Restricted Transfers and Special Local Country Provisions

The following provisions supplement the Parties' Data Protection Addendum ("Addendum") relating to the Processing and/or transfer of Personal Data, and may be updated from time to time by Gallagher only as necessary to comply with applicable Data Privacy Laws.

Definitions

In addition to the defined terms in the Addendum, the following definitions shall apply to the Restricted Transfer and Special Local Country Provisions:

"Data Discloser"	means the party disclosing Personal Data to the Data Recipient.
"Data Recipient"	means the party receiving Personal Data from or on behalf of the Data Discloser.
"EU Restricted Transfer"	means a Restricted Transfer of Personal Data by Data Discloser or any of its affiliates to the Data Recipient where such transfer would be prohibited by EU Data Privacy Laws in the absence of the protection for the transferred Personal Data provided by the EU Standard Contractual Clauses.
"EU Standard Contractual Clauses"	means the standard contractual clauses set out in the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, as amended or replaced from time to time by a competent authority under the applicable Data Privacy Laws.
"EU Standard Controller to Controller Clauses"	means Module 1 of the EU Standard Contractual Clauses.
"UK Addendum"	means the EU Standard Contractual Clauses as amended by the International Data Transfer Addendum to the EU Standard Contractual Clauses issued by the UK Information Commissioner.
"UK Restricted Transfer"	means a Restricted Transfer of Personal Data by the Data Discloser or any of its affiliates to the Data Recipient where such transfer would be prohibited by UK Data Privacy Laws in the absence of the protection for the transferred Personal Data provided by the UK Addendum.

A. Restricted Transfer Provisions

1. In respect of any EU Restricted Transfer, Data Discloser ("**data exporter"**) and Data Recipient ("**data importe**r") with effect from the commencement of any EU Restricted Transfer, hereby enter into the EU Standard Controller to Controller Clauses, which are incorporated herein by reference and which shall be deemed to be amended as follows:

    a. Clause 7 – Docking clause of the EU Standard Contractual Clauses shall not apply;

    b. Clause 11(a) – Redress of the EU Standard Contractual Clauses, the optional language shall not apply;

c. Clause 13(a) – Supervision of EU Standard Contractual Clauses: the supervisory authority with responsibility for ensuring compliance by the Data Discloser (as "data exporter") with Regulation (EU) 2016/679 as regards the Personal Data transfer, shall act as the competent supervisory authority;

d. Clause 17 – Governing law of the EU Standard Contractual Clauses "Option 1" shall apply and the "Member State" shall be Ireland;

e. Clause 18 – For the choice of forum and jurisdiction of the EU Standard Contractual Clauses, the Member State shall be Ireland;

f. Annex I of the EU Standard Controller to Controller Clauses shall be deemed to be pre-populated with the detail set out in Annex 1 attached to the Addendum;

g. Annex II of the EU Standard Controller to Controller Clauses shall be deemed to be pre-populated with the technical and organisational measures set out in Annex II attached to the Addendum.

2. In respect of any UK Restricted Transfer, Data Discloser ("**data exporter"**) and Data Recipient (**"data importer"**), with effect from the commencement of any UK Restricted Transfer, hereby enter into the UK Addendum which is incorporated herein by reference and shall be deemed completed as follows:

   a. Table 1 shall be populated with the details of the relevant parties as set out in Annex 1 attached to the Addendum;

   b. Table 2 shall be completed as follows:

      i. The second tick box shall be selected;

      ii. Module 1 shall be indicated as being in operation as Personal Data is shared by Data Discloser as a Controller to the Data Recipient as Controller;

      iii. The remainder of Table 2 shall be populated with the relevant options set out in Section 1 above;

   c. Table 3 shall be populated with the information set out in Annex I and II attached to the Addendum;

   d. Table 4 shall be completed as "neither party".

3. In respect of any Restricted Transfer which is neither an EU Restricted Transfer nor a UK Restricted Transfer, Data Discloser (as "**data exporter"**) and Data Recipient (as **"data importer"**), with effect from the commencement of any such Restricted Transfer, hereby enter into the EU Standard Contractual Clauses, which shall be deemed amended as is necessary to comply with applicable Data Privacy Laws and as set out in section 1 above, provided and only to the extent that such choices and amends are permitted under applicable Data Privacy Laws.

4. If, at any time, a Data Protection Regulator or a court with competent jurisdiction over a Party mandates that transfers from Controllers in the European Economic Area ("**EEA")** or the United Kingdom ("**UK**") to Controllers established outside the EEA or the UK must be subject to specific additional safeguards (including but not limited to specific technical and organisational measures), the Parties shall work together in good faith to implement such safeguards and ensure that any transfer of Personal Data is conducted with the benefit of such additional safeguards.

5. If and to the extent that any term contained in the Addendum governing the Processing of Personal Data conflicts with any term contained in the EU Standard Controller to Controller Clauses or the UK Addendum, the applicable term in the EU Standard Controller to Controller Clauses or the UK Addendum shall prevail.

B. Special Local Country Provisions

The following terms and conditions shall only apply to the extent that Personal Data is Processed in or transferred from any jurisdiction identified below.

PART A: Terms and Conditions of the Processing of Personal Data Subject to DIFC Data Protection Law

The following provisions shall amend, replace and supplement the corresponding provisions in the definitions section of this Addendum and the EU Standard Controller to Controller Clauses.

1 Definitions

"DIFC" means the Dubai International Financial Centre, established pursuant to United Arab Emirates Federal Law No. 8 of 2004 on Financial Free Zones and Dubai Law No. 9 of 2004 establishing the Dubai International Financial Centre;

"DIFC Data Protection Commissioner" means the person appointed by the DIFC president pursuant to article 43(1) of the DIFC Data Protection Law to administer the DIFC Data Protection Law;

"DIFC Data Protection Law" means DIFC Law No. 5 of 2020 establishing the DIFC Data Protection Law;

"DIFC Restricted Transfer" means a transfer of Personal Data by Data Discloser to the Data Recipient (or any onward transfer by the Data Recipient), in each case, where such transfer would be prohibited by the DIFC Data Protection Law in the absence of the protection for the transferred Personal Data provided by the DIFC Standard Contractual Clauses; and

"DIFC Standard Contractual Clauses" means the standard contractual clauses published by the DIFC Data Protection Commissioner to apply to DIFC Restricted Transfers, as amended or replaced from time to time by a competent authority under the relevant Data Protection Laws.

2 International Transfers

2.1 In respect of any DIFC Restricted Transfer, the Data Discloser (**"data exporter"**) and the Data Recipient (as **"data importer"**) with effect from any DIFC Restricted Transfer hereby enter into the DIFC Standard Data Protection Contractual Clauses which are deemed completed as follows:

(a) Appendix 1 shall be populated with the details of the relevant parties and details of transfer set out in Annex I to the Restricted Transfer Provisions;

(b) Appendix 2 shall be populated with details set out in Annex II to the Restricted Transfer Provisions; and

(c) Appendix 3 shall not apply.

PART B: Terms and Conditions of the Processing of Personal Data Subject to Guernsey Data Protection Law

Bailiwick of Guernsey Addendum to the European Commission Standard Contractual Clauses (The "Clauses")

1. DATE OF THIS ADDENDUM

This Addendum is effective from as of the Effective Date.

2. PURPOSE OF THIS ADDENDUM

The Data Protection Authority in the Bailiwick of Guernsey considers this Addendum (together with the Clauses) provides appropriate safeguards for the purposes of transfers of Personal Data to a third country or an international organisation in reliance on Section 56(2)(c) of The Data Protection (Bailiwick of Guernsey) Law, 2017 ("**the Law**") and, with respect to data transfers from controllers to controllers, controllers to processors, processors to controllers and/or processors to processors.

3. INTERPRETATION OF THIS ADDENDUM

3.1 Where this Addendum uses terms that are defined in the Annex those terms shall have the same meaning as in the Annex. In addition, the following terms have the following meanings:

"**Annex**" means the Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021;

"**Data Protection Law**" means all laws relating to data protection, the processing of Personal Data, privacy and/or electronic communications in force from time to time in Guernsey, including the Law and the European Communities (Implementation of Privacy Directive) (Guernsey) Ordinance 2004 (each as amended); and

"**Courts of the Bailiwick of Guernsey**" means as defined in section 81 of the Law that encompasses 'the Royal Court', 'the Court of Alderney' and 'the Court of the Seneschal'

3.2 This Addendum shall be read and interpreted in the light of the provisions of the Data Protection Law, and so that it fulfils the intention for it to provide the appropriate safeguards as required by Section 56 of the Law.

3.3 This Addendum shall not be interpreted in a way that conflicts with rights and obligations provided for in the Data Protection Law.

3.4 Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

4. HIERARCHY

4.1 In the event of a conflict or inconsistency between this Addendum and the provisions of the Clauses or other related agreements between the Parties, existing at the time this Addendum is agreed or entered into thereafter, the provisions which provide the most protection to Data Subjects shall prevail.

5. INCORPORATION OF THE CLAUSES

5.1 This Addendum incorporates the Clauses which are deemed to be amended to the extent necessary so they operate:

5.1.1 for transfers made by the data exporter to the data importer, to the extent that the Data Protection Law applies to the data exporter's processing when making that transfer; and

5.1.2 to provide appropriate safeguards for the transfers in accordance with Section 56 of the Law.

5.2 The amendments required by Section 5.1 above, include (without limitation):

5.2.1 References to the "Clauses" means this Addendum as it incorporates the Clauses;

5.2.2 Clause 6 Description of the transfer(s) is replaced with:

"The details of the transfers(s) and in particular the categories of Personal Data that are transferred and the purpose(s) for which they are transferred are those specified in Annex I.B where the Data Protection Law applies to the data exporter's processing when making that transfer."

5.2.3 References to "Regulation (EU) 2016/679" or "that Regulation" are replaced by the "Data Protection Law" and references to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent provisions of the Law. In particular:

(a) The references in Clause 2(a) of the Clauses to Article 46(1) and 46(2) of Regulation (EU) 2016/679 shall be deemed to refer to Sections 56(1) and 56(2) of the Law.

(b) The reference in Clause 2(a) of the Clauses to Article 28(7) of Regulation (EU) 2016/679 shall be deemed to refer to Section 56(2)(c) of the Law; and

(c) The reference in Clause 13 of the Clauses to Article 23(1) of Regulation (EU) 2016/679 shall continue to refer to that provision of Regulation (EU) 2016/679.

5.2.4 References to Regulation (EU) 2018/1725 are removed save as set out above.

5.2.5 References to the "Union", "EU" and "EU Member State" are all replaced with "the Bailiwick of Guernsey."

5.2.6 Clause 13(a) and Part C of Annex I are not used; the "competent supervisory authority" is the Data Protection Authority in the Bailiwick of Guernsey;

5.2.7 Clause 17 is replaced to state "These Clauses are governed by the law of the Island of Guernsey".

5.2.8 Clause 18 is replaced to state:

"Any dispute arising from these Clauses shall be resolved by the courts of the Bailiwick of Guernsey. A Data Subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Bailiwick of Guernsey. The Parties agree to submit themselves to the jurisdiction of such courts."

5.2.9 The footnotes to the Clauses do not form part of the Addendum.

6. DATA SUBJECT RIGHTS

The Parties to this Addendum intend that any Data Subject whose Personal Data is to be transferred under the Clauses may act to enforce the terms of the Clauses and this Addendum directly against the Parties to the extent set out in the Clauses and such Data Subject shall be entitled to any remedy in respect of any such right as if they were a direct party to the Clauses. By signing this Addendum, each Party undertakes to each such Data Subject to comply with the terms of the Clauses which give direct rights to Data Subjects.

7. AMENDMENTS TO THIS ADDENDUM

The Parties may amend this Addendum provided it maintains the appropriate safeguards required by Section 56 of the Law for the relevant transfer by incorporating the Clauses and making changes to them in accordance with Section 5 above.

8. EXECUTING THIS ADDENDUM

The Parties agree to be bound by the terms and conditions set out in this Addendum.

PART C: Terms and Conditions of the Processing of Personal Data Subject to Jersey Data Protection Law

Standard Data Protection Clauses issued by the Jersey Data Protection Authority pursuant to Art.67(2)(c) of the Data Protection (Jersey) Law 2018

Bailiwick of Jersey Addendum to the EU Standard Contractual Clauses

1. PURPOSE OF THIS ADDENDUM

The Jersey Data Protection Authority considers this Addendum provides appropriate safeguards for the purposes of transfers of Personal Data to a third country or an international organization in reliance on Art.67(2)(c) of Data Protection (Jersey) Law 2018 ("**DPJL 2018**") and with respect to data transfers from controllers to controllers, controllers to processors, processors to controllers, and/or processors to processors, when it is entered into as a legally binding contract.

2. PARTIES

START DATE: Effective Date

THE PARTIES:EXPORTER (WHO SENDS THE PERSONAL DATA); IMPORTER (WHO RECEIVES THE PERSONAL DATA)

Name of Exporter: See Annex I to the Restricted Transfer Provisions

Address of Exporter: See Annex I to the Restricted Transfer Provisions

Name of Importer: See Annex I to the Restricted Transfer Provisions

Address of Exporter: See Annex I to the Restricted Transfer Provisions

KEY CONTACT:

Name: See Annex I to the Restricted Transfer Provisions

Contact details (including email): GlobalPrivacyOffice@ajg.com

SIGNATURES:

See signature page of the Addendum

Date: Effective Date

3. INTERPRETATION

3.1 Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in those Approved EU SCCs. In addition, the following terms have the following meanings:

"**Appropriate Safeguards**" means the standard of protection over the Personal Data and Data Subjects' rights, which is required by the DPJL 2018 when making a transfer relying on standard data protection clauses under Art.67(2)(c) of the DPJL 2018;

"**Approved EU SCCS**" means the Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council; and

"**Data Protection Law**" means all laws relating to data protection, the processing of Personal Data, privacy and/or electronic communications in force from time to time in Jersey.

3.2 This Addendum must always be interpreted in a manner that is consistent with the DPJL 2018 and so that it fulfils the Parties' obligation to provide Appropriate Safeguards.

3.3 If there is any inconsistency or conflict between the DPJL 2018 and this Addendum, the terms of the DPJL 2018 apply.

3.4 Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

4. HIERARCHY

4.1 Notwithstanding the fact that Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties to this Addendum agree that for transfers falling within scope of Art.67(2)(c) of the DPJL 2018, the hierarchy set out in 4.2 below will prevail.

4.2 In the event of a conflict or inconsistency between this Addendum and the provisions of the Approved EU SCCs or other related agreements between the Parties, existing at the time this Addendum is agreed or entered into thereafter, the provisions of this Addendum override the Approved EU SCCs or other related agreements except where (and in so far as) the inconsistent or conflict terms of the Approved EU SCCs provide the greater protection to Data Subjects, in which case those terms will override the Addendum.

5. INCORPORATION OF AND CHANGES TO THE EU SCCs

5.1 This Addendum incorporates the Approved EU SCCs which are deemed to be amended to the extent necessary so they operate:

5.1.1 for transfers made by the data exporter to the data importer, to the extent that the DPJL 2018 applies to the data exporter's processing when making that transfer; and

5.1.2 to provide appropriate safeguards for the transfers in accordance with Art. 66 of the DPJL 2018.

5.2 The amendments required by Section 5.1 above, include (without limitation):

5.2.1 References to the "Clauses" means this Addendum as it incorporates the Approved EU SCCs;

5.2.2 Clause 6 (Description of the transfer(s)) is replaced with:

"The details of the transfers(s) and in particular the categories of Personal Data that are transferred and the purpose(s) for which they are transferred are those specified in Annex I.B where the DPJL 2018 applies to the data exporter's processing when making that transfer.";

5.2.3 References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are replaced by the "DPJL 2018". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent provisions of the DPJL 2018;

5.2.4 References to Regulation (EU) 2018/1725 are removed;

5.2.5 References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with "the Bailiwick of Jersey";

5.2.6 The reference in Clause 10(a) to "one month" is replaced with "four weeks";

5.2.7 Clause 13(a) and Part C of Annex I are not used;

5.2.8 The "competent supervisory authority" and "supervisory authority" are both replaced with the "Data Protection Authority";

5.2.9 Clause 16(e), subsection (i) is replaced with:

"Regulations are made pursuant to Article 66(3)(b) of the DPJL 2018 that make further provision about international transfers of data".

5.2.10 Clause 17 is replaced with:

"These Clauses are governed by the law of Jersey".

5.2.11 Clause 18 is replaced with:

"Any dispute arising from these Clauses shall be resolved by the courts of the Bailiwick of Jersey. A Data Subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Bailiwick of Jersey. The Parties agree to submit themselves to the jurisdiction of such courts."

5.2.12 The footnotes to the Clauses do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

5.2.13 The reference in footnote 10 to "two more months" is replaced with "eight further weeks".

6. DATA SUBJECT RIGHTS

The Parties to this Addendum intend that any Data Subject whose Personal Data is transferred under the Clauses may act to enforce the terms of the Clauses and this Addendum directly against the Parties to the extent set out in the Clauses and such Data Subject shall be entitled to any remedy in respect of any such right as if they were a direct party to the Clauses. By signing this Addendum, each Party undertakes to each such Data Subject to comply with the terms of the Clauses which give direct rights to Data Subjects.

7. AMENDMENTS TO THIS ADDENDUM

The Parties may amend this Addendum provided it maintains the appropriate safeguards required by Article 66 of the DPJL 2018 for the relevant transfer by incorporating the Clauses and making changes to them in accordance with Section 5 above.

8. EXECUTING THIS ADDENDUM

The Parties agree to be bound by the terms and conditions set out in this Addendum.

PART D: Terms and Conditions of the Processing of Personal Data Subject to Philippine Data Protection Law

1 Definitions

The following definitions shall supplement or replace (as applicable) the definitions section of this Addendum for the purposes of this Part D only.

"Commission" means the Philippine National Privacy Commission.

"DPO" means Data Privacy Officer.

"Philippine Data Protection Law" means the Data Privacy Act of 2012 (Republic Act No. 10173), as may be amended from time to time.

"Security Breach" means any unauthorized, unlawful or accidental access, processing, disclosure, alteration, loss, damage, or destruction of Personal Data whether by human or natural causes.

"Sensitive Data" means Personal Data: (i) about a Data Subject's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations; (ii) about a Data Subject's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such individual, the disposal of such proceedings, or the sentence of any court in such proceedings; (iii) issued by government agencies peculiar to an individual which includes, but is not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and (iv) specifically established by an executive order or an act of Philippine Congress to be kept classified.

2 Disclosure

In relation to the Personal Data provided by it to the Data Recipient, the Data Discloser shall provide the Data Subject with the following information prior to collection or before data is shared:

2.1 identity of the Controllers that will be given access to the Personal Data;

2.2 purpose of data sharing;

2.3 categories of Personal Data concerned;

2.4 intended recipients or categories of recipients of the Personal Data;

2.5 existence of the rights of Data Subjects, including the right to access and correction, and the right to object; and

2.6 other information that would sufficiently notify the Data Subject of the nature and extent of data sharing and the manner of processing.

3 Lawful Basis

3.1 The lawful basis for the processing of the Personal Data (Data Discloser sharing Personal Data with Data Recipient) may be (a) consent of the Data Subject; (b) necessary processing related to the fulfilment of a contract with the Data Subject or in order to take steps at the request of the Data Subject prior to entering into a contract; (c) compliance with a legal obligation to which the Data Discloser is subject; (d) necessary processing to protect vitally important interests of the Data Subject; (e) necessary processing to respond to national emergency or to comply with the requirements of public order and safety, as prescribed by law; (f) necessary processing for the fulfilment of the constitutional or statutory mandate of a public authority; or (g) necessary processing to pursue the legitimate interests of the Data Discloser, or by a third party or parties to whom the data is disclosed.

3.2 The lawful basis for the processing of Sensitive Data may be (a) consent of the Data Subject; (b) as provided for by existing laws and regulations; (c) necessary processing to protect the life and health of the Data Subject or another person, and the Data Subject is not legally or physically able to express his or her consent prior to the processing; (d) necessary processing for the purpose of medical treatment: provided, that it is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of Personal Data is ensured; or

(e) necessary processing for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise, or defense of legal claims, or when provided to government or public authority pursuant to a constitutional or statutory mandate.

4 Details of the Transfer

Sub-contracting to a third-party processor is permitted provided that any such sub-contracting is in accordance with the Agreement or this Addendum.

5 Term

The term or duration of the data sharing arrangement shall be for the term of the Agreement.

6 Implementation of the Data Transfer

The operational details for data sharing will be agreed between the parties in connection with the Agreement.

7 Data Subject Access Rights

7.1 Data Subjects have a right to exercise their rights, as provided for by applicable Philippine Data Protection Law. Data Subjects may likewise access or obtain a copy of the Agreement, subject to the right of the parties to the Agreement to redact or prevent the disclosure of trade or industrial secrets, confidential and proprietary business information, and any other detail or information that could endanger or compromise their information systems, or expose to harm the confidentiality, integrity, or availability of Personal Data under their control or custody.

7.2 Each party has an obligation to respond to these request or complaints, however request made to the receiving party should be honoured by them. Inquiry or request of Personal Data can be requested by submitting a written request in accordance with each party's privacy policy, published on its website.

7.3 The DPO will be the first port of call for questions about the Addendum, any complaint filed by the Data Subject and/or any investigation by the Commission. If there is a problem such as a potential Security Breach, the relevant DPO must be contacted.

7.4 Each party shall rectify the complaint by any Data Subject within thirty (30) days from receipt of any such complaint, if required by Philippine Data Protection Law. The Data Subject shall be given a response in writing describing how the complaint was rectified and how the situation complained of will be avoided moving forward.

8 Retention of Personal Data

8.1 Personal Data will be retained for the duration of the Agreement or any subsequent renewal thereof and until such time retention is no longer permitted by Philippine Data Protection Law (to the extent applicable).

8.2 If a complaint is received about the accuracy of Personal Data which affects Personal Data shared with the other party, an updated replacement Personal Data will be processed by the party.

9 Return or Destruction of Personal Data

9.1 Upon termination of the Agreement, the Data Recipient shall perform the following within thirty (30) days from date of the written request from the Data Discloser (provided that retention is not permitted by Philippine Data Protection Law):

(a) destroy and/or return all copies it made of Personal Data; and

(b) deliver to the Data Discloser a certificate confirming the Data Recipient’s compliance with the return or destruction obligation under this section, if requested by the Data Discloser.

PART E: Terms and Conditions of the Processing of Personal Data Subject to Singapore Data Protection Law

The EU Standard Contractual Clauses, adapted and supplemented as described in this Addendum, will apply to a transfer of Personal Data from Singapore to any country or recipient outside of Singapore. For these purposes, the following

provisions shall amend, replace and supplement the corresponding provisions in the definitions section of this Addendum and the EU Standard Controller to Controller Clauses.

1 Definitions

The following definitions shall supplement or replace (as applicable) the definitions section of this Addendum for the purposes of this Part E only.

"**Data exporter**" means the organization who transfers the Personal Data;

"**Data importer**" means the organization who agrees to receive from the data exporter Personal Data for further processing, use and/or disclosure in accordance with these clauses;

"**Data intermediary**", "**individual**", "**organization**", "**personal data**" and "**processing**" shall have the same meaning as under the Singapore Personal Data Protection Act (2012) ("**PDPA**");

"**PDPA**" means the Personal Data Protection Act 2012 of Singapore, as may be amended from time to time;

"**Regulatory or supervisory authority**" means the Personal Data Protection Commission (PDPC) or such other regulatory authority as may be designated by the Singapore Government under the PDPA from time to time for the enforcement and administration of the PDPA;

"**Sensitive data**" is a type of Personal Data and all references to sensitive data with respect to Personal Data transferred under these terms and conditions should be regarded as having the same meaning as Personal Data under the PDPA;

"**The processor**" means any data intermediary engaged by the data importer or by any other data intermediary of the data importer who agrees to receive from the data importer or from any other data intermediary of the data importer Personal Data exclusively intended for processing activities to be carried out on behalf of the data importer in accordance with its instructions, these terms and conditions and the terms of the written subcontract.

2 Obligations of the Data Importer

Clause 8 and Clause 10 of the EU Standard Controller to Controller Clauses shall be deleted and replaced with the following:

2.1 Compliance with PDPA

The data importer shall comply with all its obligations under the PDPA at its own cost.

2.2 Process, Use and Disclosure

The data importer shall only process, use or disclose the Personal Data:

(a) strictly for the purposes agreed between the Parties;

(b) with the data exporter's prior written consent; or

(c) when required by law or an order of court, but shall notify the data exporter as soon as practicable before complying with such law or order of court at its own cost.

2.3 Transfer of Personal Data outside Singapore

The data importer shall not transfer the Personal Data to a place outside Singapore without the data exporter's prior written consent subject to and conditional upon the data importer complying with these terms and conditions, and the data importer hereby confirms that the Personal Data transferred outside Singapore will be protected at a standard that is comparable to that under the PDPA. If the data importer transfers Personal Data to any third party overseas, the data importer shall enter into an agreement with such third party on substantially the same terms as these terms and conditions.

2.4 Security Measures

(a) The data importer shall protect the Personal Data in the data importer's control or possession by making reasonable security arrangements (including, where appropriate, physical, administrative, procedural and information & communications technology measures) to prevent (a) unauthorized or accidental access, collection, use, disclosure, copying, modification, disposal or destruction of the Personal Data, or other similar risks; and (b) the loss of any storage medium or device on which Personal Data is stored.

(b) If required by the data exporter, the data importer shall only permit such authorized personnel as have been agreed with the data exporter in writing to access the Personal Data on a need to know basis.

2.5 Access to Personal Data

The data importer shall provide the data exporter with access to the Personal Data that the data importer has in its possession or control, as soon as practicable upon the data exporter's written request. In addition, data importer will provide information about the ways the Personal Data has been or may have been used or disclosed by the data importer in the past 12 months, on the request of the data exporter.

2.6 Accuracy and Correction of Personal Data

Where the data exporter provides the Personal Data to the data importer, the data exporter shall make reasonable effort to ensure that the Personal Data is accurate and complete before providing the same to the data importer. The data importer shall put in place adequate measures to ensure that the Personal Data in its possession or control remains or is otherwise accurate and complete. In any case, the data importer shall take steps to correct any errors in the Personal Data, as soon as practicable upon the data exporter's written request.

2.7 Retention of Personal Data

(a) The data importer shall not retain the Personal Data (or any documents or records containing the Personal Data, electronic or otherwise) for any period of time longer than is necessary to serve the purposes agreed between the parties.

(b) The data importer shall, upon the request of the data exporter:

(i) return to the data exporter, all Personal Data; or

(ii) delete all Personal Data in its possession or under its control,

and, after returning or deleting all of the Personal Data, provide the data exporter with written confirmation that it no longer possesses any of the Personal Data. Where applicable, the data importer shall also instruct all third parties to whom it has disclosed the Personal Data for the purposes agreed between the parties to return to the data importer or delete, such Personal Data.

2.8 Others

(a) The data importer will collect, process, use and/or disclose the Personal Data in accordance with the obligations set out in the PDPA and will not make any onward transfer of the Personal Data in violation of the PDPA.

(b) The data importer has the legal authority to give the warranties and fulfil the undertakings set out in these terms and conditions.

(c) The data importer has no reason to believe that the legislation applicable to it prevents it from fulfilling its obligations under these terms and conditions and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided herein, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and the parties shall work together in good faith to agree any steps which have to be taken to allow the data importer to continue to provide such compliance.

(d) The data importer shall cause its officers, employees, volunteers, agents and processors:

(i) who have an access level which would enable them to obtain access to any transferred Personal Data, or

(ii) to whom the data importer otherwise discloses the Personal Data, to be aware of, and undertake to observe, the obligations referred to in this clause.

(e) The data importer shall support the data exporter in any request to discharge their obligations under the PDPA, in a timely manner, that may include (without limitation) providing access to, changing, editing or amending, and/or ceasing to use or retain, any Personal Data belonging to an individual at the request of the data exporter.

(f) The data importer agrees and warrants that:

(i) it has in place reasonable procedures designed to ensure that (1) any third party it authorizes to have access to the Personal Data, including processors, will respect and maintain the confidentiality and secrecy of the Personal Data, and (2) any person acting under the authority of the data importer, including a processor, shall be obligated to process the Personal Data only on instructions from the data importer. This provision does not apply to persons authorized or required by law or regulation to have access to the Personal Data;

(ii) upon reasonable request of the data exporter or the regulatory or supervisory authority within the country of the data exporter, it will submit its data processing facilities for audit of the processing activities covered by these terms and conditions by the data exporter or the regulatory or supervisory authority within the country of 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 consent or approval the data importer will attempt to obtain in a timely fashion; and

(iii) it shall deal with promptly and properly all reasonable inquiries from the data exporter relating to the fulfilment of its obligations hereunder and the data importer shall abide by the reasonable instructions or advice (if any) of the data importer or any supervisory authority in this regard.

(g) The data importer shall at all times have in place accessible documents which clearly specify its policies and practices in relation to Personal Data, and shall identify to the data exporter its data protection officer authorized to respond to enquiries concerning the processing, using and/or disclosing Personal Data.

(h) The data importer shall ensure that all such measures and standards in relation to Personal Data are regularly updated to reflect any new or generally accepted data protection standards.

3 Indemnity

Clause 12 of EU Standard Controller to Controller Clauses shall be deleted and replaced with the following:

The data importer shall indemnify the data exporter and its officers, employees and agents, against all actions, claims, demands, losses, damages, statutory penalties, expenses and cost (including legal costs on a full indemnity basis), in respect of:

(a) the data importer's breach of Clause 8 of EU Standard Controller to Controller Clauses; or

(b) any act, omission or negligence of the data importer or its subcontractor that causes or results in the data exporter being in breach of any of Singapore data protection laws.

4 Law applicable to the clauses

These clauses shall be governed by the law of Singapore.

Clauses 3, 13 to 15, 17, and 18 of the EU Standard Controller to Controller Clauses shall be deleted.

Clause 16(e) shall be deleted and replaced with the following:

(e) The parties agree that the termination of these clauses at any time, in any circumstances and for whatever reason does not exempt them from the obligations and/or conditions under the clauses as regards the processing of the Personal Data transferred.

PART F: Terms and Conditions of the Processing of Personal Data Subject to Swiss Data Protection Law

The following provisions shall amend, replace and supplement the corresponding provisions in the definitions section of this Addendum and the EU Standard Controller to Controller Clauses.

1 Definitions

The following definitions shall supplement or replace (as applicable) the definitions section of this Addendum for the purposes of Part F only.

"FADP" means the Swiss Federal Act on Data Protection

2 International Transfers

2.1 For Restricted Transfers of Personal Data that are subject to the FADP, the EU Standard Controller to Controller Clauses shall apply, but with the following changes to the extent required by the FADP:

(a) References to the GDPR in the EU Standard Controller to Controller Clauses are to be understood as references to the FADP insofar as the data transfers are subject to the FADP; and

(b) The term "member state" in the EU Standard Controller to Controller Clauses shall not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the EU Standard Controller to Controller Clauses. Accordingly, Data Subjects with their place of habitual residence in Switzerland may also bring legal proceedings before the competent courts in Switzerland.

2.2 Under Annex I(C) of the EU Standard Controller to Controller Clauses (Competent supervisory authority):

(a) Where the Restricted Transfer is subject exclusively to the FADP and not the GDPR, the supervisory authority is the Swiss Federal Data Protection and Information Commissioner; and

(b) Where the Restricted Transfer is subject to both the FADP and the GDPR, the supervisory authority is the Swiss Federal Data Protection and Information Commissioner insofar as the transfer is governed by the FADP, and the supervisory authority is as set forth in Clause 2c of the Restricted Transfer Provisions insofar as the transfer is governed by the GDPR.