Issue Date: 25 May 2018
Revision Date: As of 27 December 2022
Revision No: 2

THIS VENDOR FRAMEWORK is made as of 25 May 2018 ("this Agreement")

BETWEEN:

(1) OOCL **(Data Processor/Data Controller)**; and

(2) Vendor/ Service Provider **(Data Sub-Processor/Data Controller/Data Processor)**

(each a "**Party**" and together, the "**Parties**")

WHEREAS:

A. The Merchant Data Controller (as defined below) has authorised OOCL, as carrier (i) to process any Personal Data provided to OOCL or which is made available to OOCL for the purposes of the contract of carriage between the Merchant Data Controller and OOCL and for other purposes agreed under the Framework; and (ii) to engage the Vendor as a sub-processor of such Personal Data exclusively on the Merchant Data Controller's behalf for the same purposes and subject to the same obligations imposed on OOCL (if applicable).

B. OOCL appointed the Vendor pursuant to the Contract (as defined below) to provide Services (as defined below) to OOCL and/or Merchant Data Controller (as the case may be).

C. The Parties agree to supplement and amend the terms of the Contract to address their mutual rights, duties and obligations arising as a result of the implementation of the Regulation (as defined below) and the Applicable Data Protection Laws (as defined below), to the extent applicable.

It is hereby agreed as follows:

1 DEFINITIONS AND INTERPRETATION

1.1 Unless otherwise stated, this Agreement adopts the same definitions and interpretation in the Framework. The capitalised terms in this Agreement shall have the meanings set out in **Schedule 1**.

1.2 References to this Agreement includes the Schedules. If there is any inconsistency between the Clauses and the Schedules to this Agreement, the Clauses shall take precedence.

2 AMENDMENT TO THE CONTRACT

2.1 This Agreement amends the Contract in accordance with the provisions thereof. All existing provisions of the Contract shall continue in full force and effect save as amended by this Agreement. The Contract and this Agreement shall be read and construed together and shall be deemed to constitute one and the same instrument.

3 APPLICABILITY OF DATA PROTECTION PROVISIONS

3.1 For the avoidance of doubt:

(1) Clauses 4 shall apply to Personal Data of the Merchant Data Controller provided by OOCL to the Vendor for sub-processing pursuant to this Vendor Framework and the Contract;

(2) Clause 5 shall apply to Vendor's Personal Data provided by the Vendor to OOCL for processing pursuant to the Contract; and

(3) Clause 6 shall apply to OOCL's Personal Data provided by OOCL to the Vendor for processing pursuant to the Contract.

4 PROVISIONS APPLICABLE TO PERSONAL DATA OF MERCHANT DATA CONTROLLER

4.1 For Merchant Data Controller Personal Data, the Contract shall be amended and supplemented by Clauses 4.2 to 4.10 as and from the Effective Date. To the extent relevant, applicable and/or necessary, this Agreement shall be deemed a data protection addendum between the Parties.

4.2 The Parties agree to comply with the Regulation and any Applicable Data Protection Laws.

4.3 OOCL shall be the "Processor" and the Vendor shall be a "Sub-Processor" in respect of the Personal Data provided by the Merchant Data Controller to OOCL pursuant to the Framework.

4.4 In processing the Personal Data by the Vendor under the Contract of the Merchant Data Controller, the Vendor shall be bound by the same obligations as are imposed on OOCL under the Framework.

4.5 The Vendor represents and warrants that it has or shall (as the case may be) implement appropriate technical and organizational measures to ensure security of the Personal Data in compliance with the Regulation and Applicable Data Protection Laws.

4.6 The Vendor is permitted and instructed by OOCL to:

(a) Process all Personal Data of the Merchant Data Controller in compliance with instructions, either given directly by the Merchant Data Controller or through OOCL, in order to provide the Services under the Contract, including but not limited to transferring Personal Data of the Merchant Data Controller to competent bodies, courts or regulatory authorities in order to provide the Services, comply with Applicable Data Protection Laws or comply with requests from such bodies, courts or authorities;

(b) disclose or transfer the Personal Data of the Merchant Data Controller to its Affiliates, and any of its employees, agents, delegates, Sub-Processors, or competent authorities (including customs and tax authorities) and bodies in order to provide the Services or services ancillary thereto;

(c) Process the Personal Data of the Merchant Data Controller to carry out actions or investigations that the Vendor considers appropriate to meet its obligations arising from applicable laws relating to fraud prevention, sanction, money laundering, terrorist, bribery, corruption, and the provision of other services to persons who may be subject to economic or trade sanctions (including disclosure to any subsequent sub-processors);

(d) report regulatory related information to competent bodies or authorities in order to comply with its legal and regulatory obligations;

(e) retain the Personal Data of the Merchant Data Controller for so long as it is required to provide the Services, perform investigations in relation to such, or otherwise required by Applicable Data Protection Law and/or justified under the relevant statutory limitation periods (as applicable), whichever is the later; and

(f) Process, retrieve or track the Personal Data of the Merchant Data Controller for the purpose of updating OOCL's records for fees and billing by the Vendor and/or its Affiliates.

4.7 Unless otherwise prevented by Applicable Data Protection Laws, the Vendor agrees that it will

(a) Process the Personal Data of the Merchant Data Controller in compliance with the instructions given through OOCL and this Agreement. If it is required by any applicable laws to process or disclose Personal Data of the Merchant Data Controller for purposes other than those agreed, it shall promptly inform OOCL of that legal requirement before processing the Personal Data of the Merchant Data Controller;

(b) as soon as practicable inform OOCL if an instruction given to it breaches the Regulation, Applicable Data Protection Law and/or any applicable laws;

(c) take appropriate technical and organisational measures against unauthorised or unlawful processing, accidental loss or destruction of, or damage to, the Personal Data of the Merchant Data Controller, and ensure that all persons who have access to process Personal Data of the Merchant Data Controller have committed themselves to appropriate obligations of confidentiality;

(d) provide reasonable assistance to the Merchant Data Controller and/or OOCL to enable it to comply with (i) the rights of Data Subjects; (ii) the security requirements; and (iii) any privacy assessment procedure or consultation, as required under the Regulation and/or Applicable Data Protection Law;

(e) inform OOCL without delay of (i) any request for the disclosure of the Personal Data of the Merchant Data Controller by a law enforcement authority; (ii) any incident which gives rise to a risk of unauthorised access, disclosure, loss, destruction, misuse or alternation of Personal Data of the Merchant Data Controller; (iii) any notice, inquiry or investigation by a Supervisory Authority; and (iv) any complaint or request (in particular, requests for access to, rectification or blocking, erasure and destruction of Personal Data of the Merchant Data Controller) received directly from the Data Subjects;

(f) notify OOCL as soon as it becomes aware of a Reportable Breach and will provide the Merchant Data Controller and/or OOCL with reasonable assistance in responding to and mitigating it. Where the Vendor, sub-processor or subsequent sub-processors fail to fulfill their obligations in accordance with the Regulation or Applicable Data Protection Laws, the Merchant Data Controller and/or OOCL is entitled to suspend the transfer of Personal Data of the Merchant Data Controller and/or terminate the Framework (which shall in turn terminate this Agreement); and

(g) upon termination of the Contract, the Personal Data of the Merchant Data Controller shall, at the Merchant Data Controller/OOCL's option, be destroyed or returned to OOCL, and the Vendor agrees to certify to OOCL that it has done so upon request.

4.8 OOCL for itself and on behalf of the Merchant Data Controller acknowledges and agrees that the Vendor shall be permitted to perform any or all of its Personal Data of the Merchant Data Controller processing obligations through its Affiliates, subcontractors, or continue to use sub-contractors already engaged by the Vendor, provided that (i) the Vendor shall remain liable to OOCL for such performance of its Personal Data of the Merchant Data Controller processing obligations by any Affiliate or subcontractor; (ii) all Affiliates or subcontractors engaged by the Vendor shall be bound by the terms of an agreement which contain the same or equivalent obligations with respect to Personal Data of the Merchant Data Controller processing as are imposed on the Vendor under this

Agreement; (iii) the Merchant Data Controller remains free to agree if the sub-processor may engage subsequent subprocessors and if these latter may subsequently engage other subsequent sub-processors; and (iv) any sub-processing could be allowed only with the prior information to the OOCL and/or the Merchant Data Controller.

4.9 The Vendor may, if relevant in providing Services to OOCL, transfer the Personal Data of the Merchant Data Controller to a country outside of the European Economic Area ("EEA") in accordance with the Standard Contractual Clauses or other available data transfer solutions under the Regulation and/or Applicable Data Protection Law. The Vendor acknowledges that OOCL for itself and on behalf of the Merchant Data Controller consents to such transfers and agrees to be bound by the Standard Contractual Clauses.

4.9A Where Clause 4.9 is applicable, the Parties agree that the Standard Contractual Clauses shall be deemed incorporated into the Contract and this Vendor Framework as follows:

(a) to the extent that any transfer of Personal Data of the Merchant Data Controller is protected by the Regulation and processed in accordance with Clause 4, the EU SCCs shall apply and be completed as follows:

(i) Module Three will apply;

(ii) For Clause 7 thereof, the optional docking clause will apply;

(iii) For Clause 9(a) thereof, Option 2 will apply, and the time period for prior notice of Sub-Processor change is set out in Clause 7 hereof;

(iv) For Clause 11 thereof, the optional language will not apply;

(v) For Clause 17 thereof, Option 1 will apply, and the EU SCCs will be governed by Irish law;

(vi) For Clause 18(b) thereof, the courts shall be courts of Ireland;

(vii) Annex I thereof shall be deemed completed with the information set out in **Schedule 2** hereof; and

(viii) Annex II thereof shall be deemed completed with the information set out in **Schedule 5** hereof.

(b) to the extent that any transfer of Personal Data of Merchant Data Controller is protected by the UK Data Protection Law and processed in accordance with Clause 4, the UK SCCs shall apply and be completed as follows (for the purpose of this sub-paragraph (b), the definitions and references of the UK SCCs are adopted unless otherwise specified):

(i) For Table 1 of Part 1, where Clause 4 hereof is applicable, OOCL shall be the "Exporter" and Vendor shall be the "Importer";

(ii) For Table 2 and Table 3 of Part 1, the EU SCCs as modified pursuant to Clause 4.9A(a) above will apply mutatis mutandis;

(iii) For Table 4 of Part 1, the Importer may end the Addendum as set out in Section 19 of those Mandatory Clause; and

(iv) For Part 2, Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

4.10 The Vendor shall indemnify and hold OOCL and the Merchant Data Controller harmless against any claim brought by a Data Subject and/or any competent authority or body arising out of the Vendor's breach of its obligations in respect of the Personal Data of the Merchant Data Controller under this Agreement and Framework or failure to comply with the Regulation and/or any Applicable Data Protection laws.

5 PROVISIONS APPLICABLE TO PERSONAL DATA OF THE VENDOR

5.1 For Vendor's Personal Data (as defined below), the Contract shall be amended and supplemented by Clauses 5.2 to 5.10 as and from the Effective Date. To the extent relevant, applicable and/or necessary, this Agreement shall be deemed a data protection addendum between the Parties.

5.2 The Vendor authorises OOCL to process Vendor's Personal Data provided to OOCL or which is made available to it for the purposes of providing Services to OOCL pursuant to the Contract and for any other purposes set out in **Schedule 3**.

5.3 The Vendor shall be the "*Data Controller*" and OOCL shall be a "*Data Processor*" for the purposes of the Regulation and/or the Applicable Data Protection Law. The Data Subjects, Categories of Vendor's Personal Data, Processing Operations and Duration of Processing relevant to the provision of the Services are defined in **Schedule 3**.

5.4 The Vendor represents and warrants that it complies with the Regulation and any Applicable Data Protection Laws regarding the collection, use and all other security measures of the Vendor's Personal Data, in particular:

(a) all of the Vendor's Personal Data that the Vendor provides or makes available to OOCL has been lawfully and validly obtained or processed by the Vendor, and can be lawfully disclosed to OOCL for the provision of Services and any other agreed purposes. The Processing of Vendor's Personal Data will be relevant, fair, lawful and proportionate to the respective uses of the Vendor;

(b) all Data Subjects of Vendor's Personal Data have been informed of the OOCL's Processing of their Personal Data for the agreed purposes and the Vendor can demonstrate a lawful basis for such Processing; and

(c) the Vendor has established a procedure for the exercise of the rights of individuals whose personal data are collected and are in its custody or under its control.

5.5 The Vendor agrees that OOCL is permitted to, and instructs OOCL to:

(a) Process all Vendor's Personal Data that OOCL collects from, or relating to, the Vendor for the Vendor's provision of Services under the Contract, including but not limited to transferring Vendor's Personal Data to competent bodies, courts or regulatory authorities in order to provide the Services, comply with Applicable Data Protection Laws or comply with requests from such bodies, courts or authorities;

(b) disclose or transfer the Vendor's Personal Data to its Affiliates, and any of its employees, agents, delegates, Sub-Processors, or competent authorities (including customs and tax authorities) and bodies for the Vendor's provision of Services or services ancillary thereto;

(c) Process the Vendor's Personal Data to carry out actions or investigations that OOCL considers appropriate to meet its obligations arising from applicable laws relating to fraud prevention, sanction, money laundering, terrorist, bribery, corruption, and the provision of other services to persons who may be subject to economic or trade sanctions (including disclosure to Sub-Processors);

(d) report regulatory related information to competent bodies or authorities in order to comply with its legal and regulatory obligations;

(e) retain the Vendor's Personal Data for so long as it is required to provide the Services or perform investigations in relation to such, or otherwise required by Applicable Data Protection Law and/or justified under the relevant statutory limitation periods (as applicable), whichever is the later; and

(f) Process, retrieve or track the Vendor's Personal Data for the purpose of settlement of fees and future business with the Vendor.

5.6 Unless otherwise prevented by Applicable Data Protection Laws, OOCL agrees that it will

(a) Process the Vendor's Personal Data only on behalf of the Vendor and in compliance with the written instructions of the Vendor and this Agreement. If it is required by any applicable laws to process or disclose the Vendor's Personal Data for purposes other than those agreed, it shall promptly inform the Vendor of that legal requirement before processing the Vendor's Personal Data;

(b) as soon as practicable inform the Vendor if in OOCL's opinion, and without any obligation to perform any legal assessment, an instruction given to it breaches the Regulation, Applicable Data Protection Law and/or any applicable laws;

(c) take appropriate technical and organisational measures against unauthorised or unlawful processing, accidental loss or destruction of, or damage to, the Vendor's Personal Data, and ensure that all persons who have access to process Vendor's Personal Data have committed themselves to appropriate obligations of confidentiality;

(d) provide reasonable assistance to the Vendor to enable it to comply with (i) the rights of Data Subjects; (ii) the security requirements; and (iii) any privacy assessment procedure or consultation, as required under the Regulation and/or Applicable Data Protection Law;

(e) inform the Vendor without delay of (i) any request for the disclosure of the Vendor's Personal Data by a law enforcement authority; (ii) any incident which gives rise to a risk of unauthorised access, disclosure, loss, destruction, misuse or alternation of Vendor's Personal Data; (iii) any notice, inquiry or investigation by a Supervisory Authority; and (iv) any complaint or request (in particular, requests for access to, rectification or blocking, erasure and destruction of Vendor's Personal Data) received directly from the Data Subjects;

(f) notify the Vendor as soon as it becomes aware of a Reportable Breach and will provide the Vendor with reasonable assistance in responding to and mitigating it. Where the Reportable

Breach is connected to OOCL's Processing of the Vendor's Personal Data, the Vendor shall provide OOCL with a copy of the intended notification (if any) to be made by the Vendor to the affected Data Subjects and/or Supervisory Authority for OOCL's prior written approval; and

(g) upon termination of the Contract, the Vendor's Personal Data shall, at the Vendor's option, be destroyed or returned to the Vendor, at the Vendor's costs.

5.7 The Vendor acknowledges and agrees that OOCL shall be permitted to perform any or all of its Vendor's Personal Data processing obligations through its Affiliates, subcontractors, or continue to use sub-contractors engaged by OOCL, provided that (i) OOCL shall remain liable to the Vendor for such performance of its Vendor's Personal Data processing obligations by any Affiliate or subcontractor; and (ii) all Affiliates or subcontractors engaged by OOCL shall be bound by the terms of an agreement which contain the same or equivalent obligations with respect to Vendor's Personal Data processing as are imposed on OOCL under this Agreement.

5.8 The Vendor acknowledges and agrees that OOCL may transfer the Vendor's Personal Data to a country outside of the European Economic Area ("EEA") in accordance with the Standard Contractual Clauses or other available data transfer solutions under the Regulation and/or Applicable Data Protection Law, and Clause 4.9A above and the terms of the Framework and this Agreement will apply mutatis mutandis. The Vendor hereby consents to such transfers and agrees to be bound by such Standard Contractual Clauses. The Vendor represents and warrants to OOCL that disclosure of any transfer contemplated will be made in the Vendor's documentation.

5.9 The Vendor shall remain solely and fully liable for any damage which a Data Subject may suffer as a result of the Processing of their Personal Data which is under the Vendor's control and which does not result from a breach by OOCL of its obligations under this Agreement and the Applicable Data Protection Law.

5.10 The Vendor acknowledges and agrees that OOCL is reliant upon the Vendor as the Data Controller for lawful direction and documented instructions as to the extent to which OOCL is entitled to process any Vendor's Personal Data. The Vendor agrees that OOCL will not be liable and it shall fully and effectively indemnify OOCL for any claim brought by a Data Subject and/or any competent authority or body arising from any action or omission of OOCL, to the extent that such action or omission resulted from the Vendor's instructions given to OOCL.

6 PROVISIONS APPLICABLE TO PERSONAL DATA OF OOCL

6.1 For OOCL's Personal Data (as defined below), the Contract shall be amended and supplemented by Clauses 6.2 to 6.6 as and from the Effective Date. To the extent relevant, applicable and/or necessary, this Agreement shall be deemed a data protection addendum between the Parties.

6.2 OOCL authorises the Vendor to process OOCL's Personal Data provided to the Vendor or which is made available to it for the purposes of the Vendor's provision of Services to OOCL pursuant to the Contract and for any other purposes set out in **Schedule 4**.

6.3 OOCL shall be the "*Data Controller*" and the Vendor shall be a "*Data Processor*" for the purposes of the Regulation and/or the Applicable Data Protection Law. The Data Subjects, Categories of OOCL's Personal Data, Processing Operations and Duration of Processing relevant to the provision of the Services are defined in **Schedule 4**.

6.4 OOCL represents and warrants that it complies with the Regulation and any Applicable Data Protection Laws regarding the collection, use and all other security measures of the OOCL's Personal Data, in particular:

(a) all of OOCL's Personal Data that OOCL provides or makes available to the Vendor has been lawfully and validly obtained or processed by OOCL, and can be lawfully disclosed to the Vendor for the provision of Services and any other agreed purposes. The Processing of such OOCL's Personal Data will be relevant, fair, lawful and proportionate to the respective uses of OOCL;

(b) all Data Subjects have been informed of the Vendor's Processing of their Personal Data for the agreed purposes and OOCL can demonstrate a lawful basis for such Processing; and

(c) OOCL has established a procedure for the exercise of the rights of individuals whose OOCL's Personal Data are collected and are in its custody or under its control.

6.5 OOCL agrees that the Vendor is permitted to, and instructs the Vendor to Process all OOCL's Personal Data that the Vendor collects from, or relating to, the Vendor in order to provide the Services under the Contract.

6.6 Unless otherwise prevented by Applicable Data Protection Laws, the Vendor agrees that it will

(a) Process OOCL's Personal Data only on behalf of the OOCL and in compliance with the written instructions of OOCL and this Agreement. If it is required by any applicable laws to process or disclose OOCL's Personal Data for purposes other than those agreed, it shall promptly inform OOCL of that legal requirement before processing the OOCL's Personal Data;

(b) as soon as practicable inform OOCL if in the Vendor's opinion, and without any obligation to perform any legal assessment, an instruction given to it breaches the Regulation, Applicable Data Protection Law and/or any applicable laws;

(c) take appropriate technical and organisational measures against unauthorised or unlawful processing, accidental loss or destruction of, or damage to, OOCL's Personal Data, and ensure that all persons who have access to process OOCL's Personal Data have committed themselves to appropriate obligations of confidentiality;

(d) provide reasonable assistance to OOCL to enable it to comply with (i) the rights of Data Subjects; (ii) the security requirements; and (iii) any privacy assessment procedure or consultation, as required under the Regulation and/or Applicable Data Protection Law;

(e) inform OOCL without delay of (i) any request for the disclosure of OOCL's Personal Data by a law enforcement authority; (ii) any incident which gives rise to a risk of unauthorised access, disclosure, loss, destruction, misuse or alternation of OOCL's Personal Data; (iii) any notice, inquiry or investigation by a Supervisory Authority; and (iv) any complaint or request (in particular, requests for access to, rectification or blocking, erasure and destruction of OOCL's Personal Data) received directly from the Data Subjects;

(f) notify OOCL as soon as it becomes aware of a Reportable Breach and will provide OOCL with reasonable assistance in responding to and mitigating it. Where the Reportable Breach is connected to the Vendor's Processing of OOCL's Personal Data, OOCL shall provide the Vendor with a copy of the intended notification (if any) to be made by OOCL to the affected Data Subjects and/or Supervisory Authority for the Vendor's prior written approval; and

(g) upon termination of the Contract, OOCL's Personal Data shall, at OOCL's option, be destroyed or returned to OOCL.

6.7 To the extent relevant, applicable and necessary, in the event the Vendor transfers any OOCL's Personal Data to a country outside of the EEA, such transfer shall be in accordance with the Standard Contractual Clauses or other available data transfer solutions under the Regulation and/or Applicable Data Protection Law, and Clauses 4.9A above and the terms of this Agreement will apply mutatis mutandis.

7 SUB-PROCESSOR

7.1 The Parties acknowledges and expressly agrees the Parties may engage new Sub-Processors as described in this Clause 7. Where Clause 5 is applicable, OOCL makes available to the Vendor the current list of Sub-Processors used by OOCL to process Vendor's Personal Data listed at **Schedule 6**, as may be updated from time to time.

7.2 The Parties will provide to each other an up-to-date list of the Sub-Processors it has engaged upon receiving written request from the other Party; and notify the other Party for any new Sub-Processors within 7 days (or such timeframe otherwise mutually agreed) prior to such new Sub-Processor(s) to process the Personal Data of the other Party.

7.3 If a Party has a reasonable basis to object to the other Party's use of new Sub-Processors, such Party shall notify the other Party promptly in writing within 14 days after receiving the new list of Sub-Processors. The Parties will seek a commercially reasonable resolution in good faith and if the Parties are unable to reach a resolution, the objecting Party may terminate the portion of any Contract relating to the Services that cannot be reasonably provided without the use of such new Sub-Processor(s) such Party objects to.

8 INFORMATION AND AUDITS

8.1 Subject to Clauses 8.2 and 8.4, the Parties shall make available to each other upon request all reasonable information necessary to demonstrate its compliance with this Agreement and shall allow for and contribute to audits and inspections conducted by the other Party (or the relevant controller(s)) or another auditor specified by the other Party.

8.2 The Parties shall ensure that all requests for information or to exercise a right of audit or inspection under Clause 8.1 are reasonable and are provided to the other Parties in writing with no fewer than 60 days' notice. Any such audit or inspection shall be strictly limited to auditing the other Party's compliance with this Agreement and shall be undertaken at the requesting Party's sole expense, during working hours and subject to any reasonable conditions the other Party may impose to prevent disruption to the other Party's operations and business. The requesting Party shall ensure that a written report is produced with the findings of any audit or inspection and that a copy of this report is promptly provided to the other Party. Any information obtained or received shall only be used or disclosed to the extent strictly necessary to assess the other Party's compliance with this Agreement and not for any other purpose.

8.3 The Parties shall immediately inform each other if, in its opinion, an instruction from the other Party with regard to Clause 8.1 infringes Applicable Data Protection Laws.

8.4 The Vendor shall reimburse OOCL promptly on demand for any and all reasonable expenses OOCL may incur in connection with any request for information or any audit or inspections under

Clauses 8.1 to 8.3. The indemnity in Clause 4.10 and 5.9 to 5.10 (as the case may be) shall apply in respect of any breach by the Vendor (or the Vendor's personnel or auditors) of the conditions in Clause 8.2.

9. RETURN OR DELETION OF PERSONAL DATA

9.1 Following the termination of the Agreement, OOCL shall either return to Vendor the Personal Data or delete the Vendor's Personal Data, unless such Personal Data is required to be retained under Applicable Data Protection Laws. Some Vendor's Personal Data may remain in system backups until the expiry of those backups.

10 PRECEDENCE

10.1 In the event of any conflict and/or inconsistency between any Data Protection Provisions contained in the Contract (if any) and the data protection provisions contained in this Agreement, the provisions on data protection only in this Agreement shall prevail.

11 COUNTERPARTS

11.1 This Agreement may be executed in any number of counterparts and by the different Parties hereto on separate counterparts each of which when executed and delivered shall constitute an original and all such counterparts together constituting but one and the same instrument.

12 VARIATION

12.1 No provisions of this Agreement may be amended, changed, waived, discharged or terminated except in writing signed by each of the Parties, except that OOCL may, for the purpose of compliance with Applicable Data Protection Law(s), in its sole discretion update, revise and/or amend this Agreement from time to time by updating the link to this Agreement as referenced in the Contract and/or OOCL's websites.

12.2 If any of the provisions of this Agreement is found by an arbitrator, court or other competent authority to be void, illegal or unenforceable, this will not affect the remaining provisions of this Agreement. The Parties shall negotiate in good faith in order to replace this void, illegal or unenforceable provision with such a valid, legal or enforceable provision which the parties would have agreed upon if they have been aware of the void, illegal or unenforceable provision. The same procedure to apply in case of a contractual gap.

13 GOVERNING LAW AND JURISDICTION

13.1 This Agreement (including any non-contractual obligations arising out of or in connection with the same) shall be governed by and construed, and any and all claims, suits, proceedings or disputes howsoever arising in connection with this Agreement or the rights and obligations in the Contract shall be determined in accordance with the laws of England.

13.2 The provisions of this Clause 13 shall continue to apply notwithstanding the termination of this Agreement.

14 INCONSISTENT DATA PROTECTION LAWS

14.1 There may be circumstances in which Applicable Data Protection Laws in different jurisdictions conflict or are inconsistent or incompatible or in which complying with a lawful request from a governmental authority in one jurisdiction may breach Applicable Data Protection Laws in another

jurisdiction, in connection with the processing of Personal Data in the use of Services (inconsistent data protection laws).

14.2 If Vendor becomes aware of any problem of inconsistent data protection laws Vendor shall cease to provide the Services and notify OOCL of the problem. OOCL shall take into consideration the necessity to comply with the Applicable Data Protection Laws to the extent practicable and liaise with relevant supervisory authorities and/or other relevant governmental authorities to identify practical and constructive solution. Nonetheless, to the extent that no practical solution to the problem of inconsistent data protection laws can be found, OOCL may elect to cease to use some or all Services from one or more of the jurisdictions from which the inconsistent data protection laws arise.

15 DATA PROTECTION CONTACT

15.1 OOCL can be contacted in respect of any privacy and data protection matters at:

Corporate Customer Service Department
Orient Overseas Container Line Ltd.
Address: 31st Floor, Harbour Centre,
25 Harbour Road, Wanchai,
Hong Kong
Telephone: (852) 2833 3888
Email: support@oocl.com

SCHEDULE 1

"Contract" means the contract entered into or will be entered into pursuant to which the Vendor provides Services (as defined below) to OOCL, and including all schedules and appendices thereto (as may be amended from time to time);

"contracts of carriage" means the contracts of carriage entered into or will be entered into pursuant to which OOCL provides the Services (as defined below) to the Merchant Data Controller, and including all schedules and appendices thereto (as may be amended from time to time);

"Affiliate" means any subsidiary or holding company of OOCL or the Vendor, as the case may be, and any subsidiary of such holding company and for these purposes the terms "**subsidiary**" and "**holding company**" are defined as follows:

(i) a company is a "**subsidiary**" of another company only if—

(a) it is controlled by—

i. that other company; or

ii. that other company and one or more companies each of which is controlled by that other company; or

iii. two or more companies each of which is controlled by that other company; or

(b) it is a subsidiary of a subsidiary of that other company.

(ii) a company is the "**holding company**" of another only if that other company is its subsidiary.

"Applicable Data Protection Law(s)" means

(i) for the purposes of English law, all applicable national laws, regulations and other legal requirements relating to (a) privacy, data security, consumer protection, marketing, promotion and text messaging, email and other communications; and (b) the use, collection, retention, storage, security, disclosure, transfer, disposal, and other processing of any Personal Information, in which OOCL or its Affiliate is subject to or which are otherwise applicable;

(ii) for the purposes of European Union law, the Data Protection Acts 1988 and 2003 (as amended), the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications Regulations 2011 and the Regulation (as defined below) (as amended or replaced from time to time), and any other EU regulations, directives, guidance, directions, determinations, codes of practice, circulars, orders, notices or demands issued by any Supervisory Authority in which OOCL or its Affiliate is subject to; and

(iii) any applicable national, international, regional, municipal or other data privacy authority or other data protection laws or regulations in any other territory in which OOCL or its Affiliate is subject to or which are otherwise applicable.

"Data Controller" has the meaning assigned to it in the Regulation and/or any Applicable Data Protection Law and as defined in Schedule 2, Schedule 3 and Schedule 4 (as the case may be) and shall collectively refer to:

(i) The Merchant Data Controller who provides the Personal Data to OOCL for processing pursuant to the contract of carriage and the Framework;

(ii) The Vendor who provides the Vendor's Personal Data to OOCL for processing pursuant to the Contract;

(iii) OOCL who provides the OOCL's Personal Data to the Vendor for processing pursuant to the Contract.

For avoidance of doubt, the Merchant Data Controller, the Vendor and OOCL when acting as Data Controller has the same meaning assigned to it as Data Controller under the Regulation and/or any Applicable Date Protection Law.

"Data Processor" has the meaning assigned to it in the Regulation and/or any Applicable Data Protection Law and as defined in Schedule 2, Schedule 3 and Schedule 4 (as the case may be) and shall include:

(i) OOCL who processes Personal Data on behalf of Merchant Data Controller pursuant to the contract of carriage and the Framework; and

(ii) OOCL who processes the Vendor's Personal Data pursuant to the Contract;

(iii) The Vendor who processes OOCL's Personal Data pursuant to the Contract.

"Data Protection Provisions" mean any and all provisions in the Contract relating to the Parties' rights, duties and obligations under any Applicable Data Protection Law;

"Data Subjects" means the identified or identifiable natural person to whom the Personal Data relates and includes the categories of data subjects listed in the **Schedule 2, 3 and 4**;

"Effective Date" means the date on which the Regulation become applicable to the Services;

"Framework" means the agreement concluded between the Merchant Data Controller and OOCL to reflect the rights and obligations in compliance with the Regulation and/or Applicable Data Protection Laws, the terms of which can be found at https://www.oocl.com/eng/resourcecenter/industrylinks/Documents/Framework(A)-Shipper.pdf.

"Merchant Data Controller" means the parties described as Merchant Data Controller in Schedule 2.

"Personal Data"/"Personal Information" has the meaning assigned to it in Applicable Data Protection Laws and includes (i) the categories of Personal Data provided by the Merchant Data Controller to OOCL for the purpose of providing service under the contract of carriage to the Merchant and processed (as defined below) by the Parties under the Contract, as set out in the **Schedule 2**; and (ii) the categories of Vendor's Personal Data provided by Vendor to OOCL for the purpose of providing service under the Contract to OOCL or the Merchant and processed by the Parties under the Contract as set out in **Schedule 3**; and (iii) the categories of OOCL's Personal Data provided by OOCL to the Vendor for the purpose of the Vendor's provision of service under the Contract to OOCL and processed by the Parties under the Contract as set out in **Schedule 4**. For the avoidance of doubt, Personal Data means any information about an identified or identifiable individual who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors

specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual, including Sensitive Personal Data and further includes:

(a) the categories of Personal Data set out in **Schedule 2**, **Schedule 3** or **Schedule 4** (as the case may be); and

(b) Personal Data collected as part of the monitoring and recording of calls and electronic communications by the Vendor.

"Processing (and its derivatives)" means carrying out any operation on Personal Data, including collecting, obtaining, recording, holding, storing, organising, adapting, structuring, altering, retrieving, transferring, consulting, using, disclosing, disseminating or otherwise making available, aligning, combining, restricting, blocking, erasing or destroying it.

"Regulation" means the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of the 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) as and when it becomes applicable to the Services on and from 25 May 2018;

"Reportable Breach" means (i) any breach of security leading to the loss or unlawful destruction or unauthorised disclosure of or access to Personal Information which is likely to adversely affect a Data Subject; and/or (ii) the unauthorised or unlawful Processing, and/or any accidental or unlawful destruction of, loss of, alteration to, or corruption to Personal Data;

"Sensitive Personal Data" means any Personal Data relating to an individual's place of origin, race, colour, national or ethnic origin, sex, sexual orientation, sexual life, marital status, physical or mental disability, physical or mental health, family status, religious beliefs, political opinions, trade union membership, biometric information or genetic information;

"Services" have either (a) the same meaning as the term "Services" set out in the Contract or the contract of carriage (as the case may be), or (b) in the event that the Contract or the contract of carriage (as the case may be) do not contain any such defined term, the services that the Vendor has agreed to perform pursuant to the terms of the Contract, or the services that OOCL has agreed to perform pursuant to the terms of OOCL Bill of Lading or the contracts of carriage (as the case may be);

"Standard Contractual Clauses" means (i) the standard contractual clauses annexed to the European Commission's Implementing Decision 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 pf the European Parliament and of the Council (**"EU SCCs"**); or (ii) the applicable standard data protection clauses issued by the Information Commissioner of the United Kingdom under section 119A(1) of Data Protection Act 2018 as per the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses as of 21 March 2022 (**"UK SCCs"**), as the case may be, and as may be amended or replaced from time to time by a competent authority under the relevant Applicable Data Protection Law(s), to the extent that they relate to an international transfer of Personal Data;

"Sub-Processor" means (i) the Vendor who sub-processes the Personal Data of the Merchant Data Controller pursuant to Clause 4 of this Agreement; or (ii) a third party engaged by the Data Processor or by any Sub-Processor of the Data Processor who is not a Party to this Agreement and who agrees to receive from the Data Processor or from any other Sub-Processor of the Data Processor, Personal Data exclusively for processing activities to be carried out on behalf of the Data Controller;

"Supervisory Authority" means an authority established in accordance with Article 51 of the Regulation or any other equivalent authority established under the Applicable Data Protection Law, the Minister responsible for information and communication technologies policy and innovation or any other authority or official appointed and/or delegated with responsibility for the oversight or enforcement of the Applicable Data Protection Law;

"Vendor's Personal Data" means the personal data provided by Vendor to OOCL for the purpose of providing Services under the Contract to OOCL including the categories of Vendor's Personal Data set out in **Schedule 3**;

"OOCL's Personal Data" means the personal data provided by OOCL to the Vendor for the purpose of the Vendor's provision of Services under the Contract to OOCL including the categories of OOCL's Personal Data set out in **Schedule 4**; and**"UK 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 the United Kingdom including the Data Protection Act 2018 and the Regulation as saved into the law of the United Kingdom by virtue of Section 3 of the United Kingdom's European Union (Withdrawal) Act 2018.

SCHEDULE 2

Merchant Data Controller

The Merchant, including various shippers, consignors, endorsees, transferees, holders of Bills of Lading, consignees, receivers of the goods and any person or entity owning or entitled to the possession of the goods under the Bills of Lading, and anyone acting on behalf of any such persons.

Data exporter (Data Processor)

OOCL is a company engaging in container transport and logistics services, ports and terminals, which processes Personal Data of the Merchant Data Controller upon the instruction of the Merchant Data Controller pursuant to the Framework and engages the services of third parties to carry out data processing activities for the purpose of performing or as agreed under the Framework.

Name: OOCL (as provided in the Contract)

Address: As provided for in the Contract

Contact person's name, position and contact details: As provided for in the Contract

Activities relevant to the data transferred under these Clauses: See Section 4 below

Signature and date: Please refer to the Contract

Data importer (Sub-Processor)

The Vendor has been engaged by OOCL to carry out the Services under the Contract.

Name: Vendor (as provided in the Contract)

Address: As provided for in the Contract

Contact person's name, position and contact details: As provided for in the Contract

Activities relevant to the data transferred under these Clauses: See section "Nature and Purposes of Processing Operations" below

Signature and date: Please refer to the Contract

1. Data Subjects

The personal data transferred concern the following categories of data subjects (*please specify*):

(1) The Merchant;
(2) all employees, representatives, contractors, Affiliates and agents of the Merchant.

2. Categories of data

Depending on the particular data subject, the Personal Data transferred may concern the following categories of data:

(1) Name or user ID
(2) Business Card
(3) Number of identity card, passport or other personal identification documents
(4) Department
(5) Role/Job Title
(6) Contact number
(7) Mail address
(8) Signature
(9) Email (office or private)
(10) Address
(11) Source of Funds
(12) Identity details of instant messaging or social networking applications
(13) Social media profile

3. Special categories of data (if appropriate)

The special categories of data transferred may concern the following:

(1) Sex
(2) Age
(3) Date of Birth
(4) Images of identity cards, passports or other personal identification documents
(5) Bank account number
(6) Nationality
(7) Legal domicile
(8) Place of birth
(9) Photograph
(10) Sanction screening and adverse media searches

Sensitive Personal Data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures as set out in **Schedule 5**.

4. Nature and Purposes of Processing operations

The personal data transferred will be subject to the following basic processing activities and purposes:

(1) The data importer processes personal data as instructed by the date exporter as mandated by the Framework
(2) Performance of contracts of carriage and/or the Contract
(3) Communications
(4) Payment requests and settlement
(5) Conducting Sanction and Anti-Money Laundering checks and other legal/regulatory obligations related to client processing
(6) Software development

(7) Business development
(8) Relationship improvement development
(9) Service improvement and development
(10) System testing and troubleshooting
(11) Insurance and claims
(12) Audit and compliance activities related to the above

The frequency of the transfer: Continuous

5. Duration

The personal data may be processed by the Vendor for the duration during which it is to provide Services pursuant to the Contract or perform investigations in relation to such, unless otherwise required by applicable laws and/or justified under applicable statutory limitation periods, whichever is the later.

6. Competent Supervisory Authority

The competent supervisory authority(ies), in accordance with Clause 13 of the EU SCCs, refers to:

(i) The supervisory authority applicable to the data exporter in its EEA country of establishment;

(ii) Where the data exporter is not established in the EEA, the supervisory authority applicable in the EEA country where the data exporter's EU representative has been appointed pursuant to Article 27(1) of the Regulation;

(iii) Where the data exporter is not obliged to appoint a representative, the supervisory authority applicable to the EEA country where the data subjects relevant to the transfer are located; or

(iv) Where the processing of Personal Data to which UK Data Protection Law applies, the Information Commissioners Office.

SCHEDULE 3

This Schedule describes the categories of Vendor's Personal Data, Data Subjects and the Processing operations to be carried out by OOCL as the Data Processor.

Data exporter(s):

Name: Vendor (as provided in the Contract)

Address: As provided for in the Contract

Contact person's name, position and contact details: As provided for in the Contract

Activities relevant to the data transferred under these Clauses: See Section 4 below

Signature and date: Please refer to the Contract

Role (controller/processor): Data Controller

Data importer(s):

Name: OOCL (as provided in the Contract)

Address: As provided for in the Contract

Contact person's name, position and contact details: As provided for in the Contract

Activities relevant to the data transferred under these Clauses: See Section 4 below

Signature and date: Please refer to the Contract

Role (controller/processor): Data Processor

1. Data Subjects

The Vendor's Personal Data to be Processed by OOCL concerns but are not limited to the following categories of Data Subjects:

(1) the Vendor; and
(2) all employees, representatives, contractors, Affiliates and agents of the Vendor.

2. Categories of Vendor's Personal Data

The Vendor's Personal Data to be Processed by OOCL includes but are not limited to:

(1) Name or user ID
(2) Business Card
(3) Number of identity card, passport or other personal identification documents
(4) Department
(5) Role/Job title

(6) Contact number (home, mobile or fax)
(7) Mail address
(8) Signature
(9) Email (office or private)
(10) Address
(11) Source of Funds
(12) Identity details of instant messaging or social networking applications
(13) Social media profile

3. Categories of Sensitive Vendor's Personal Data

The Categories of Sensitive Vendor's Personal Data are:

(1) Sex
(2) Age
(3) Date of Birth
(4) Images of identity cards, passports or other personal identification documents
(5) Bank account number
(6) Nationality
(7) Legal domicile
(8) Place of birth
(9) Photograph
(10) Sanction screening and adverse media searches

Sensitive Personal Data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures as set out in **Schedule 5**.

4. Nature and Purposes of Processing Operations

The Vendor's Personal Data will be Processed for purposes including, but not limited to:

(1) Performance of the Contract
(2) Payment requests and settlement
(3) Communications
(4) Conducting Sanction, Anti-Money Laundering checks and other legal/regulatory obligations
(5) Future business with the Vendor
(6) Business development
(7) Insurance and Claims
(8) Audit and compliance activities related to the above

The frequency of the transfer: Continuous

5. Duration

Vendor's Personal Data may be processed by OOCL for the duration during which the Vendor is to provide Services pursuant to the Contract or perform investigations in relation to such, unless otherwise required by applicable laws and/or justified under applicable statutory limitation periods, whichever is the later.

6. Competent Supervisory Authority

The competent supervisory authority(ies), in accordance with Clause 13 of the EU SCCs, refers to:

(i) The supervisory authority applicable to the data exporter in its EEA country of establishment;

(ii) Where the data exporter is not established in the EEA, the supervisory authority applicable in the EEA country where the data exporter's EU representative has been appointed pursuant to Article 27(1) of the Regulation;

(iii) Where the data exporter is not obliged to appoint a representative, the supervisory authority applicable to the EEA country where the data subjects relevant to the transfer are located; or

(iv) Where the processing of Personal Data to which UK Data Protection Law applies, the Information Commissioners Office.

SCHEDULE 4

This Schedule describes the categories of OOCL's Personal Data, Data Subjects and the Processing operations to be carried out by Vendor as the Data Processor.

Data exporter(s):

Name: OOCL (as provided in the Contract)

Address: As provided for in the Contract

Contact person's name, position and contact details: As provided for in the Contract

Activities relevant to the data transferred under these Clauses: See Section 4 below

Signature and date: Please refer to the Contract

Role (controller/processor): Data Controller

Data importer(s):

Name: Vendor (as provided in the Contract)

Address: As provided for in the Contract

Contact person's name, position and contact details: As provided for in the Contract

Activities relevant to the data transferred under these Clauses: See Section 4 below

Signature and date: Please refer to the Contract

Role (controller/processor): Data Processor

1. Data Subjects

The Personal Data (that are subject to the GDPR) to be processed by the Vendor concerns but are not limited to:

(1) OOCL's prospective candidates, existing employees and former employees.

(2) all directors, officers, representatives and Affiliates of OOCL.

2. Categories of Personal Data

The Personal Data (that are subject to the GDPR) to be processed by the Vendor includes but are not limited to:

(1) Name
(2) Identity card number or passport number
(3) Tax number and social security number

(4) Department
(5) Role/Job Title
(6) Contact number (home and mobile)
(7) Mail address
(8) Signature
(9) Email (office or private)
(10) Home Address
(11) Language proficiency
(12) Identity details of instant messaging or social networking applications
(13) Social media profile
(14) Education and professional qualification
(15) Membership of professional bodies
(16) Training records
(17) Attendance and leave records
(18) Business travel records
(19) Employment movement
(20) Awards and/or achievement
(21) Resume

3. Categories of Sensitive Personal Data

The Categories of Sensitive Personal Data are:

(1) Sex
(2) Age
(3) Date of birth
(4) Place of birth
(5) Images of identity cards, passports or other personal identification documents of employees or their family members
(6) Nationality or racial and ethnic origin
(7) Legal domicile and citizenship
(8) Religion
(9) Political status
(10) Previous employment history and details/Performance history
(11) Reference check details
(12) Salaries, payroll data and benefits
(13) Bank account number and details
(14) Finance credit report
(15) Performance ratings and comments
(16) Photograph
(17) Sickness or Health records
(18) Marital status
(19) Family member's name (spouse, children, etc)
(20) Disciplinary and grievance records
(21) Criminal records (if relevant and required by the local jurisdiction)
(22) Adverse media searches
(23) Emergency contact details

Sensitive Personal Data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict

purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures as consistent with **Schedule 5**.

4. Nature and Purposes of Processing Operations

The Personal Data will be processed for purposes including, but not limited to:

(1) Recruitment and employment
(2) Compliance with employment and business contracts;
(3) Administration, planning, evaluation and development of employment
(4) Conduct of business activities of OOCL
(5) Comply with any legal and regulatory requirements, including prevention/detection of fraud and crime, anti-terrorist financing, statutory filing and record keeping, tax evasion, bribery and corruption
(6) Compliance with request or demand from competent authorities, including company registries, tax authorities, labour authorities, courts and law enforcement agencies
(7) Communications
(8) Reference check
(9) Remuneration and Reimbursement
(10) Insurance and claims
(11) Contributions to social security schemes
(12) Performance review
(13) Disciplinary actions
(14) Promotion or award
(15) Decision on removal from employment
(16) Protection of employees in case of emergency
(17) Hosting
(18) Business development
(19) Internal and external marketing
(20) Direct marketing
(21) Data matching
(22) Tonnage schemes
(23) Branch projects
(24) Audit and compliance activities related to the above
(25) Organization and report on social and business activities
(26) Pursuit of OOCL's legitimate interests and protection of OOCL's legal position in the event of legal proceedings

The frequency of the transfer: Continuous

5. Duration

OOCL's Personal Data may be processed by the Vendor for the duration during which the Vendor is to provide Services pursuant to the Contract or perform investigations in relation to such, unless otherwise required by applicable laws and/or justified under applicable statutory limitation periods, whichever is the later.

6. Competent Supervisory Authority

The competent supervisory authority(ies), in accordance with Clause 13 of the EU SCCs, refers to:

(i) The supervisory authority applicable to the data exporter in its EEA country of establishment;

(ii) Where the data exporter is not established in the EEA, the supervisory authority applicable in the EEA country where the data exporter's EU representative has been appointed pursuant to Article 27(1) of the Regulation;

(iii) Where the data exporter is not obliged to appoint a representative, the supervisory authority applicable to the EEA country where the data subjects relevant to the transfer are located; or

(iv) Where the processing of Personal Data to which UK Data Protection Law applies, the Information Commissioners Office.

SCHEDULE 5

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

	Measures	**Description**
1.	Measures of pseudonymisation and encryption of personal data	Data Protection Policy is in place. Multi-layered security protection in network, system, application, data and physical location to provide protection to Personal Data.
2.	Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Multi-layered security protection in network, system, application, data and physical location to provide protection to Personal Data. High-availability system design, regular data backup and recovery testing, and disaster recovery plan are in place.
3.	Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	High-availability system design, regular data backup and recovery testing, and disaster recovery plan are in place.
4.	Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing	Regular vulnerability assessment and penetration testing are arranged.
5.	Measures for user identification and authorisation	Strong password policy and Multi-Factor Authentication (MFA) are adopted.
6.	Measures for the protection of data during transmission	Data-in-Transit are encrypted.
7.	Measures for the protection of data during storage	Access control and data encryption are adopted to protect Personal Data.
8.	Measures for ensuring physical security of locations at which personal data are processed	Physical security perimeter and entry controls protect Personal Data from unauthorized access, damage and interference.
9.	Measures for ensuring events logging	Event logging, monitoring and audit trails are enabled with regular review.
10.	Measures for ensuring system configuration, including default configuration	System configuration is standardized with security best practices. Regular vulnerability assessment and penetration testing are arranged.

11.	Measures for internal IT and IT security governance and management	ISO 27001 certification compliance on information security management system. Cybersecurity Management Framework is adopted which governs the security management, protection, threat detection, incident response and cyberattack recovery plan.
12.	Measures for certification/assurance of processes and products	ISO 27001 certification compliance on information security management system.
13.	Measures for ensuring data minimisation	Data Protection Policy is in place. Multi-layered security protection in network, system, application, data and physical location to provide protection to Personal Data.
14.	Measures for ensuring data quality	Data Protection Policy is in place. Multi-layered security protection in network, system, application, data and physical location to provide protection to Personal Data.
15.	Measures for ensuring limited data retention	Personal Data are processed only for the duration during which provision of services pursuant to the relevant contract or perform investigations in relation to such, unless otherwise required by applicable laws and/or justified under applicable statutory limitation periods, whichever is the later.
16.	Measures for ensuring accountability	Data Protection Policy, logging and monitoring are in place.
17.	Measures for allowing data portability and ensuring erasure	Personal Data are processed only for the duration during which provision of services pursuant to the relevant contract or perform investigations in relation to such, unless otherwise required by applicable laws and/or justified under applicable statutory limitation periods, whichever is the later. All data on the hard drives are erased before hardware disposal.

SCHEDULE 6

OOCL's Sub-Processors include below:

Principal Registrar	MUFG Fund Services (Bermuda) Limited 4th Floor North, Cedar House 41 Cedar Avenue Hamilton HM 12 Bermuda
Branch Registrar	Computershare Hong Kong Investor Services Limited Shops 1712-1716, 17th Floor Hopewell Centre 183 Queen's Road East, Wanchai Hong Kong, China
Listing Exchange	The Stock Exchange of Hong Kong Limited
Major Banks	Australia and New Zealand Banking Group Limited Bank of America, National Association Bank of China (Hong Kong) Limited Bank of Communications Co., Ltd. China Construction Bank Corporation China Everbright Bank Co., Ltd. Citibank, N.A. DBS Bank Ltd. HSBC Holdings plc Industrial and Commercial Bank of China (Asia) Limited ING Bank N.V. JPMorgan Chase Bank, N.A. MUFG Bank, Ltd. Oversea-Chinese Banking Corporation Limited Shanghai Pudong Development Bank Co., Ltd. Société Générale Standard Chartered Bank (Hong Kong) Limited Sumitomo Mitsui Trust Bank, Limited
Solicitors	Conyers Dill & Pearman Clarendon House 2 Church Street Hamilton HM 11 Bermuda; and 29th Floor, One Exchange Square 8 Connaught Place Central Hong Kong, China Ince & Co Suites 4404-10, 44th Floor One Island East 18 Westlands Road, Taikoo Place Hong Kong, China Slaughter and May 47th Floor, Jardine House 1 Connaught Place, Central Hong Kong, China
Auditors	PricewaterhouseCoopers 22nd Floor Prince's Building Central Hong Kong, China