue directions or warnings and make recommendations to Data Controllers;
- (e) impose fines in the event of non-compliance with its direction; and

- (f) impose fines in the event of non-compliance with these Regulations and any rules made pursuant to these Regulations.

15. Production of information

- (1) The Registrar may require a Data Controller by written notice to–
 - (a) give specified information; or
 - (b) produce specified documents which relate to the Processing of Personal Data.
- (2) The Data Controller in respect of whom a requirement is made pursuant to subsection (1) shall comply with that requirement.

Part 5 The Board

16. Power to make rules

- (1) The Board may make rules in respect of any matters related to the Processing of Personal Data.
- (2) In particular, the Board when exercising the power in subsection (1) may make rules in respect of–
 - (a) forms, procedures and requirements under these Regulations;
 - (b) the keeping of the register of notifications established under section 13;
 - (c) the conduct of the Registrar and its staff in relation to the exercise of powers and performance of functions under these Regulations;
 - (d) the procedures relating to the imposition of sanctions or fines and the recovery of fines under Part 6;
 - (e) the level of fees payable for any matter listed in Schedule 4 to these Regulations or the level of fees payable for any other matter or step, and shall be entitled to amend any of the amounts specified in Schedule 4; and
 - (f) requiring any other fees to be paid in connection with any application or notification.
- (3) Where the Board issues a standard or code of practice, the Board may incorporate such a standard or code into the rules by reference and in such circumstances, except to the extent that the rules otherwise provide, a person who is subject to the provisions of any such standard or code shall comply with such provisions as if they were provisions of the rules.
- (4) Where any rules made for the purpose of these Regulations purport to be made in exercise of a particular power or powers, they shall be taken also to be made in the exercise of all powers under which they may be made.

Part 6 Remedies, Liability and Sanctions

17. Directions and compensation

- (1) If the Registrar is satisfied that a Data Controller, Data Processor or data controller

established outside the Abu Dhabi Global Market has contravened or is contravening these Regulations or any rules made under these Regulations, the Registrar may issue a direction to the Data Controller requiring him to do either or both of the following-

- (a) to do or refrain from doing any act or thing within such time as may be specified in the direction; or
 - (b) to refrain from Processing any Personal Data specified in the direction or to refrain from Processing Personal Data for a purpose or in a manner specified in the direction.
- (2) A direction issued under subsection (1) shall contain-
- (a) a statement of the contravention of these Regulations or rules which the Registrar is satisfied is being or has been committed; and
 - (b) a statement to the effect that the Data Controller may refer the matter the Court for review.
- (3) A Data Controller, who fails, without reasonable excuse, to comply with-
- (a) any direction issued by the Registrar under this section;
 - (b) these Regulations; or
 - (c) any rules made pursuant to these Regulations,
- commits a contravention of these Regulations and shall be liable to a fine of up to USD 25,000.
- (4) A Data Controller, who receives a direction under this section may refer the matter to the Court for review within three (3) months of the issuing of the direction.
- (5) A direction issued under subsection (1) is enforceable, on the application of the Registrar or any person authorised in writing by the Registrar, by injunction.
- (6) Any person who suffers damage by reason of any contravention by a Data Controller, Data Processor or data controller established outside the Abu Dhabi Global Market of any of the requirements of these Regulations or any rules made under these Regulations is entitled to compensation from the Data Controller, Data Processor or data controller for that damage.
- (7) In proceedings brought against a person by virtue of subsection (6), it is a defence to prove that he had taken such care as in all the circumstances was reasonably required to comply with the requirement concerned.
- (8) Court Procedure Rules may make provision for any reference to the Court under subsection (4).
- (9) A Data Controller may ask the Registrar to review the direction within fourteen (14) days of receiving a direction under this part of the Regulations. The Registrar may receive further submissions and amend or discontinue the direction.

17A. **Fines**

- (1) The Board may make rules in respect of the procedures relating to the imposition and

recovery of fines under this Part.

(2) Where the Registrar considers that a Data Controller has contravened—

- (a) any direction issued by the Registrar under section 17;
- (b) these Regulations; or
- (c) any rules made pursuant to these Regulations,

the Registrar, by written notice (a “monetary penalty notice”) to the Data Controller, may impose a fine in respect of the contravention.

(3) A monetary penalty notice is a written notice requiring the Data Controller to pay to the Registrar a fine of an amount determined by the Registrar as the Registrar may consider appropriate.

(4) The amount determined by the Registrar must not exceed the maximum fine specified in section 17(3).

(5) The fine must be paid to the Registrar within the period specified in the monetary penalty notice.

(6) The monetary penalty notice must contain such information as may be prescribed.

(7) A Data Controller, who receives a monetary penalty notice under this section, may refer the matter to the Court for review of—

- (a) the issue of the monetary penalty notice;
- (b) the amount of the fine specified in the notice.

(8) Court Procedure Rules may make provision for any reference to the Court under subsection (7).

(9) If, within the period specified in the monetary penalty notice—

- (a) the Data Controller pays the fine specified in the notice to the Registrar—
 - (i) subject to paragraph (ii) below, no proceeding or actions pursuant to this Part may be commenced, whether in the Court or otherwise, by the Registrar against the Data Controller in respect of the relevant contravention; and
 - (ii) without prejudice to paragraph (i) above, neither the imposition nor payment of a fine shall restrict the Registrar from taking any action against a Data Controller or refrain from doing any act or thing in relation to any continuing contravention; or
- (b) if all or any portion of the fine has not been paid at the end of the period stated in a monetary penalty notice, the obligation of the Data Controller to pay the fine is

enforceable as a debt payable to the Registrar. The Registrar may apply to the Court for the recovery of the debt.

- (10) In this section “prescribed” means prescribed by rules made by the Board pursuant to these Regulations.

17B. Certificates

A certificate that is signed by the Registrar and states that a direction under section 17 was issued to, or a monetary penalty notice prescribing a fine under section 17A was imposed on, a Data Controller is—

- (a) conclusive evidence of the giving of the direction or the imposition of the notice to the Data Controller; and
- (b) prima facie evidence of the facts contained in the direction or the notice,

in any proceeding commenced under section 17(4), 17(5), 17(6) or sections 17A(7) and 17A(9)(b).

17C. Referral to the Court

- (1) Any Data Controller who is found to contravene these regulations or a direction of the Registrar may refer the matter to the Court for review of the issuing of the finding or direction within three (3) months.
- (2) The Court Procedure Rules may make provision for any reference under subsection (1).

18. Lodging claims and mediation

- (1) A person who believes on reasonable grounds that he has been adversely affected by a contravention of these Regulations or any rules made under these Regulations in respect of the Processing of their Personal Data and as regards the exercise of their rights under sections 10 and 11 may lodge a claim with the Registrar.
- (2) Without prejudice to any of its powers under these Regulations, the Registrar may mediate between the affected Data Subject referred to in subsection (1) and the relevant Data Controller and may refer the dispute to the Court where it deems necessary.

Part 7 General Exemptions

19. General exemptions

- (1) The Board may make rules exempting Data Controllers from compliance with these Regulations or any parts of these Regulations.
- (2) Without prejudice to subsection (1) above, section 12 shall not apply to the Board, the Court, the Regulator or the Registrar, except that the Registrar is still required to maintain records per section 12(1) and where necessary, prescribe written notifications per section 12(2).
- (3) Without prejudice to subsection (1) above, none of sections 4, 5, 6, 7, 10, 11, 17 or 17A shall apply to the Board, the Court, the Regulator or the Registrar if the application of

these sections would be likely to prejudice the proper discharge by those entities of their powers or functions in so far as such powers or functions are designed for protecting members of the public against–

- (a) financial loss due to dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons carrying on any Controlled Activities; or
 - (b) dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons carrying on Regulated Activities.
- (4) The restrictions in these Regulations relating to the transfer of Personal Data and Sensitive Personal Data do not apply to the Board, the Court, the Regulator or the Registrar if disclosures are made pursuant to any memorandum of understanding or other arrangements for information exchange to any other governmental or other regulatory body or authority whether in the Abu Dhabi Global Market or otherwise for the purpose of assisting the performance by any such person of its functions and powers or made in good faith for the purposes of the exercise of the functions and powers of the Board, the Court, the Regulator, or the Registrar or in order to further the Court's, the Board's, the Regulator's or the Registrar's objectives.

20. Interpretation

In these Regulations, unless the context indicates otherwise, the defined terms listed below shall have the following meanings–

"Abu Dhabi Global Market" has the meaning given to "Abu Dhabi Global Market" in the Interpretation Regulations 2015;

"ADGM Founding Law" means Law No. 4 of 2013 concerning the Abu Dhabi Global Market issued by His Highness the Ruler of the Emirate of Abu Dhabi;

"Board" has the meaning given to "Board" in the Interpretation Regulations 2015;

"Company" has the meaning given to that term in the Financial Services and Markets Regulations 2015;

"Controlled Activities" means controlled activities as defined in the Commercial Licensing Regulations 2015;

"Court" has the meaning given to "Courts" in the Interpretation Regulation 2015;

"Court Procedure Rules" has the meaning given under Part 7 of the ADGM Courts, Civil Evidence, Judgments, Enforcement and Judicial Appointments Regulations 2015;

"Data" means any information which–

- (a) Is being processed by means of equipment operating automatically in response to instruction given for that purpose;
- (b) is recorded with the intention that it should be processed by means of such equipment; or

- (c) is recorded as part of a Relevant Filing System or with the intention that it should form part of a Relevant Filing System;

"Data Controller" means any person in the Abu Dhabi Global Market (excluding a natural person acting in his capacity as a staff member) who alone or jointly with others determines the purposes and means of the Processing of Personal Data;

"Data Processor" means any person (excluding a natural person acting in his capacity as a staff member) who Processes Personal Data on behalf of a Data Controller;

"Data Subject" shall mean the natural person to whom Personal Data relate;

"Group" has the meaning given to that term in the Financial Services and Markets Regulations 2015;

Identifiable Natural Person means a natural person who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his biological, physical, biometric, physiological, mental, economic, cultural or social identity;

"Personal Data" means any Data relating to an identified natural person or Identifiable Natural Person;

"Processing" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction, and "Processed", "Processes" and "Process" shall be construed accordingly;

"Recipient" means any person to whom Personal Data are disclosed, whether a Third Party or not, but does not include any person to whom disclosure is or may be made as a result of, or with a view to, a particular inquiry by or on behalf of that person made in the exercise of any power conferred by law;

"Registrar" means the "Registration Authority" as that term is defined in the Interpretation Regulations 2015;

"Regulated Activities" has the meaning given to it in the Financial Services and Markets Regulations 2015;

"Regulator" means the "Financial Services Regulator" as that term is defined in the Interpretation Regulations 2015;

"Relevant Filing System" means any set of information relating to an Identifiable Natural Person to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible;

"Sensitive Personal Data" means Personal Data revealing or concerning (directly or indirectly) racial or ethnic origin, political opinions, religious or philosophical beliefs, criminal record, trade-union membership and health or sex life;

"Staff" include past, existing or prospective employees, directors, partners, trustees, officers, office

holders, temporary or casual workers, agents and volunteers; and

"**Third Party**" means any person other than the Data Subject, the Data Controller, the Data Processor and the persons who, under the direct control of the Data Controller or the Data Processor, are authorised to Process the Personal Data.

21. **Short title, extent and commencement**

- (1) These Regulations may be cited as the Data Protection Regulations 2015.
- (2) These Regulations shall apply in the Abu Dhabi Global Market.
- (3) These Regulations shall come into force on the date of their publication. The Board may by rules make any transitional, transitory, consequential, saving, incidental or supplementary provision in relation to the commencement of these Regulations as the Board thinks fit.
- (4) Rules made under subsection (3) may amend any provision of any other enactment (including subordinate legislation made under such enactment).

SCHEDULE 1

DATA TRANSFER AGREEMENT (Data Controller to Data Controller transfers)

For the purposes of section 5 of the Data Protection Regulations 2015 (the "**Regulations**") for the transfer of Personal Data to data controllers established in jurisdictions outside the Abu Dhabi Global Market which do not ensure an adequate level of data protection ("**Non-Abu Dhabi Global Market Data Controllers**")

between

..... (name)

..... (address)

hereinafter, the "**Data Exporter**"

and

..... (name)

..... (address and jurisdiction of establishment)

hereinafter, the "**Data Importer**"

each a "Party"; together "the Parties",

The Parties agree as follows with respect to the transfer by the Data Exporter to the Data Importer of the Personal Data specified in Annex B.

1. Definitions and interpretation

For the purposes of the Clauses:

- (a) "**Data**", "**Personal Data**", "**Sensitive Personal Data**", "**Processing**", "**Data Controller**", "**Data Processor**", "**Data Subject**", "**Third Party**" and "**Court**" shall have the same meaning as in the Regulations;
- (b) "**Automated Decision**" shall mean a decision by the Data Exporter or the Data Importer which produces legal effects concerning a Data Subject or significantly affects a Data Subject and which is based solely on automated Processing of Personal Data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.;
- (c) "**Clauses**" shall mean the contractual clauses set out in this agreement, which constitute a free-standing agreement that does not incorporate commercial business terms established by the Parties under separate commercial arrangements, or rely or depend upon the same for its validity;
- (d) "**Data Exporter**" shall mean the Data Controller who transfers the Personal Data;
- (e) "**Data Importer**" shall mean the Non-Abu Dhabi Global Market Data Controller who agrees to receive from the Data Exporter Personal Data for further Processing in

accordance with the terms of these Clauses and who is not subject to a system outside the jurisdiction of the Abu Dhabi Global Market ensuring adequate protection within the meaning of section 4 of the Regulations;

- (f) **"Third Parties Act"** shall mean the Contracts (Rights of Third Parties Act) 1999 as applied in the Abu Dhabi Global Market by virtue of the Application of English Law Regulations 2015.

The details of the transfer (as well as the Personal Data covered) are specified in Annex B, which forms an integral part of the Clauses.

2. Obligations of the Data Exporter

The Data Exporter warrants and undertakes that–

- (a) the Personal Data have been collected, Processed and transferred in accordance with the Regulations;
- (b) it has used reasonable efforts to determine that the Data Importer is able to satisfy its legal obligations under these Clauses;
- (c) it will provide the Data Importer, when so requested, with copies of the Regulations or references to them (where relevant, and not including legal advice);
- (d) if the transfer involves Sensitive Personal Data the Data Exporter is in compliance with section 3 of the Regulations in respect of the transfer to the Data Importer; and
- (e) it will respond to enquiries from Data Subjects and the Registrar concerning Processing of the Personal Data by the Data Importer, unless the Parties have agreed that the Data Importer will so respond, in which case the Data Exporter will still respond to the extent reasonably possible and with the information reasonably available to it if the Data Importer is unwilling or unable to respond. Such responses will be made within a reasonable time.

3. Obligations of the Data Importer

(1) The Data Importer warrants and undertakes that–

- (a) it will have in place appropriate technical and organisational measures to protect the Personal Data against unauthorised or unlawful processing and against accidental loss or destruction or damage, and which provide a level of security appropriate to the risk represented by the Processing and the nature of the Data to be protected;
- (b) it will have in place procedures so that any Third Party it authorises to have access to the Personal Data, including Data Processors, will respect and maintain the confidentiality and security of the Personal Data. Any person acting under the authority of the Data Importer, including a Data Processor, shall be obligated to Process the Personal Data only on instructions from the Data Importer. This provision does not apply to persons authorised or required by the Regulations to have access to the Personal Data;
- (c) it has no reason to believe in the existence of any non-Abu Dhabi Global Market laws that would have a substantial adverse effect on the enforceability of these

Clauses, and it will promptly inform the Data Exporter (which will pass such notification on to the Registrar where required) if it becomes aware of any such laws or any changes in such laws which have such a substantial adverse effect;

(d) it will Process the Personal Data for purposes described in Annex B, and has the legal authority to give the warranties and fulfil the undertakings set out in these Clauses;

(e) it will identify to the Data Exporter a contact point within its organisation authorised to respond to enquiries concerning Processing of the Personal Data, and will cooperate in good faith with the Data Exporter, the Data Subject and the Registrar concerning all such enquiries within a reasonable time;

(f) at the request of the Data Exporter, it will provide the Data Exporter with evidence of financial resources sufficient to fulfil its responsibilities under Clause 4 (which may include insurance coverage);

(g) upon reasonable request of the Data Exporter, it will submit its Data Processing facilities, Data files and documentation needed for Processing to reviewing, auditing and/or certifying by the Data Exporter (or any independent or impartial inspection agents or auditors, selected by the Data Exporter and not reasonably objected to by the Data Importer) to ascertain compliance with the warranties and undertakings in these Clauses, with reasonable notice and during regular business hours. The request will be subject to any necessary consent or approval from a regulatory or supervisory authority within the country of the Data Importer, which the Data Importer will attempt to obtain in a timely fashion;

(h) it will Process the Personal Data, at its option, in accordance with–

(i) the Regulations, or

(ii) the Data Processing principles set forth in Annex A,

Data Importer to indicate which option it selects:

Initials of Data Importer:; and

(i) it will promptly notify the Data Exporter about–

(i) any legally binding request for disclosure of the Personal Data by a law enforcement authority unless otherwise prohibited, such as a prohibition under the criminal law of any jurisdiction outside the Abu Dhabi Global Market to preserve the confidentiality of a law enforcement investigation;

(ii) any accidental or unauthorised access; and

(iii) any request received directly from the Data Subjects without responding to that request, unless it has been otherwise authorised to do so.

(2) The Data Importer warrants and undertakes that it will not disclose or transfer the Personal Data to a third party data controller located outside the Abu Dhabi Global Market unless it notifies the Data Exporter about the transfer and–

- (i) the third party data controller processes the Personal Data in accordance with the laws of a jurisdiction outside the Abu Dhabi Global Market that has been designated under the Regulations or by the Registrar as providing adequate protection for Personal Data;
- (ii) the third party data controller becomes a signatory to these Clauses or another data transfer agreement approved by the Registrar;
- (iii) Data Subjects have been given the opportunity to object, after having been informed of the purposes of the transfer, the categories of recipients and the fact that the jurisdictions to which Data is exported may have different data protection standards; or
- (iv) with regard to onward transfers of Sensitive Personal Data, Data Subjects have given their consent to the onward transfer.

4. Third Party rights

- (1) Unless expressly provided to the contrary in these Clauses, a person who is not a Party has no right under the Third Parties Act to enforce or to enjoy the benefit of any provision of these Clauses.
- (2) Notwithstanding any provision of these Clauses, the consent of any person who is not a Party is not required to rescind or vary these Clauses at any time.
- (3) Any Data Subject may rely on and enforce any provision of these Clauses which expressly confers rights on it against the Data Importer or Data Exporter.
- (4) The Parties do not object to a Data Subject being represented by an association or other body if the Data Subject so expressly wishes and if permitted by relevant national law.

5. Liability

- (1) Each Party shall be liable to the other Parties for damages it causes by any breach of these Clauses. Liability as between the Parties is limited to actual damage suffered. Punitive damages (i.e. damages intended to punish a Party for its outrageous conduct) are specifically excluded.
- (2) Each Party shall be liable to Data Subjects for damages it causes by any breach of Third Party rights under these Clauses. This does not affect the liability of the Data Exporter under the Regulations.
- (3) In cases involving allegations of breach by the Data Importer, the Data Subject must first request the Data Exporter to take appropriate action to enforce his rights against the Data Importer; if the Data Exporter does not take such action within a reasonable period (which under normal circumstances would be one month), the Data Subject may then enforce his rights against the Data Importer directly. A Data Subject is entitled to proceed directly against a Data Exporter that has failed to use reasonable efforts to determine that the Data Importer is able to satisfy its legal obligations under these Clauses (the Data Exporter shall have the burden to prove that it took reasonable efforts).

6. Law applicable to the Clauses

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

7. Resolution of disputes with Data Subjects or the Registrar

- (1) In the event of a dispute or claim brought by a Data Subject or the Registrar concerning the Processing of the Personal Data against either or both of the Parties, the Parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.
- (2) The Parties agree to respond to any generally available non-binding mediation procedure initiated by a Data Subject or by the Registrar. If they do participate in the proceedings, the Parties may elect to do so remotely (such as by telephone or other electronic means). The Parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.
- (3) Each Party shall abide by a decision of the Court.
- (4) The Parties agree that the Registrar has the right to exercise its functions and powers outlined in section 14 of the Regulations in respect of the Data Importer, in the same scope and subject to the same conditions as would apply the to Data Exporter under the Regulations.

8. Termination

- (1) In the event that the Data Importer is in breach of its obligations under these Clauses, then the Data Exporter may temporarily suspend the transfer of Personal Data to the Data Importer until the breach is repaired or the contract is terminated.
- (2) In the event that–
 - (a) the transfer of Personal Data to the Data Importer has been temporarily suspended by the Data Exporter for longer than one month pursuant to sub-clause (1);
 - (b) compliance by the Data Importer with these Clauses would put it in breach of its legal or regulatory obligations in the jurisdiction of import;
 - (c) the Data Importer is in substantial or persistent breach of any warranties or undertakings given by it under these Clauses;
 - (d) a final decision of the Court or a decision of the Registrar rules that there has been a breach of the Clauses by the Data Importer or the Data Exporter; or
 - (e) a petition is presented for the administration or winding-up of the Data Importer, which is not dismissed within the applicable period for such dismissal under the Insolvency Regulations 2015, a winding-up order is made, a receiver is appointed over any of its assets, a trustee in bankruptcy is appointed, a company voluntary arrangement is commenced by it, or any equivalent event in any jurisdiction occurs,

then the Data Exporter, without prejudice to any other rights which it may have against the Data Importer, shall be entitled to terminate these Clauses, in which case the Registrar shall be informed where required. In cases covered by (a), (b), or (d) above, the Data Importer may also terminate these Clauses.

- (3) Either Party may terminate these Clauses if each jurisdiction in which the Data Importer is incorporated or operates or uses the Personal Data is either: (a) subject to a designation under section 4 of the Regulations by the Registrar; or (b) is or becomes listed in Schedule 3 to the Regulations.
- (4) The Parties agree that the termination of these Clauses at any time, in any circumstances and for whatever reason (except for termination under sub-clause (3)) does not exempt them from the obligations and/or conditions under the Clauses as regards the Processing of the Personal Data transferred.

9. Variation of these Clauses

The Parties may not modify these Clauses except to update any information in Annex B. This does not preclude the Parties from adding additional commercial clauses where required as long as they do not contradict the Clauses.

10. Description of the Transfer

The details of the transfer and of the Personal Data are specified in Annex B. The Parties agree that Annex B may contain confidential business information which they will not disclose to Third Parties, except as required by the Regulations or in response to a competent regulatory or government agency. The Parties may execute additional annexes to cover additional transfers, which will be submitted to the Registrar where required. Annex B may, in the alternative, be drafted to cover multiple transfers.

Dated:

On behalf of the Data Exporter:

Name (in full):

Position:

Address:

Signature.....

[stamp of organisation]

On behalf of the Data Importer:

Name (in full):

Position:

Address:

Signature.....

[stamp of organisation]

ANNEX A
DATA PROCESSING PRINCIPLES

1. Purpose limitation: Personal Data may be Processed and subsequently used or further communicated only for purposes described in Annex B or subsequently authorised by the Data Subject.
2. Data quality and proportionality: Personal Data must be accurate and, where necessary, kept up to date. The Personal Data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further Processed.
3. Transparency: Data Subjects must be provided with information necessary to ensure fair Processing (such as information about the purposes of Processing and about the transfer), unless such information has already been given by the Data Exporter.
4. Security and confidentiality: Technical and organisational security measures must be taken by the Data Controller that are appropriate to the risks, such as against unlawful or unauthorised Processing of Personal Data and against accidental loss or destruction of, or damage to, such Personal Data. Any person acting under the authority of the Data Controller, including a Data Processor, must provide sufficient guarantees that such technical measures shall be complied with.
5. Rights of access, rectification, erasure or blocking: Data Subjects have the right to be provided with written confirmation as to whether Personal Data relating to them are being Processed, provided that such requests are made at reasonable intervals. Data Subjects must also be able to have their Personal Data rectified, erased or blocked, as appropriate, where it is Processed against the requirements of the Regulations. A Data Subject must also be able to object to the Processing of the Personal Data relating to him if there are reasonable grounds for such an objection, and such grounds relate to his particular situation.
6. Sensitive Personal Data: The Data Importer shall take such additional measures (e.g. relating to security) as are necessary to protect Sensitive Personal Data in accordance with its obligations under Clause 3 or the Data Exporter's obligations under the Regulations.
7. Data used for marketing purposes: Where Data are Processed for the purposes of direct marketing, effective procedures should exist allowing the Data Subject at any time to object to having his Data used for such purposes.
8. Automated Decisions: The Data Importer shall not make any Automated Decisions concerning Data Subjects, except when –
 - (a)
 - (i) such decisions are made by the Data Importer in entering into or performing a contract with the Data Subject; and
 - (ii) the Data Subject is given an opportunity to discuss the results of a relevant Automated Decision with a representative of the parties making such decision or otherwise to make representations to those parties; or
 - (b) where otherwise provided by the Regulations.

**ANNEX B
DESCRIPTION OF THE TRANSFER**

This Annex forms part of the Clauses and must be completed and signed by the Parties.

Data Subjects

The Personal Data transferred concern the following categories of Data Subjects:

.....
.....
.....

Purposes of the transfer(s)

The transfer is made for the following purposes:

.....
.....
.....

Categories of Data

The Personal Data transferred concern the following categories of Data:

.....
.....
.....

Recipients

The Personal Data transferred may be disclosed only to the following recipients or categories of recipients:

.....
.....
.....

Sensitive Personal Data (if appropriate)

The Personal Data transferred concern the following categories of Sensitive Personal Data:

.....
.....
.....

Additional useful information (storage limits and other relevant information)

.....
.....
.....

Contact points for Data protection enquiries:

Data Importer

.....
.....

Data Exporter

.....
.....

ILLUSTRATIVE COMMERCIAL CLAUSES (OPTIONAL)

Indemnification between the Data Exporter and Data Importer:

"The Parties will indemnify each other and hold each other harmless from any cost, charge, damages, expense or loss which they cause each other as a result of their breach of any of the provisions of these Clauses. Indemnification hereunder is contingent upon (a) the Party(ies) to be indemnified (the "Indemnified Party(ies)") promptly notifying the other Party(ies) (the "Indemnifying Party(ies)") of a claim; (b) the Indemnifying Party(ies) having sole control of the defence and settlement of any such claim; and (c) the Indemnified Party(ies) providing reasonable cooperation and assistance to the Indemnifying Party(ies) in defence of such claim."

Allocation of costs:

"Each Party shall perform its obligations under these Clauses at its own cost."

Extra termination clause:

"In the event of termination of these Clauses, the Data Importer must return all Personal Data and all copies of the Personal Data subject to these Clauses to the Data Exporter forthwith or, at the Data Exporter's choice, will destroy all copies of the same and certify to the Data Exporter that it has done so, unless the Data Importer is prevented by its national law or local regulator from destroying or returning all or part of such Data, in which event the Data will be kept confidential and will not be actively Processed for any purpose. The Data Importer agrees that, if so requested by the Data Exporter, it will allow the Data Exporter, or an inspection agent selected by the Data Exporter and not reasonably objected to by the Data Importer, access to its establishment to verify that this has been done, with reasonable notice and during business hours."

SCHEDULE 2

**DATA TRANSFER AGREEMENT
(Data Controller to Data Processor transfers)**

For the purposes of section 5 of the Data Protection Regulations 2015 (the "**Regulations**") for the transfer of Personal Data to Data Processors established in jurisdictions outside the Abu Dhabi Global Market which do not ensure an adequate level of data protection

between

..... (name)

..... (address)

hereinafter, the "**Data Exporter**"

and

..... (name)

..... (address)

hereinafter, the "**Data Importer**"

each a "Party"; together "the Parties",

The Parties agree as follows with respect to the transfer by the Data Exporter to the Data Importer of the Personal Data specified in Annex A.

1. Definitions and interpretation

For the purposes of the Clauses–

- (a) "**Data**", "**Personal Data**", "**Processing**", "**Data Controller**", "**Data Processor**", "**Data Subject**", "**Third Party**" and "**Court**" shall have the same meaning as in the Regulations;
- (b) "**Clauses**" shall mean the contractual clauses set out in this agreement which constitute a free-standing agreement that does not incorporate commercial business terms established by the Parties under separate commercial arrangements, or rely or depend upon the same for its validity;
- (c) "**Data Exporter**" means the Data Controller who transfers the Personal Data;
- (d) "**Data Importer**" means the data processor who agrees to receive from the Data Exporter Personal Data intended for Processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a legal system in a jurisdiction outside the Abu Dhabi Global Market ensuring adequate protection within the meaning of section 4 of the Regulations;
- (e) "**Subprocessor**" means any Data Processor engaged by the Data Importer or by any other subprocessor of the Data Importer who agrees to receive from the Data Importer or from any other subprocessor of the Data Importer Personal Data

exclusively intended for Processing activities to be carried out on behalf of the Data Exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

- (f) **"Third Parties Act"** shall mean the Contracts (Rights of Third Parties Act) 1999 as applied in the Abu Dhabi Global Market by virtue of the Application of English Law Regulations 2015.

2. Details of the transfer

The details of the transfer and in particular the categories of Personal Data subject to the transfer are specified in Annex A which forms an integral part of the Clauses.

3. Third Party rights

- (1) Unless expressly provided to the contrary in these Clauses, a person who is not a Party has no right under the Third Parties Act to enforce or enjoy the benefit of any provision of these Clauses.
- (2) Notwithstanding any provision of these Clauses, the consent of any person who is not a Party is not required to rescind or vary these Clauses at any time.
- (3) Any Data Subject may rely on and enforce any provision of these Clauses which expressly confers rights on it against any of the Parties or a Subprocessor.
- (4) The Parties do not object to a Data Subject being represented by an association or other body if the Data Subject so expressly wishes and if permitted by relevant national law.

4. Obligations of the Data Exporter

The Data Exporter agrees and warrants–

- (a) that the Processing, including the transfer itself, of the Personal Data has been and will continue to be carried out in accordance with the relevant provisions of the Regulations (and, where applicable, has been notified to the Registrar) and does not violate those Regulations;
- (b) that it has instructed, and throughout the duration of the Personal Data Processing services will instruct, the Data Importer to Process the Personal Data transferred only on the Data Exporter's behalf and in accordance with the Regulations and the Clauses;
- (c) that the Data Importer will provide sufficient guarantees in respect of the technical and organisational measures specified in Annex B to these Clauses;
- (d) that after assessment of the requirements of the Regulations, the security measures are appropriate to protect Personal Data against unauthorised or unlawful Processing and against accidental loss or destruction or damage, particularly where the Processing involves the transmission of Data over a network, and against all other unlawful forms of Processing, and that these measures ensure a level of security appropriate to the risks presented by the Processing and the nature of the Data to be protected having regard to the state of the art and the cost of their implementation;
- (e) that it will ensure compliance with the security measures specified in paragraph (d);

- (f) that, if the transfer involves Sensitive Personal Data, the Data Exporter is in compliance with section 3 of the Regulations in respect of the transfer to the Data Importer;
- (g) that, in the event of subprocessing, the Processing activity is carried out in accordance with Clause 11 by a Subprocessor providing at least the same level of protection for the Personal Data and the rights of the Data Subject as the Data Importer under the Clauses; and
- (h) that it will ensure compliance with Clause 4(a) to (g).

5. **Obligations of the Data Importer**

The Data Importer agrees and warrants–

- (a) to Process the Personal Data only on behalf of the Data Exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reason, it agrees to inform the Data Exporter promptly of its inability to comply, in which case the Data Exporter is entitled to suspend the transfer of Data and/or terminate the Clauses;
- (b) that it has no reason to believe in the existence of any non-Abu Dhabi Global Market laws that would have a substantial adverse effect on the enforceability of these Clauses, and it will promptly inform the Data Exporter (which will pass such notification on to the Registrar where required) if it becomes aware of any such laws or any changes in such laws which have such a substantial adverse effect;
- (c) that it has implemented the technical and organisational measures specified in Annex B before Processing the Personal Data transferred;
- (d) that it will promptly notify the Data Exporter about–
 - (i) any legally binding request for disclosure of the Personal Data by a law enforcement authority unless otherwise prohibited, such as a prohibition under the criminal law of any jurisdiction outside the Abu Dhabi Global Market to preserve the confidentiality of a law enforcement investigation;
 - (ii) any accidental or unauthorised access; and
 - (iii) any request received directly from the Data Subjects without responding to that request, unless it has been otherwise authorised to do so;
- (e) to deal promptly and properly with all inquiries from the Data Exporter relating to its Processing of the Personal Data subject to the transfer and to abide by the advice of the Registrar with regard to the Processing of the Data transferred;
- (f) at the request of the Data Exporter to submit its Data Processing facilities for audit of the Processing activities covered by the Clauses which shall be carried out by the Data Exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the Data Exporter, where applicable, in agreement with the Registrar;
- (g) to make available to the Data Subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial

information, in which case it may redact such commercial information, with the exception of Annex B which shall minimally be replaced by a summary description of the security measures in those cases where the Data Subject is unable to obtain a copy from the Data Exporter;

- (h) that, in the event of subprocessing, it has previously informed the Data Exporter and obtained its prior written consent;
- (i) that the Processing services by the Subprocessor will be carried out in accordance with Clause 11; and
- (j) to send promptly a copy of any Subprocessor agreement it concludes under the Clauses to the Data Exporter.

6. Liability and termination

- (1) The Parties agree that any Data Subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any Party or Subprocessor is entitled to receive compensation from the Data Exporter for the damage suffered.
- (2)
 - (a) If a Data Subject is not able to bring a claim for compensation in accordance with sub-clause (1) against the Data Exporter, arising out of a breach by the Data Importer or his Subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the Data Exporter has factually disappeared or ceased to exist in law or has become insolvent, the Data Importer agrees that the Data Subject may issue a claim against the Data Importer as if it were the Data Exporter, unless any successor entity has assumed the entire legal obligations of the Data Exporter by contract or by operation of law, in which case the Data Subject can enforce its rights against such entity.
 - (b) The Data Importer may not rely on a breach by a Subprocessor of its obligations in order to avoid its own liabilities.
- (3) If a Data Subject is not able to bring a claim against the Data Exporter or the Data Importer referred to in sub-clauses (1) and (2), arising out of a breach by the Subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the Data Exporter and the Data Importer have factually disappeared or ceased to exist in law or have become insolvent, the Subprocessor agrees that the Data Subject may issue a claim against the Data Subprocessor with regard to its own Processing operations under the Clauses as if it were the Data Exporter or the Data Importer, unless any successor entity has assumed the entire legal obligations of the Data Exporter or Data Importer by contract or by operation of law, in which case the Data Subject can enforce its rights against such entity. The liability of the Subprocessor shall be limited to its own Processing operations under the Clauses.
- (4) In addition to the Data Exporter's entitlement to terminate the Clauses in accordance with Clause 5(a), either Party may terminate these Clauses if: each jurisdiction in which the Data Importer and each of its Subprocessors is incorporated or operates or uses the Personal Data is either: (a) subject to a designation under section 4 of the Regulations by the Registrar; or (b) is or becomes listed in Schedule 3 to the Regulations.

- (5) The Parties agree that the termination of these Clauses at any time, in any circumstances and for whatever reason (except for termination under sub-clause (4)) does not exempt them from the obligations and/or conditions under the Clauses as regards the Processing of the Personal Data transferred.

7. Mediation and jurisdiction

- (1) The Data Importer agrees that if the Data Subject invokes against it Third Party beneficiary rights and/or claims of compensation for damages under the Clauses, the Data Importer will accept the decision of the Data Subject–
- (a) to refer the dispute to mediation, by an independent person or, where applicable, by the Registrar; and
- (b) to refer the dispute to the Court.
- (2) The Parties agree that the choice made by the Data Subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

8. Cooperation with the Registrar

- (1) The Data Exporter shall be entitled to deposit a copy of these Clauses with the Registrar if the Registrar so requests or if such deposit is required under the Regulations.
- (2) The Parties agree that the Registrar has the right to exercise its functions and powers outlined in section 14 of the Regulations in respect of the Data Importer and any Subprocessor, in the same scope and subject to the same conditions as would apply to a Data Processor of the Data Exporter under the Regulations.

9. Governing Law

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

10. Variation of the clauses

The Parties undertake not to vary or modify the Clauses except to update any information in Annex A. This does not preclude the Parties from adding clauses on business related issues where required, as long as they do not contradict the Clauses.

11. Subprocessing

- (1) The Data Importer shall not subcontract any of its Processing operations performed on behalf of the Data Exporter under the Clauses without the prior written consent of the Data Exporter. Where the Data Importer subcontracts its obligations under the Clauses with the consent of the Data Exporter, it shall do so only by way of a written agreement with the Subprocessor which imposes the same obligations on the Subprocessor as are imposed on the Data Importer under the Clauses. This may be satisfied by the Subprocessor executing and becoming bound contractually by the Clauses as entered into between the Data Exporter and the Data Importer. Where the Subprocessor fails to fulfil its data protection obligations under such written agreement, the Data Importer shall remain fully liable to the Data Exporter for the performance of the Subprocessor's obligations under such agreement.

- (2) The prior written contract between the Data Importer and the Subprocessor shall also provide for a Third Party beneficiary clause as laid down in Clause 3 for cases where the Data Subject is not able to bring the claim for compensation referred to in Clause 6(1) against the Data Exporter or the Data Importer because they have factually disappeared or have ceased to exist in law or have become insolvent, and no successor entity has assumed the entire legal obligations of the Data Exporter or Data Importer by contract or by operation of law. Such third party liability of the Subprocessor shall be limited to its own Processing operations under the Clauses.
- (3) The provisions relating to data protection aspects for subprocessing of the contract referred to in sub-clause (1) shall be governed by the law of the Abu Dhabi Global Market.
- (4) The Data Exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the Data Importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be made available to the Registrar.

12. Obligation after the termination of Personal Data Processing services

- (1) The Parties agree that on the termination of the provision of Data Processing services, the Data Importer and the Subprocessor shall, at the choice of the Data Exporter, return all the Personal Data transferred and the copies thereof to the Data Exporter or shall destroy all the Personal Data and certify to the Data Exporter that it has done so, unless legislation imposed upon the Data Importer prevents it from returning or destroying all or part of the Personal Data transferred. In that case, the Data Importer warrants that it will guarantee the confidentiality of the Personal Data transferred and will not actively process the Personal Data transferred any further.
- (2) The Data Importer and the Subprocessor warrant that upon request of the Data Exporter and/or of the Registrar, it will submit its Data Processing facilities for an audit of the measures referred to in sub-clause (1).

Dated:

On behalf of the Data Exporter:

Name (in full):

Position:

Address:

Signature.....

[stamp of organisation]

On behalf of the Data Importer:

Name (in full):

Position:

Address:

Signature.....

[stamp of organisation]

ANNEX A

This Annex forms part of the Clauses and must be completed and signed by the Parties.

The Registrar may complete or specify any additional necessary information to be contained in this Appendix.

Data Exporter

The Data Exporter is (please specify briefly your activities relevant to the transfer):

.....
.....

Data Importer

The Data Importer is (please specify briefly activities relevant to the transfer):

.....
.....

Data Subjects

The Personal Data transferred concern the following categories of Data Subjects (please specify):

.....
.....

Categories of Data

The Personal Data transferred concern the following categories of Data (please specify):

.....
.....

Sensitive Personal Data (if appropriate)

The Personal Data transferred concern the following sensitive Personal Data (please specify):

.....
.....

Processing operations

The Personal Data transferred will be subject to the following basic Processing activities (please specify):

.....
.....

DATA EXPORTER

Name:.....

Authorised Signature

DATA IMPORTER

Name:.....

Authorised Signature

ANNEX B

This Annex forms part of the Clauses and must be completed and signed by the Parties.

Description of the technical and organisational measures to protect Personal Data against unauthorised or unlawful Processing, and against accidental loss or destruction of, or damage to, Personal Data, implemented by the Data Importer in accordance with Clauses 4(d) and 5(c):

.....
.....
.....

ILLUSTRATIVE INDEMNIFICATION CLAUSE (OPTIONAL)

Liability:

The Parties agree that if one Party is held liable for a violation of the Clauses committed by the other Party, the latter will, to the extent to which it is liable, indemnify the first Party for any cost, charge, damages, expenses or loss it has incurred.

Indemnification is contingent upon—

- (a) the Data Exporter promptly notifying the Data Importer of a claim; and
- (b) the Data Importer being given the possibility to cooperate with the Data Exporter in the defence and settlement of the claim.

SCHEDULE 3 JURISDICTIONS WITH AN ADEQUATE LEVEL OF PROTECTION

The following jurisdictions have been designated herein as providing an adequate level of protection in accordance with section 4–

- (1) Andorra
- (2) Argentina
- (3) Austria
- (4) Belgium
- (5) Bulgaria
- (6) Canada (provided the recipient is subject to the Canadian Personal Information Protection and Electronic Documents Act [PIPED Act])
- (7) Cyprus
- (8) Czech Republic
- (9) Denmark
- (10) Dubai International Financial Centre
- (11) Estonia
- (12) Faeroe Islands
- (13) Finland
- (14) France
- (15) Germany
- (16) Greece
- (17) Guernsey
- (18) Hungary
- (19) Jersey
- (20) Iceland
- (21) Ireland
- (22) Isle of Man
- (23) Italy
- (24) Latvia
- (25) Liechtenstein

- (26) Lithuania
- (27) Luxembourg
- (28) Malta
- (29) Netherlands
- (30) New Zealand
- (31) Norway
- (32) Poland
- (33) Portugal
- (34) Romania
- (35) Slovakia
- (36) Slovenia
- (37) Spain
- (38) Sweden
- (39) Switzerland
- (40) United Kingdom
- (41) Uruguay
- (42) United States of America, subject to compliance with the terms of the EU-US Privacy Shield.

SCHEDULE 4 FEES

The following fees are payable by a Data Controller or Data Processor in respect of the applications and notifications made in accordance with the Regulations–

<u>Application or notification</u>	<u>Fee payable (USD)</u>
Application for initial registration as a Data Controller	300
Application for initial appointment of a Data Processor (per appointment if more than one Data Processor)	Nil
Annual renewal of registration as a Data Controller	100
Annual renewal of appointment of a Data Processor (per appointment if more than one Data Processor)	Nil
Notification of Data Controller no longer Processing Personal Data and/or removal of a Data Processor	Nil
Notification of change in the particulars of an appointed or Data Processor	Nil
Notification of a change in the contact details of a Data Controller	Nil
Application to obtain a permit to process Sensitive Personal Data	100
Application to obtain a permit to transfer Personal Data	100