



ICE TRADE VAULT EUROPE PARTICIPANT AGREEMENT

This agreement (the "ICE European TR Agreement") sets out the terms on which ICE Trade Vault Europe Limited ("ICE Trade Vault"), which operates an electronic platform (the "ICE Trade Vault Europe Platform") for the collection, storage and regulatory reporting of a range of trade data in respect of derivatives trades (the "ICE Europe TR Service"), has agreed to provide the party identified below ("Participant") with access to the ICE Trade Vault Europe Platform. All capitalized terms used in this ICE European TR Agreement shall have the meanings ascribed to them in this ICE European TR Agreement.

1) ACCESS TO ICE TRADE VAULT EUROPE PLATFORM.

ICE Trade Vault hereby grants Participant a non-exclusive, non-transferable, revocable license to access the ICE Trade Vault Europe Platform as it may exist from time to time and to utilize any hardware, software, systems and/or communications links furnished by ICE Trade Vault to Participant from time to time (collectively, the "ICE Europe System") in accordance with the ICE Trade Vault Europe Terms (as defined below), solely for the purpose of allowing Participant to use the ICE Europe TR Service in the form offered by ICE Trade Vault from time to time. Participant is not required to subscribe to or use any ancillary service offered by any affiliate of ICE Trade Vault in order to access and use the ICE Europe TR Service.

2) TERMS OF ACCESS.

Participant's access to and use of the ICE Europe System and the ICE Europe TR Service will be governed by this ICE European TR Agreement, taken together with (i) the Service and Pricing Schedules (the "Fee Schedule") available on ICE Trade Vault's website at <https://www.theice.com/technology/post-trade/ice-trade-vault-europe>, (ii) the ICE Trade Vault Europe TR Rulebook governing the ICE Europe TR Service pursuant to Annex A, and (iii) any other applicable Annexes relating to this ICE European TR Agreement (collectively referred to herein as the "ICE Trade Vault Europe Terms"). ICE Trade Vault may amend the ICE Trade Vault Europe Terms at any time by posting amendments on ICE Trade Vault's website at <https://www.theice.com/technology/post-trade/ice-trade-vault-europe> and any such amendments will be prospectively binding on Participant, provided that ICE Trade Vault will provide at least two weeks' prior notice, through electronic or other direct communication with Participant, of any such amendments that are likely to materially and adversely affect Participant or its rights or obligations hereunder. Participant's use of the ICE Trade Vault Europe Platform after the effective date of any such amendment shall constitute its ratification of and agreement to any such amendment. If ICE Trade Vault elects to require Participant to acknowledge and agree to an amendment, such amendment will not become effective until Participant has done so in the manner specified by ICE Trade Vault.

3) PARTICIPANT'S REPRESENTATIONS, WARRANTIES AND COVENANTS.

Participant hereby represents, warrants and covenants as follows:

a) The ICE Europe TR Service, the ICE Europe System and ICE Trade Vault Europe Information (as defined below) are the exclusive proprietary property of ICE Trade Vault constituting trade secrets and confidential information. For purposes of this Agreement, "ICE Trade Vault Europe Information" means all information and content displayed or distributed on the ICE Europe System or as part of the ICE Europe TR Service or derived therefrom. Participant has been granted a limited license to use the ICE Europe System, the ICE Europe TR Service and the ICE Trade Vault Europe Information solely for the purposes set forth herein, and Participant will have no other rights with respect to the ICE Europe System, the ICE Europe TR Service or the ICE Trade Vault Europe Information. Without limitation of the foregoing, Participant will access and utilize the ICE Europe System, the ICE Europe TR Service and the ICE Trade Vault Europe Information solely for its own internal business activities in accordance with the ICE Trade Vault Europe Terms. In accordance with the foregoing, Participant will not provide access to the ICE Europe System, the ICE Europe TR Service or the ICE Trade Vault Europe Information to any third party unless such third party is



an affiliate of Participant or an ICE Trade Vault-approved Authorized Agent as provided in Section 4 below. Participant agrees that it will not copy, modify, reverse engineer, reverse assemble or reverse compile the ICE Europe System, the ICE Europe TR Service or any of the ICE Trade Vault Europe Information displayed on the ICE Europe System and that it will not distribute, rent, sell, retransmit, redistribute, release or license the ICE Europe System, the ICE Europe TR Service or any ICE Trade Vault Europe Information, or any part thereof to any third party (other than to its affiliates and agents subject to and in accordance with this ICE European TR Agreement). Participant further agrees that it will not, without limitation (other than for its own internal use in accordance with this ICE European TR Agreement), communicate, redistribute, or otherwise furnish, or permit to be communicated, redistributed or otherwise furnished, all or any portion of the ICE Trade Vault Europe Information, in any format, to any third party or in constructing or calculating the value of any index or indexed products. Participant will use its best efforts to ensure that its partners, officers, directors, employees and agents maintain sole control and possession of, and sole access to, ICE Trade Vault Europe Information obtained through Participant's access to the ICE Europe System. Participant hereby grants to ICE Trade Vault a non-exclusive, perpetual, non-transferable, irrevocable license to use all of Participant's trade data submitted to the ICE Europe TR Service (whether submitted by Participant, on Participant's behalf, by one of Participant's trading counterparties, or otherwise) (collectively, "ICE Europe TR Service Data") as contemplated by the ICE Trade Vault Europe Terms and to retain all such data as may be required to discharge the obligations of ICE Trade Vault under Applicable Law. For purposes of this Agreement, "Applicable Law" means all applicable treaties, legislation, statutes, directives, regulations or any other laws, rules and regulations, judicial orders, decrees and decisions, and the rules, regulations, interpretations and protocols of any applicable regulatory or self-regulatory organization or authority or any other applicable public authority, as amended from time to time.

b) Participant will comply with the ICE Trade Vault Europe Terms and Applicable Law in connection with Participant's access to and use of the ICE Europe System, the ICE Europe TR Service and the ICE Trade Vault Europe Information.

c) Participant acknowledges and accepts that it shall be solely responsible for any and all costs or expenses associated with its accessing and utilizing the ICE Trade Vault Europe Platform.

d) Participant acknowledges that ICE Trade Vault may, in its sole discretion, with or without cause or prior notice to Participant but subject to compliance with Applicable Law, temporarily or permanently cease to make ICE Trade Vault Europe Information available or suspend, terminate or restrict Participant's access to and utilization of the ICE Trade Vault Europe Platform. Participant acknowledges that its access to and utilization of the ICE Trade Vault Europe Platform may be monitored and recorded by ICE Trade Vault for its own purposes (including, without limitation, for purposes of monitoring levels of activity in categories of transactions for purposes of maintaining the functional and operational integrity of the ICE Europe System and for purposes of complying with Applicable Law) and not for the benefit of Participant. The ICE Trade Vault Europe TR Rulebook may set forth additional terms and conditions under which ICE Trade Vault may temporarily or permanently suspend the respective ICE Europe TR Service.

e) Participant has all necessary power and authority to execute and perform this ICE European TR Agreement, and this ICE European TR Agreement is its legal, valid and binding agreement, enforceable against Participant in accordance with its terms. Neither the execution of nor performance under this ICE European TR Agreement by Participant violates any law, rule, regulation or order, or any agreement, document or instrument, binding on or applicable to Participant.

f) Participant agrees to provide ICE Trade Vault with information related to Participant's use of the ICE Europe System and the ICE Europe TR Service that are reasonably requested by ICE



Trade Vault, if such information is reasonably necessary in order to enable ICE Trade Vault to assess the identity of persons or entities accessing the ICE Europe System and the ICE Europe TR Service through Participant's Passwords (as defined in Section 4), maintain the integrity of the ICE Europe System, or to comply with Applicable Law, and such information will be accurate and complete in all material respects and subject to the Confidentiality provisions of Section 7.

g) Participant acknowledges that it will not take any action to cause ICE Trade Vault to breach the U.S. Export Administration Regulations ("EAR"); the U.S. Department of the Treasury's Office of Foreign Assets Controls' ("OFAC") sanctions programs, including the Specially Designated Nationals List or any other sanctions or comparable (in the opinion of ICE Trade Vault in its unlimited discretion) programs in any jurisdiction. The EAR regulations can be found here: <https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear>. A current list of sanctions programs and additional information about OFAC sanctions can be found here: <http://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx>. ICE Trade Vault reserves the right to terminate its contractual relationships pertaining to the use of, or access to, ICE Trade Vault systems, information, applications, technology or any other property of any kind whatsoever (the "Property") with:

- (i) any entity (including but not limited to the Participant) which is a target of any sanctions or comparable (in the opinion of ICE Trade Vault in its unlimited discretion) programs (in any jurisdiction) or which has been granted access to the Property in contravention of the EAR as determined by ICE Trade Vault; and
- (ii) any entity, including but not limited to the Participant, via which persons or entities who are the target of any sanctions or comparable (in the opinion of ICE Trade Vault in its unlimited discretion) programs in any jurisdiction access the Property.

The Participant shall immediately notify ICE Trade Vault in writing if the Participant has breached, or will breach, this section 3(g).

h) Participant acknowledges and agrees that all fees and other charges incurred by Participant under this ICE European TR Agreement in any calendar month shall be invoiced by ICE Trade Vault to Participant based on the ICE Europe Schedules, as amended from time to time. If Participant elects via the ICE Europe System to pay certain fees and charges on behalf of another firm, Participant acknowledges and agrees that it will also be invoiced for such fees and charges based on the ICE Europe Schedules, as amended from time to time. ICE Trade Vault will provide Participant with an invoice which states the amount owed by Participant, including any fees, other charges or related taxes, which will be due and payable in the currency, timeframe and manner specified in the ICE Europe Schedules. Late payments will bear interest after the due date at a rate per annum of interest equal to LIBOR plus 1.5%, to the extent that such rate shall not exceed the maximum rate allowed by Applicable Law.

i) Participant acknowledges that Participant shall be liable for all taxes and duties (other than franchise and income taxes owed by ICE Trade Vault) on or with respect to the services or other transactions contemplated in this ICE European TR Agreement, including, without limitation, indirect taxes (such as sales tax, use tax or value-added tax) and taxes and duties levied by non-U.K. jurisdictions. Participant acknowledges that all fees and other charges with respect to the services or other transactions contemplated in this ICE European TR Agreement are exclusive of VAT. Participant shall not withhold any payments in respect of fees and/ or other charges due under this Agreement for any reason, including, but not limited to, for the purpose of withholding fees or charges for tax reasons.

j) Participant acknowledges that excessive levels of messages and queries submitted via the ICE Trade Vault API by Participant can negatively impact ICE Europe System performance, and acknowledges that ICE Trade Vault reserves the right to, if deemed necessary by ICE Trade Vault in its sole discretion, suspend Participant's access to the ICE Europe TR Service and the ICE Europe System pursuant to this Section 3(j). Following any suspension, ICE Trade Vault will notify Participant



of the remedial actions necessary in order to reinstate Participant's access to the ICE Europe TR Service.

k) Participant represents that any ICE Europe TR Service Data submitted by Participant or on its behalf is accurate and complete in all material respects and compliant with Applicable Law and agrees to comply with its obligations under Applicable Law to verify ICE Europe TR Service Data submitted to the ICE Europe TR Service on its behalf. Participant further agrees that it will report



any errors or omissions in respect of the ICE Europe TR Service Data as soon as technologically practicable after discovery of any such error or omission in accordance with the ICE Trade Vault TR Rulebook.

4) USER IDs AND PASSWORDS.

ICE Trade Vault may, in its sole and absolute discretion, issue to Participant, through its employees designated as its administrator(s) with respect to Participant's use of the ICE Europe System ("Participant User Administrator"), one or more user IDs and passwords (collectively, the "Passwords") to the system via the user interface ("UI") only for use exclusively by employees or ICE Trade Vault-approved third party agents ("Authorized Agents") of Participant or a Participant affiliate that are properly authorized to access the ICE Europe TR Service on behalf of Participant. The initial Participant User Administrator(s) for the ICE Europe TR Service, if applicable, are identified, respectively, at the end of this ICE European TR Agreement and Participant will notify ICE Trade Vault promptly of any change in its Participant User Administrator(s) in writing. ICE Trade Vault may, in its sole and absolute discretion, issue to Participant, through ICE Trade Vault employees or ICE Trade Vault-approved third party agents, one or more Passwords to the system via the ICE Trade Vault API only for use exclusively by employees or Authorized Agents of Participant or a Participant affiliate that are properly authorized to access to the ICE Europe TR Service and the ICE Trade Vault API on behalf of Participant. Participant will be solely responsible for controlling and monitoring the use of the Passwords, will provide the Passwords only to its Authorized Agents, and will not provide the Passwords to any third party other than an Authorized Agent. Participant will immediately notify ICE Trade Vault in writing of any unauthorized disclosure or use of the Passwords or access to the ICE Europe TR Service or of the need to deactivate any Passwords. Participant acknowledges and agrees that it will be bound by any actions taken through the use of its Passwords (except through the breach or negligence of ICE Trade Vault or if such actions would cause ICE Trade Vault to be in breach Applicable Law or regulation), whether or not such actions were authorized. The Participant User Administrator shall be responsible for all communications between ICE Trade Vault and Participant and any notices or other communications sent to the Participant User Administrator by ICE Trade Vault shall be binding on Participant. Upon issuance of Passwords to Participant, the Participant agrees that ICE Trade Vault may include the Participant's name among any list of participants in promotional materials relating to the ICE Europe TR Service. Any use of the trademark, trade name or logo of Participant by ICE Trade Vault in a press release or other promotional material will require the prior written consent of Participant.

5) TERM.

This ICE European TR Agreement, as amended from time to time, will continue in effect unless and until terminated by either party upon 30 days' written notice to the other, provided that this ICE European TR Agreement shall remain in effect with respect to any ICE Europe TR Service Data submitted prior to such termination. Termination of this ICE European TR Agreement shall terminate the ICE Europe TR Service provided by ICE Trade Vault to Participant. Each party's continuing obligations under this ICE European TR Agreement and the ICE Trade Vault Europe Terms, including, without limitation, those relating to "Indemnification" and "Confidentiality", will survive the termination of this ICE European TR Agreement.

6) LIMITATION OF LIABILITY; INDEMNITY.

a) SUBJECT TO SECTION 6(E), PARTICIPANT ACKNOWLEDGES, UNDERSTANDS AND ACCEPTS THAT ICE TRADE VAULT MAKES NO WARRANTY WHATSOEVER TO PARTICIPANT AS TO THE ICE EUROPE SYSTEM, OR THE ICE EUROPE TR SERVICE, EXPRESS OR IMPLIED, AND THAT THE ICE EUROPE SYSTEM, AND ICE EUROPE TR SERVICE IS PROVIDED ON AN "AS IS" BASIS AT PARTICIPANT'S SOLE RISK. ICE TRADE VAULT EXPRESSLY DISCLAIMS ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. NEITHER ICE TRADE VAULT NOR ITS MANAGERS, OFFICERS, AFFILIATES, SUBSIDIARIES, SHAREHOLDERS, EMPLOYEES OR AGENTS MAKE ANY WARRANTY WITH RESPECT TO, AND NO SUCH PARTY SHALL HAVE ANY LIABILITY TO PARTICIPANT (i) FOR THE ACCURACY, TIMELINESS, COMPLETENESS, RELIABILITY, PERFORMANCE OR CONTINUED AVAILABILITY OF THE ICE



EUROPE SYSTEM OR THE ICE EUROPE TR SERVICE OR (ii) FOR DELAYS, OMISSIONS OR INTERRUPTIONS THEREIN. PARTICIPANT ACKNOWLEDGES AND AGREES THAT THE ICE EUROPE TR SERVICE DOES NOT AND SHALL NOT SERVE AS THE PRIMARY BASIS FOR ANY DECISIONS MADE BY PARTICIPANT AND THAT ICE TRADE VAULT IS NOT AN ADVISOR OR FIDUCIARY OF PARTICIPANT.

b) Subject to Sections 6(c) and 6(e) of this ICE European TR Agreement, Participant shall indemnify, protect and hold harmless ICE Trade Vault, its directors, officers, affiliates, employees and agents from and against any and all losses, liabilities, judgments, suits, actions, proceedings, claims, damages, and costs (including attorney's fees) resulting from or arising out of any act or omission by any person obtaining access to the ICE Trade Vault Europe Platform through the Passwords (other than through the breach or negligence of ICE Trade Vault), whether or not Participant has authorized such access.

c) IN NO EVENT WILL EITHER PARTY BE LIABLE (WHETHER IN CONTRACT, OR TORT (INCLUDING NEGLIGENCE), FOR BREACH OF STATUTORY DUTY, OR OTHERWISE) FOR ANY SPECIAL, INDIRECT, INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, EVEN IF IT HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

d) Notwithstanding the terms of Section 6(a) and subject to Sections 6(c) and 6(e), in the event that ICE Trade Vault is determined to be liable to Participant for any cause, Participant expressly agrees that in entering into this ICE European TR Agreement, ICE Trade Vault's aggregate liability, for all causes of action (whether in contract, or tort (including negligence), for breach of statutory duty, or otherwise), will not exceed the total fees and other amounts (excluding any applicable taxes or duties) paid to ICE Trade Vault by Participant in the previous six months from the date of the occurrence of the liability.

e) THE LIMITATIONS AND EXCLUSIONS OF LIABILITY SET OUT HEREIN SHALL NOT APPLY TO EITHER PARTY'S LIABILITY FOR: (I) DEATH OR PERSONAL INJURY CAUSED BY THAT PARTY'S NEGLIGENCE; (II) FRAUD OR FRAUDULENT MISREPRESENTATION; OR (III) ANY OTHER LIABILITY THAT CANNOT BE EXCLUDED OR LIMITED BY APPLICABLE LAW.

7) CONFIDENTIALITY.

a) Any and all non-public information in any form obtained by either party or its employees arising out of or related to the provision or use of the ICE Europe System or the ICE Europe TR Service, including but not limited to trade secrets, processes, computer software and other proprietary data, research, information or documentation related thereto and ICE Trade Vault Europe Information, shall be deemed to be confidential and proprietary information. Each party agrees to hold such information in strict confidence and not to disclose such information to third parties (other than to its employees, its affiliates and their employees or its agents) or to use such information for any purpose whatsoever other than as contemplated by the ICE Trade Vault Europe Terms and to advise each of its employees, affiliates and agents who may be exposed to such proprietary and confidential information of their obligations to keep such information confidential in accordance with this Section 7.

b) The restrictions in Section 7(a) shall not apply to information which: (i) is in or becomes part of the public domain other than by unauthorized disclosure including by but not limited to by a party disclosing confidential information in violation of this ICE European TR Agreement; (ii) is known to or obtained by such party previously without an obligation of confidentiality; (iii) is independently developed by such party outside of this ICE European TR Agreement; (iv) is required to be disclosed by Applicable Law (including, without limitation, provisions of Applicable Law that mandate the publication of aggregated trade data), or pursuant to a subpoena or order of a court or regulatory, self-regulatory or legislative body of competent jurisdiction; or (v) is disclosed in connection with any regulatory or self-regulatory request for information.



c) In the event that ICE Trade Vault receives a subpoena, data request, or order of court in any private-party litigation requesting confidential information of Participant, ICE Trade Vault will notify Participant of such requirement or request (if permitted by Applicable Law and/ or regulation). ICE Trade Vault will make reasonable commercial efforts to cooperate with Participant to enable Participant to narrow the scope of the required or requested disclosures or to seek a protective order or other similar relief. If requested by Participant, ICE Trade Vault will formally request that any governmental body or public authority treat the information provided as confidential, to the extent permitted and not already treated as such, pursuant to Applicable Law.

d) Any access to ICE Europe TR Service Data provided by ICE Trade Vault to a corporate affiliate, whether pursuant to a license or otherwise, shall be allowed solely in accordance with Applicable Law. The provision of such access is an essential element of ICE Trade Vault's outsourcing business model. Such access will be granted to corporate affiliates of ICE Trade Vault based outside the European Union. No entity that has a parent undertaking or a subsidiary relationship with ICE Trade Vault will be permitted to use information submitted by Participant that is subject to the restrictions in Section 7(a) for commercial purposes.

8) NOTICES.

All notices delivered with respect to this ICE European TR Agreement shall be in writing and either (i) hand delivered or forwarded by registered or certified mail, or (ii) sent via electronic mail, in either case to the relevant address provided by a party for such purpose.

9) THIRD PARTY RIGHTS.

a) A person who is not a party to this ICE European TR Agreement has no right under the Contracts (Rights of Third Parties) Act 1999 (the "Third Parties Act") to enforce any term of this ICE European TR Agreement.

b) The parties to this ICE European TR Agreement do not require the consent of any Third Party to rescind or vary this ICE European TR Agreement at any time.

10) FORCE MAJEURE.

Neither ICE Trade Vault nor Participant shall be deemed to be in breach of any provision hereof or be liable for any delay, failure in performance, or interruption of service resulting directly or indirectly from acts of God, civil or military authority, civil disturbance, war, strikes, fires, other catastrophes, power failure or any other cause beyond its reasonable control.

11) WAIVER.

No waiver by either party of any breach by the other in the performance of any provisions of this ICE European TR Agreement shall operate as a waiver of any continuing or future breach, whether of a like or different character.

12) ASSIGNMENT.

Rights and/or obligations under this ICE European TR Agreement may not be assigned by either party without the other party's express prior written consent; provided, however, that (A) Participant may assign this ICE European TR Agreement to any entity (i) controlling, controlled by, or under common control with Participant, or (ii) which succeeds to all or substantially all of the assets and business of Participant, provided that, in the case of any such assignment by Participant, the assignee agrees in writing to assume the assignor's obligations under, and to be bound by the provisions of, this ICE European TR Agreement (as it may be amended from time to time); and (B) ICE Trade Vault may assign all or part of its rights and obligations under this ICE European TR Agreement to any entity (i) controlling, controlled by, or under common control with ICE Trade Vault, or (ii) which succeeds to all or substantially all of the assets and business of ICE Trade Vault, provided that, in the case of any such assignment by ICE Trade Vault, the assignee agrees in writing to assume the obligations under, and to be bound by the provisions of, this ICE European TR



Agreement that have been assigned. On the effective date of any valid assignment pursuant to this Section 12, the assignor shall be released from all obligations and liabilities arising under this ICE European TR Agreement or, in case of a partial assignment by ICE Trade Vault, from all obligations and liabilities arising from the parts of this ICE European TR Agreement that have been assigned. This ICE European TR Agreement shall be binding upon and shall inure to the benefit of the parties and their respective successors and permitted assigns in accordance with its terms.

13) GOVERNING LAW.

This ICE European TR Agreement and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed in all respects by, and construed in accordance with the laws of England and Wales. ICE Trade Vault's ICE Europe TR Service is subject to regulation by the Financial Conduct Authority ("FCA") as a UK Trade Repository.

14) ARBITRATION.

a) Any dispute, difference, controversy or claim (of any and every kind or type, whether based on contract, tort, statute, regulation, or otherwise) arising out of, in relation to, or in connection with this ICE European TR Agreement, including any dispute as to the existence, construction, validity, interpretation, enforceability, termination or breach of this ICE European TR Agreement ("Dispute") shall be referred to and finally resolved by arbitration under the rules of the London Court of International Arbitration ("LCIA", and such rules, "LCIA Rules"), which LCIA Rules are deemed to be incorporated into this Section 14. In the event of a conflict between any provision of the LCIA Rules and this Section 14, this Section 14 shall prevail. Any provision of the LCIA Rules relating to the nationality of an arbitrator shall to that extent not apply. For purposes of this Section 14, the term "Other Participant" means a person other than ICE Trade Vault that is party to an ICE European TR Agreement in the same or substantially the same form as this ICE European TR Agreement.

b) The seat of arbitration will be London and the language of the arbitration proceedings shall be English.

c) The tribunal will be comprised of three arbitrators appointed by the LCIA. The LCIA shall appoint one of the arbitrators to act as the chairman of the tribunal. The Tribunal members will be persons considered by the LCIA in its discretion to have experience with respect to the subject matter of the dispute. Tribunal members shall not be current or former employees or directors of Participant, current or former employees or directors of any Other Participant, current or former employees of ICE Trade Vault, or any person or persons with a material interest or conflict of interest in the outcome of the Dispute.

d) The award of the arbitral tribunal will be final and binding on ICE Trade Vault and Participant from the day it is made. Judgment upon the award may be entered or the award enforced through any other procedure in any court of competent jurisdiction.

e) The provisions of this Section 14 may not be varied by Participant save where it and ICE Trade Vault agree in express written terms.

f) If Participant has now or hereafter has a right to claim sovereign immunity from suit or sovereign immunity from enforcement for itself or any of its assets, it shall be deemed to have waived any such immunity to the fullest extent permitted by any applicable national, federal, supranational, state, regional, provincial, local or other statute, law, ordinance, regulation, rule, code, guidance, order, published practice or concession, judgment or decision of a governmental authority. Such waiver shall apply in respect of any immunity from:

- (i) any proceedings commenced pursuant to this Section 14;



- (ii) any judicial, administrative or other proceedings to aid an arbitration commenced pursuant to this Section 14; and
- (iii) any effort to confirm, enforce or execute any decision, settlement, award, judgment, service of process, execution order or attachment (including pre-judgment attachment) that results from any judicial or administrative proceedings commenced pursuant to this Section 14.
- (iv) The rights and obligations of Participant under this ICE European TR Agreement are of a commercial and not a governmental nature.
- (v) Participant shall not raise or in any way whatsoever assert a defense of sovereign immunity in relation to any claim or enforcement proceedings arising from a Dispute under this ICE European TR Agreement.

15) HEADINGS.

The headings in this ICE European TR Agreement are intended for convenience of reference and shall not affect its interpretation.

16) SEVERABILITY.

If any provision of this ICE European TR Agreement (or any portion thereof) shall be invalid, illegal or unenforceable, the validity, legality or enforceability of the remainder of this ICE European TR Agreement shall not in any way be affected or impaired thereby.

17) WHOLE AGREEMENT.

This ICE European TR Agreement (including without limitation any annexes hereto) and any documents to be executed pursuant to it constitute the entire agreement between the parties and supersede all prior agreements and arrangements (if any) whether written, oral or implied between the parties relating to the subject matter of this ICE European TR Agreement. Each party acknowledges and agrees that, in entering into this ICE European TR Agreement, it has not been induced to enter into this ICE European TR Agreement by any representation or warranty other than those contained in this ICE European TR Agreement.



Date: _____, 20__

Signed on behalf of ICE Trade Vault Europe Limited

Signature:

Name:

Title: _____ :

Signature: _____

Name:

Title:

Signed on behalf of [Participant Full Legal Name]

Signature:

Name:

Title:

Participant Legal Entity Identifier:

Participant User Administrator for the ICE Europe TR Service: (Required to gain access to the ICE Europe TR Service)

Name: _____

Title: _____

Address: _____

Telephone: _____

Fax: _____

Email: _____



ANNEX A — ICE EUROPE TR SERVICE

ICE Trade Vault offers the ICE Europe TR Service as a regulated service. The rules, terms, conditions and procedures applicable to the ICE Europe TR Service are set forth in the ICE Trade Vault Europe TR Rulebook available at www.icetradevault.com. Participant agrees to be bound by the ICE Trade Vault Europe TR Rulebook, as amended from time to time, together with this Agreement for purposes of the ICE Europe TR Service.



ANNEX B - DATA PROTECTION

Where Participant is incorporated in any member state of the European Economic Area (“**EEA**”); in the United Kingdom or is established or has a branch or presence through other form of stable arrangement in or is otherwise subject to the jurisdiction of one or more of the jurisdictions addressed in Schedules 7-12, the following additional terms in this Annex B (“**Additional Terms**”) and the relevant Schedule(s) shall be incorporated into and form part of the ICE Trade Vault Europe Participant Agreement (“**Agreement**”) under which ICE Trade Vault Europe Limited (“**ICE**”) provides the ICE Europe TR service as defined in the Agreement (“**Services**”) to Participant. In the event of conflict with any other terms of the Agreement, these Additional Terms shall prevail. ICE and Participant agree to be bound by the terms and conditions of this Agreement with respect to the Personal Data that is the subject matter of these Additional Terms. ICE may amend these Additional Terms at any time by providing notice to Participant, which may be sent via email, and any such amendments will be binding on Participant effective ten (10) days from the date of such notice.

1. INTERPRETATION

1.1 In these Additional Terms, the terms "**Controller**", "**Data Subject**", "**Personal Data**", "**Personal Data Breach**", "**Process/Processing**", "**Processor**", "**Special Categories of Data**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR.

1.2 Capitalised terms not otherwise defined in these Additional Terms shall have the same meaning as the Agreement.

1.3 The following further terms shall have the meanings ascribed to them:

"**Applicable Laws**" means any law, statute, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule or other binding restriction (including any and all legislative and/or regulatory amendments or successors thereto), to which a party to this Agreement is subject and which is applicable to a party's information protection and privacy obligations;

"**C-to-C Transfer Clauses**" means Sections I, II and III (as applicable) in so far as they relate to Module One (Controller-to-Controller) within the Standard Contractual Clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by EC Commission Decision of 4 June 2021 as incorporated in these Additional Terms as Schedule 2);

"**C-to-P Processing Clauses**" has the meaning given to it in clause 2.3;

"**C-to-P Transfer Clauses**" means Sections I, II and III (as applicable) in so far as they relate to Module Two (Controller-to-Processor) within the Standard Contractual Clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by EC Commission Decision of 4 June 2021 as incorporated in these Additional Terms as Schedule 5);

"**Data Exporter**" means a party which exports Personal Data to a Data Importer in circumstances where the Personal Data are transferred from one country to another;

"**Data Importer**" means a party which imports Personal Data from a Data Exporter in circumstances where the Personal Data are transferred from one country to another;



"**Data Protection Laws**" means the any applicable laws from time to time that govern the processing of Personal Data under this Agreement or that otherwise relate to data protection or privacy;

"**EEA**" means the European Economic Area;

"**Effective Date**" means the date of this Agreement;

"**GDPR**" means Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016;

"**Swiss Data Protection Laws**" means the Federal Act on Data Protection ("**FADP**") of 19 June 1992 as updated by the revised version of the FADP as updated from time to time;

"**Transfer Clauses**" means either the C-to-C Transfer Clauses or the C-to-P Transfer Clauses, as the case may be.

"**UK**" means the United Kingdom of Great Britain and Northern Ireland;

"**UK Data Protection Laws**" 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 UK, including the UK GDPR and the Data Protection Act 2018;

"**UK GDPR**" means the United Kingdom General Data Protection Regulation, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.

2. GENERAL TERMS

- 2.1 The parties shall each Process Personal Data in accordance with Data Protection Laws.
- 2.2 Where Participant transfers Personal Data to ICE:
 - (a) Schedule 1 describes the details of processing where ICE as the recipient of the transfer acts as a Controller of the Personal Data;
 - (b) Schedule 3 describes the details of processing where ICE as the recipient of the transfer acts as a Processor of the Personal Data.
- 2.3 For the purposes of section 2.2 (b) where ICE as the recipient of the transfer acts as a Processor of that Personal Data, ICE will comply with Schedule 6 to the extent that such obligations are required by Applicable Laws to which the processing of Personal Data is subject (the "**C-to-P Processing Clauses**").
- 2.4 Where Participant provides Personal Information as defined in and that is subject to the California Consumer Privacy Act or the California Privacy Rights Act to ICE for purposes of providing the services, ICE shall act as a service provider with respect to Participant's Personal Information. ICE shall process Participant's Personal Information consistent with ICE's Privacy Policy and unless Participant provides prior written approval, ICE shall not collect, retain, use, disclose, or sell Participant's Personal Information for any purpose other than performing the services pursuant to the Agreement, enabling ICE to meet its legal and regulatory requirements, or product improvement and development.



- 2.5 In the event of a conflict between Applicable Laws and the terms of this Agreement then the parties shall endeavour (as far as reasonably possible) to comply with the terms of this Agreement but without contravening Applicable Laws. ICE will promptly notify Participant if it believes that it may no longer be able to comply with any of these Additional Terms.
- 2.6 The parties shall each implement appropriate technical and organisational security measures to ensure a level of security appropriate to the risks that are presented by the Processing and the nature of the Personal Data to be protected.
- 2.7 In relation to all Personal Data provided by it to ICE, Participant shall ensure that:
- (a) where consent is required under Applicable Laws, all relevant Data Subjects have consented (in the appropriate manner) to their Personal Data being disclosed to ICE for Processing in accordance with the Agreement and that the Processing otherwise complies with Data Protection Laws and these Additional Terms, including any onward international transfer of Personal Data by ICE;
 - (b) the disclosure of Personal Data by Participant to ICE will be in each case and in all respects lawful;
 - (c) notice of the disclosure of their Personal Data to ICE for Processing in accordance with the Agreement and these Additional Terms will be provided to all relevant Data Subjects (including any authorised users) prior to any such disclosure, including notice of Processing where ICE is the Controller for the purposes set out in Schedule 1. If requested by ICE, Participant shall provide evidence that it has provided such notice;
 - (d) Participant complies with, and represents and warrants that it has complied with, Data Protection Laws in relation to the use of the Services by Participant and its authorised users;
 - (e) it shall not, by any act or omission, put ICE or any of its affiliates or subsidiaries in breach of any Data Protection Laws; and
 - (f) it shall do and execute, or arrange to be done and executed, each act, document and thing necessary or desirable in order to comply with this clause 2.

3. DATA TRANSFERS

- 3.1 Where Personal Data are transferred from Participant as Data Exporter to ICE as Data Importer, Participant and ICE shall transfer and Process the Personal Data in accordance with:
- (a) all Applicable Laws; and
 - (b) to the extent that they apply to the transfer, the specific jurisdiction provisions set forth in Schedules 7-12.
- 3.2 Where Section 3.1(a) applies to (i) a transfer of Personal Data from the EEA to a territory outside the EEA that has not been the subject of a finding of an adequate level of protection by the European Commission as described in Article 45(1) of the GDPR or any other law that may replace or amend it in the future; or (ii) a transfer of Personal Data that was originally transferred in the circumstances described in clauses 3.2(i) to another territory not covered by clause 3.2(i):
- (a) where ICE acts as a Controller of that Personal Data, Participant and ICE shall comply with the "**C-to-C Transfer Clauses**".
 - (b) where ICE acts as a Processor of that Personal Data, Participant and ICE shall comply with the "**C-to-P Transfer Clauses**".
- 3.3 For the purposes of the Transfer Clauses the following provisions shall apply:
- (i) The names, addresses, and contact information of Participant as Data Exporter shall be considered to be incorporated into Schedule 1 and Schedule 3 of these Additional Terms;
 - (ii) The contents of Schedule 1 to these Additional Terms (categories of Data Subjects, categories of Personal Data and special categories of Personal Data (as defined in the GDPR),, countries of origin, processing locations, nature of the processing, purposes of the transfer, duration of processing and retention periods) shall form Annex I to the C-to-C Transfer Clauses;
 - (iii) The contents of Schedule 3 to these Additional Terms (categories of Data Subjects, categories of Personal Data and special categories of Personal Data (as defined in the GDPR),, countries of origin, processing locations, nature of the processing, purposes of the transfer, duration of processing and retention periods) shall form Annex I to the C-to-P Transfer Clauses;
 - (iv) The contents of Schedule 4 to these Additional Terms (description of technical and organisational measures by the Data Importer) shall form Annex II (Technical and organisational measures including technical and organisational measures to ensure the security of the data) to the C-to-C and C-to-P Transfer Clauses; and
 - (v) For the purposes of paragraph (a) of Clause 13 (Supervision) in Schedules 2 and 5, each "[" and "]" shall be deleted in their entirety.
 - (vi) the relevant party's signature to this Agreement shall be considered as a signature to the Transfer Clauses.



- 3.4 Where Section 3.2 applies, ICE and Participant shall comply with the following additional safeguards:
- (a) ICE will assess whether the laws applicable to it provide adequate safeguards to protect the Personal Data under Data Protection Laws. To the extent that ICE determines that any such laws are not in line with the requirements of the Transfer Clauses and Data Protection Laws, ICE undertakes to comply with the safeguards set out in this Section 3.4.
 - (b) ICE undertakes to adopt supplementary measures to protect the Personal Data received under the Transfer Clauses in accordance with the requirements of Data Protection Laws, including by implementing appropriate technical and organisational safeguards, such as encryption or similar technologies, access controls or other compensating controls, to protect the Personal Data against any interference that goes beyond what is necessary in a democratic society to safeguard national security, defence and public security.
 - (c) ICE agrees that any audits carried out pursuant to the Transfer Clauses may include inquiries as to whether any Personal Data has been disclosed to public authorities and, if so, the conditions under which such disclosure has been made.
 - (d) If ICE receives a legally binding request for access to the Personal Data by a public authority, ICE will:
 - (i) promptly notify Participant of such request to enable Participant to intervene and seek relief from such disclosure, unless ICE is otherwise prohibited from providing such notice, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation. If ICE is so prohibited:
 - (1) It will use its reasonable best efforts to obtain the right to waive this prohibition in order to communicate as much information as it can and as soon as possible, and be able to demonstrate that it did so.
 - (2) In the event that, despite having used its reasonable best efforts, ICE is not permitted to notify Participant, ICE will make available on an

annual basis general information on the requests it received to the competent supervisory authority of Participant.

(3) Oppose any such request for access and contest its legal validity to the extent legally permitted under applicable law.

(ii) not make any disclosures of the Personal Data to any public authority that are determined to be massive, disproportionate and indiscriminate in a manner that it would go beyond what is necessary in a democratic society; and

(iii) upon request from Participant, provide general information on the requests from public authorities ICE has received in the preceding 12-month period relating to the Personal Data.

3.5 To the extent that the processing of Personal Data under these Additional Terms is subject to UK Data Protection Laws and/or Swiss Data Protection Laws, the Transfer Clauses shall apply as required and shall be interpreted as follows:

(a) The Transfer Clauses shall be read and interpreted in the light of the provisions of UK Data Protection Laws and/or Swiss Data Protection Laws as applicable, and so that they fulfil the intention for them to provide the appropriate safeguards as required under UK Data Protection Laws and Swiss Data Protection Laws as applicable.

(b) The Transfer Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in UK Data Protection Laws or in Swiss Data Protection Laws as applicable.

3.6 For the purposes of Swiss Data Protection Laws:

(a) In Clause 18 (c) of the Transfer Clauses “Member State” will be interpreted in such a way as to not to exclude Data Subjects in Switzerland from the possibility of bringing a claim under this Addendum before the courts in Switzerland.

(b) Part C of Schedules 1 and 3 shall also include the FDPIC

3.7 For the purposes of UK Data Protection Laws:

(a) The 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, shall apply.

(b) The information required by Part 1, Tables 1 to 3 of the Approved Addendum is set out in Schedules 1 to 5 of this DPA (as applicable).

(c) For the purposes of Part 1, Table 4 of the Approved Addendum, neither party may end the Approved Addendum when it changes.



- 3.8 In the event of any conflict between:
- (a) these Additional Terms and the Transfer Clauses then the Transfer Clauses shall prevail.
 - (b) the Transfer Clauses and Section 3.6, the provisions that provide the most protection to data subjects shall prevail.
 - (c) these Additional Terms and the specific jurisdiction provisions set forth in Schedules 7-12, then precedence shall be given to the specific jurisdiction provisions set forth in Schedules 7-12.
- 3.9 Save for the provisions in Section 3 the terms of this Agreement shall not vary the Transfer Clauses in any way.
- 3.10 If so required by the laws or regulatory procedures of any jurisdiction, Participant and ICE shall execute or re-execute the Transfer Clauses, any agreements that may be necessary to meet the requirements of them or any provisions set forth in Schedule 7- 12 as separate documents setting out the proposed transfers of Personal Data in such manner as may be required.
- 3.11 In the event that the Transfer Clauses or any of the specific jurisdiction provisions set forth at Section 3.6 or 3.7 or Schedules 7-12 are amended, replaced or repealed by the European Commission, Switzerland, the United Kingdom or under applicable Data Protection Laws, the parties shall work together in good faith to enter into any updated version of the Transfer Clauses or to take such steps as may be reasonably necessary to comply with the specific jurisdiction provisions (to the extent required) or negotiate in good faith a solution to enable a transfer of Personal Data to be conducted in compliance with Data Protection Laws.

4. GOVERNING LAW AND JURISDICTION

Without prejudice to clause 17 of the Transfer Clauses, these Additional Terms and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed in all respects by, and construed in accordance with, the laws of England and Wales.



SCHEDULE 1

Details of the processing activities for C-to-C transfers

A. LIST OF PARTIES

DATA EXPORTER(S): *[IDENTITY AND CONTACT DETAILS OF THE DATA EXPORTER(S) AND, WHERE APPLICABLE, OF ITS/THEIR DATA PROTECTION OFFICER AND/OR REPRESENTATIVE IN THE EUROPEAN UNION]*

Name, Address, Contact Details Signature and Date are incorporated per Section 3 of the Additional Terms.

Activities relevant to the data transferred under these Clauses: The Data Exporter is a customer of the Data Importer, which it has engaged to provide certain services relating to the collection, storage and regulatory reporting of a comprehensive range of trade data in respect of derivatives trades services. In the course of receiving these services and related support, the Data Exporter will transfer Personal Data to the Data Importer for processing, the nature of which and the purposes for which are specified in this Schedule.

Role (controller/processor): Controller

DATA IMPORTER(S):

Name: ICE Trade Vault Europe Limited

Address: Milton Gate, 60 Chiswell Street, London EC1Y 4SA

Contact person's name, position and contact details: ICE Data Protection Officer,
Regulatory-DataProtection@ice.com

Activities relevant to the data transferred under these Clauses: The Data Importer is a provider of certain services relating to the collection, storage and regulatory reporting of a comprehensive range of trade data in respect of derivatives trades services.

Role (controller/processor): Controller

B. DESCRIPTION OF TRANSFER

CATEGORIES OF DATA SUBJECTS WHOSE PERSONAL DATA IS TRANSFERRED

The personal data transferred concern the following categories of Data Subjects: past, potential, present and future staff of the Data Exporter (including candidates, volunteers, agents, interns, contractors, temporary and casual workers) ("Employees").

CATEGORIES OF PERSONAL DATA TRANSFERRED

The Personal Data transferred relating to employees includes (without limitation): employee name, log-in credentials, business contact details, IP address, information generated by employees in relation to their use of the services.



SENSITIVE 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.

Not applicable.

THE FREQUENCY OF THE TRANSFER (E.G. WHETHER THE DATA IS TRANSFERRED ON A ONE-OFF OR CONTINUOUS BASIS)

Ongoing throughout the duration of the Agreement.

NATURE OF THE PROCESSING

Storage, consultation, analysis, communication, and other processing needed to support the purposes noted below.

PURPOSE(S) OF THE DATA TRANSFER AND FURTHER PROCESSING

The transfer is made for the following purposes:

- Achieve ICE's legitimate interests in marketing its products and services, improving and developing its products, and securing information and its operating environment.
- To enable the Data Importer to meet legal and regulatory requirements.

THE PERIOD FOR WHICH THE PERSONAL DATA WILL BE RETAINED, OR, IF THAT IS NOT POSSIBLE, THE CRITERIA USED TO DETERMINE THAT PERIOD

The Data Exporter may retain Personal Data for the duration of the Agreement. Personal Data will be retained and deleted in accordance with the Agreement.

C. COMPETENT SUPERVISORY AUTHORITY

IDENTIFY THE COMPETENT SUPERVISORY AUTHORITY/IES IN ACCORDANCE WITH CLAUSE 13

The competent supervisory authority shall be the supervisory authority which is competent to supervise the activities of the Data Exporter.

SCHEDULE 2

C-to-C Transfer Clauses

SECTION I

Clause 1

Purpose and scope

- (a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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)⁽¹⁾ for the transfer of personal data to a third country.
- (b) The Parties:
- (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I (hereinafter each 'data exporter'), and
 - (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I (hereinafter each 'data importer').
- have agreed to these standard contractual clauses (hereinafter: 'Clauses').
- (c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.
- (d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

- (a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including

(1) Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.



the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

- (b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

- (a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
 - (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
 - (ii) Clause 8.5 (e) and Clause 8.9(b);
 - (iv) Clause 12(a) and (d);
 - (v) Clause 13;
 - (vi) Clause 15.1(c), (d) and (e);
 - (vii) Clause 16(e);
 - (viii) Clause 18(a) and (b).
- (b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

- (a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
- (b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
- (c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

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



Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.

Clause 7 - Optional

[Intentionally left blank.]

SECTION II - OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I. It may only process the personal data for another purpose:

- (i) where it has obtained the data subject's prior consent;
- (ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- (iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 Transparency

- (a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:
 - (i) of its identity and contact details;
 - (ii) of the categories of personal data processed;
 - (iii) of the right to obtain a copy of these Clauses;
 - (iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer.

- (b) In the latter case, the data importer shall, to the extent possible, make the information publicly available.
- (c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.
- (d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 Accuracy and data minimisation

- (a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.
- (b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.
- (c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation⁽²⁾ of the data and all back-ups at the end of the retention period.

8.5 Security of processing

- (a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.
- (b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(2) This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible.

- (c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- (d) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.
- (e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.
- (f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.
- (g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 Sensitive data

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

8.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union⁽³⁾ (in the same country as the data importer or in another third country, hereinafter 'onward transfer') unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

(3) The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.



- (i) it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- (ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;
- (iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;
- (iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;
- (v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or
- (vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.8 Processing under the authority of the data importer

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

8.9 Documentation and compliance

- (a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.
- (b) The data importer shall make such documentation available to the competent supervisory authority on request.

Clause 9

[Intentionally left blank]

Clause 10

Data subject rights

- (a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue

delay and at the latest within one month of the receipt of the enquiry or request.⁽⁴⁾ The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

- (b) In particular, upon request by the data subject the data importer shall, free of charge:
 - (i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);
 - (ii) rectify inaccurate or incomplete data concerning the data subject;
 - (iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.
- (c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.
- (d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter 'automated decision'), which would produce legal effects concerning the data subject or similarly significantly affect him / her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:
 - (i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and
 - (ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.
- (e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.
- (f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

(4) That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.

- (g) If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

Clause 11

Redress

- (a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.
- (b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
- (c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
 - (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
 - (ii) refer the dispute to the competent courts within the meaning of Clause 18.
- (d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
- (e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
- (f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

- (a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
- (b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.
- (c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.



- (d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.
- (e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

Clause 13

Supervision

- (a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I, shall act as competent supervisory authority.

- (b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

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

Clause 14

Local laws and practices affecting compliance with the Clauses

- (a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and

proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

- (b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
- (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
 - (ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards⁽⁵⁾;
 - (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
- (c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
- (d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
- (e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so.

- (f) In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

(5) As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified



at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

Clause 15

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

15.1 Notification

- (a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
 - (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
 - (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
- (b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
- (c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
- (d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
- (e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

- (a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).
- (b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.
- (c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

- (a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
- (b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
- (c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
 - (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
 - (ii) the data importer is in substantial or persistent breach of these Clauses; or
 - (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

- (d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data



exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

- (e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of The Netherlands.

Clause 18

Choice of forum and jurisdiction

- (a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- (b) The Parties agree that those shall be the courts of The Netherlands.
- (c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
- (d) The Parties agree to submit themselves to the jurisdiction of such courts.



ANNEX I TO SCHEDULE 2

See Schedule 1 to the Additional Terms.



ANNEX II TO SCHEDULE 2

See Schedule 4 to the Additional Terms.



SCHEDULE 3

Details of the processing activities for C-to-P transfer

A. LIST OF PARTIES

DATA EXPORTER(S): *[IDENTITY AND CONTACT DETAILS OF THE DATA EXPORTER(S) AND, WHERE APPLICABLE, OF ITS/THEIR DATA PROTECTION OFFICER AND/OR REPRESENTATIVE IN THE EUROPEAN UNION]*

Name, Address, Contact Details, Signature and Date are incorporated per Section 3 of the Additional Terms.

Activities relevant to the data transferred under these Clauses: The Data Exporter is a customer of the Data Importer, which it has engaged to provide certain services relating to the collection, storage and regulatory reporting of a comprehensive range of trade data in respect of derivatives trades services. In the course of receiving these services and related support, the Data Exporter will transfer Personal Data to the Data Importer for processing, the nature of which and the purposes for which are specified in this Schedule.

Role (controller/processor): Controller

DATA IMPORTER(S): *[IDENTITY AND CONTACT DETAILS OF THE DATA IMPORTER(S), INCLUDING ANY CONTACT PERSON WITH RESPONSIBILITY FOR DATA PROTECTION]*

Name: ICE Trade Vault Europe Limited

Address: Milton Gate, 60 Chiswell Street, London EC1Y 4SA

Contact person's name, position and contact details:

ICE Data Protection Officer, Regulatory-DataProtection@ice.com

Activities relevant to the data transferred under these Clauses: The Data Importer is a provider of certain services relating to the collection, storage and regulatory reporting of a comprehensive range of trade data in respect of derivatives trades services.

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

CATEGORIES OF DATA SUBJECTS WHOSE PERSONAL DATA IS TRANSFERRED

Past, potential, present and future staff of the Data Exporter (including candidates, volunteers, agents, interns, contractors, temporary and casual workers) ("employees") who use the services provided by the Data Importer);

CATEGORIES OF PERSONAL DATA TRANSFERRED

The personal data transferred relating to employees includes (without limitation): Employee name, login credentials, business contact details, IP address, information generated by employees in relation to their use of the services.



SENSITIVE 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.

Not Applicable.

THE FREQUENCY OF THE TRANSFER (E.G. WHETHER THE DATA IS TRANSFERRED ON A ONE-OFF OR CONTINUOUS BASIS)

Ongoing throughout the duration of the agreement.

NATURE OF THE PROCESSING

Storage, consultation, analysis, and disclosure as needed to provide services to Customer.

PURPOSE(S) OF THE DATA TRANSFER AND FURTHER PROCESSING

The Data Importer will process the Personal Data in order to provide the contracted services to the Data Exporter.

THE PERIOD FOR WHICH THE PERSONAL DATA WILL BE RETAINED, OR, IF THAT IS NOT POSSIBLE, THE CRITERIA USED TO DETERMINE THAT PERIOD

The processing shall endure for the term of the Agreement unless the Data Importer is required by law to store Personal Data transferred under these clauses.

FOR TRANSFERS TO (SUB-) PROCESSORS, ALSO SPECIFY SUBJECT MATTER, NATURE AND DURATION OF THE PROCESSING

Same as specified above.

C. COMPETENT SUPERVISORY AUTHORITY

IDENTIFY THE COMPETENT SUPERVISORY AUTHORITY/IES IN ACCORDANCE WITH CLAUSE 13

.....

The competent supervisory authority shall be the supervisory authority which is competent to supervise the activities of the Data Exporter.



Schedule 4

Technical and organizational security measures including technical and organisational measures to ensure the security of the data

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.

A summary of the technical, organisational and physical security measures implemented by the data importer and sub-processor is set out below.

This will be in accordance with the Data Importer's "Corporate Information Security Policy". The Data Importer provides electronic services to the global commodities trading marketplace. The engineering and operations of these services involve the creation, transfer and storage of commercially sensitive data. The Data Importer recognises this responsibility and dedicates significant resources to information security. Policies are used to ensure Data Importer employees have standardised, accountable, documented, and secure guidelines for conducting business. This document summarizes the policies in place at the Data Importer and documents the structure and strategy of these policies.

Network Connectivity

Data transfer will be operated only through the Data Importer's network, a secure VPN connection to the Data Importer's network and the secure connection to the Data Exporter's network.

Procedural Controls

Logical Security

In addition, privileged and non-privileged access to systems and network devices are based upon a documented, approved request. Only authorised users can request logical access to the Data Exporter's environments. A periodic verification is performed in accordance with instructions to determine that the owner of a user ID is still employed and assigned to provide services for the entity issuing the user ID in the service delivery centre. Exceptions identified during the verification process are remediated. An annual business need revalidation is performed to determine that access is commensurate with the user's job function. Exceptions identified during the revalidation process are remediated.

User access to the Data Importer's internal network infrastructure is revoked within 24 hours of termination of employment.

Computer Operations

Job scheduling change requests are tracked and approved in accordance with the agreed process.

Change Management

Changes to the Data Exporter's systems and network devices which are implemented by the Data Importer adhere to the agreed change management process and procedures for handling routine, expedited, emergency, and business as usual changes. Change controls to the production environment may include categorisation of the change risk and applicable back out plans. All approvals must be obtained prior to implementation.



Problem Management

The Data Importer documents and tracks problems implementing the agreed problem management process, procedures and tools. Problem tickets may be populated with problem severity, customer information, date and time problem was identified, reported, symptom description and type of problem; and actions taken to resolve the problem, including date and time action was taken.

Confidentiality Agreement

All employees sign a confidentiality agreement at the start of their employment.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter.

ICE conducts reasonable due diligence and security assessments of Sub-processors, and enters into agreements with Sub-processors that contain provisions similar to or more stringent than those provided for in the Agreement. ICE will work directly with Sub-processors, as necessary, to provide assistance to the Data Exporter.

SCHEDULE 5

C-to-P Transfer Clauses

SECTION I

Clause 1

Purpose and scope

- (a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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)⁽⁶⁾ for the transfer of personal data to a third country.
- (b) The Parties:
- (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I (hereinafter each 'data exporter'), and
 - (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I (hereinafter each 'data importer').

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

- (c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
- (d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

- (a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not

(6) Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.



contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

- (b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

- (a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
 - (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
 - (ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);
 - (iii) Clause 9(a), (c), (d) and (e);
 - (iv) Clause 12(a), (d) and (f);
 - (v) Clause 13;
 - (vi) Clause 15.1(c), (d) and (e);
 - (vii) Clause 16(e);
 - (viii) Clause 18(a) and (b).
- (b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

- (a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
- (b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
- (c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)



The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.

Clause 7 – Optional

[Intentionally left blank.]

SECTION II - OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

- (a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
- (b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data

exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

- (a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
- (b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- (c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.
- (d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union⁽⁷⁾ (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

- (i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- (ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
- (iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- (iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

- (a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
- (b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
- (c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(7) The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

- (d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
- (e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

- (a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least thirty (30) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.
- (b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.⁽⁸⁾ The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
- (c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
- (d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.
- (e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

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

(8) This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

- (b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
- (c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

- (a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.
- (b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
- (c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
 - (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
 - (ii) refer the dispute to the competent courts within the meaning of Clause 18.
- (d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
- (e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
- (f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

- (a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
- (b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

- (c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.
- (d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
- (e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
- (f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.
- (g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

- (a) Where the data exporter is established in an EU Member State, the supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679, the supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679, the supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I, shall act as competent supervisory authority.

- (b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

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

Clause 14

Local laws and practices affecting compliance with the Clauses

- (a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
- (b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
- (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
 - (ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards⁽⁹⁾;
 - (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
- (c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
- (d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(9) As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

- (e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).
- (f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

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

15.1 Notification

- (a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
 - (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
 - (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
- (b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
- (c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

- (d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
- (e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

- (a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).
- (b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.
- (c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

- (a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
- (b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
- (c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
 - (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
 - (ii) the data importer is in substantial or persistent breach of these Clauses; or



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

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

- (d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.
- (e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of The Netherlands.

Clause 18

Choice of forum and jurisdiction

- (a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- (b) The Parties agree that those shall be the courts of The Netherlands.
- (c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
- (d) The Parties agree to submit themselves to the jurisdiction of such courts.



ANNEX I TO SCHEDULE 5

See Schedule 3 to the Additional Terms.



ANNEX II TO SCHEDULE 5

See Schedule 4 to the Additional Terms.

Schedule 6

C-to-P Processing Clauses

1. C-TO-P PROCESSING CLAUSES

- 1.1 For the purposes of this Schedule 6, with respect to the Personal Data transferred by Participant to ICE (the "**Transferred Personal Data**"), Participant is the Controller (or transfers the Transferred Personal Data at the instruction of the Controller) and ICE acts as a Processor.
- 1.2 ICE agrees that it will, acting as a Processor in the provision of the Services:
 - (a) Process the Transferred Personal Data only for the purpose of providing the Services or as otherwise instructed in writing by Participant, and inform Participant if any instruction contradicts any legal requirements to which ICE is subject;
 - (b) keep all Transferred Personal Data confidential as required under the Agreement;
 - (c) ensure that access to Transferred Personal Data shall only be provided to those of its employees, affiliates or service providers who need access to such data for the performance of the Services, and that they will only access Transferred Personal Data in order to provide the Services or in accordance with Participant's instructions;
 - (d) take adequate technical and organizational security measures to safeguard Transferred Personal Data against unauthorised access, destruction, disclosure, transfer, or other improper use;
 - (e) provide Participant access to the Transferred Personal Data which has been provided by Participant to enable Participant to comply with its obligations to Data Subjects exercising their rights under applicable Data Protection Laws. ICE shall refer such Data Subjects to Participant and shall also, at the request of Participant, amend, correct, delete, add to, cease using or restrict the use of Transferred Personal Data relating to such Data Subjects to ensure that their Transferred Personal Data is accurate and complete;
 - (f) promptly notify Participant of any accidental or unauthorised access, destruction, disclosure, transfer or other improper use of Transferred Personal Data that has been supplied by Participant, after ICE becomes aware of any such access, destruction, disclosure, transfer or other improper use, or of any complaints by individuals or third parties that involve or pertain to such Transferred Personal Data, and shall, taking into account the nature of the Processing and the information available to ICE, provide such assistance to Participant as may be reasonable in the circumstances to enable Participant to meet its obligations to notify any competent Supervisory Authority or any other regulatory or governmental authorities or Data Subjects of such event where Participant is required to do so by law;
 - (g) taking into account the nature of the Processing and the information available to ICE, assist Participant in relation to any privacy impact assessments or consultations with competent Supervisory Authorities about the Processing of Transferred Personal Data in the context of the provision of the Services or any inquiry, complaint or claim in relation to the Processing of Transferred Personal Data provided by Participant;



- (h) make available to Participant all information necessary to demonstrate that ICE is in compliance with this clause 1.2;
- (i) audit the adequacy of its security measures used to Process Transferred Personal Data on behalf of Participant, which will: (i) be performed at least annually; (ii) be in accordance with SSAE 16 standards or such alternative standards that are substantially equivalent to SSAE 16; (iii) be performed by third party professionals at ICE's selection and expense; and (iv) result in the generation of an audit report ("**Audit Report**"), which will be ICE's confidential information;
 - (j) contribute to audits by Participant or an auditor designated by Participant, including under the Transfer Clauses if applicable, by providing a confidential summary of the Audit Report ("**Summary Report**") so that Participant can reasonably verify ICE's compliance with the obligations of this clause 1.2, which will be ICE's confidential information; nothing in this clause 1.2(j) varies or modifies the Transfer Clauses nor affects any competent Supervisory Authority's or Data Subject's rights under the Transfer Clauses or Data Protection Laws; and
 - (k) at the termination of the Agreement or these Additional Terms, at Participant's election, delete or return the Transferred Personal Data to Participant.
- 1.3 Participant acknowledges and agrees that ICE may subcontract the provision of the Services to sub-processors (third parties and ICE affiliates) and ICE will make a list of sub-processors Processing Transferred Personal Data for the Services available to the Participant under the data protection disclosure section of ICE's website (<https://www.theice.com/data-protection>), which may be updated from time to time by ICE. ICE will ensure that any such transfers of Transferred Personal Data to sub-processors will be subject to contractual requirements to safeguard Transferred Personal Data equivalent to those set out in clause 1.2, and ICE shall remain liable to Participant for any breaches caused by sub-processors.



SCHEDULE 7

Additional terms for Abu Dhabi Global Market

The following provisions apply to all transfers of Personal Data from Subscriber to ICE subject to Abu Dhabi Global Market laws.

- A. For the avoidance of doubt, “Applicable Laws” includes the Data Protection Regulations 2015, as amended from time to time or any Data Protection Regulations that take their place.



SCHEDULE 8

Additional terms for Australia

The following provisions apply to all transfers of Personal Data from Subscriber to ICE subject to Australian Data Protection Laws.

- B. For the avoidance of doubt, “Applicable Laws” includes the Australian Privacy Act 1988 (Cth), as amended from time to time, including the Australian Privacy Principles or any equivalent privacy principles that take their place.
- C. When collecting, using, disclosing and storing Personal Data provided by or on behalf of Subscriber, ICE must comply with the Australian Privacy Principles.
- D. ICE shall only Process Personal Data for the purposes specified in Schedule 1 and Schedule 3, or as otherwise agreed by Subscriber and ICE.



SCHEDULE 9

Additional terms for Brazil

The following provisions apply to all transfers of Personal Data from Subscriber to ICE subject to Brazilian Data Protection Laws.

- A. For the avoidance of doubt, “Applicable Laws” includes the General Data Protection Law, Brazilian Law 13.709/2018, which came into effect August 2020 and may be amended from time to time, and guidance issued by the Brazilian National Data Protection Agency.
- B. Subscriber shall process Personal Data in compliance with the Brazilian General Data Protection Law, and shall only issue instructions to ICE for processing such Personal Data that comply with the Brazilian General Data Protection Law.
- C. ICE shall carry out the processing of Personal Data according to the instructions provided by Subscriber or as otherwise permitted by Applicable Law.

Subscriber shall transfer Personal Data outside of Brazil in compliance with Chapter V of the Brazilian General Data Protection Law. To the extent transfers of such data are reliant on a transfer mechanism approved by the Brazilian National Data Protection Agency, such as standard contractual clauses, the Parties agree to adopt an approved transfer mechanism to safeguard such transfers in compliance with the Brazilian General Data Protection Law. In the absence of approved transfer mechanisms, ICE commits to provide a standard of protection to Personal Data that is comparable to that which is required of Subscriber in compliance with the Brazilian General Data Protection Law.



SCHEDULE 10

Additional terms for Canada

The following provisions apply to all transfers of Personal Data from Subscriber to ICE subject to Canadian Data Protection Laws.

To the extent that a Subscriber acts as a Controller of Personal Data pertaining to residents of Canada collected under this Agreement ("**Canadian Personal Data**"), and engages in the transfer of the Canadian Personal Data to ICE acting as a Controller of the Canadian Personal Data, the following provisions apply:

- A. ICE shall Process the Canadian Personal Data in accordance with this Agreement and Subscriber shall ensure that adequate notice is provided and appropriate consents are obtained as required by, as applicable, Personal Information Protection Act, SBC 2003, c 63, *Personal Information Protection Act*, SA 2003, c P-6.5 or *An Act respecting the Protection of Personal Information in the Private Sector*, CQLR c P-39.1, as amended or supplemented from time to time, and any similar Canadian federal or provincial legislation now in force or that may in the future come into force governing the protection of personal employee information in the private sector.
- B. ICE shall implement security measures to protect Canadian Personal Data consistent with Schedule 4 of this Agreement.
- C. Both Subscriber and ICE shall comply with all valid requests made by competent legal authorities.
- D. Upon request by Subscriber, ICE shall provide Subscriber with the opportunity to retrieve the Canadian Personal Data.




SCHEDULE 11

Additional terms for Japan

The following provisions apply to all transfers of Personal Data from Subscriber to ICE subject to Japan Data Protection Laws.

- A. For the avoidance of doubt, “Applicable Laws” includes the Act on the Protection of Personal Information (Act No. 57 of 2003, as amended).
- B. ICE shall not Process Personal Data for purposes other than those specified in Schedule 1 and Schedule 3 of these Additional Terms, or as otherwise agreed by the Subscriber and ICE (for the purpose of this section, the “**Utilization Purposes**”) without the prior written consent of the Subscriber. Subscriber represents that it has notified all applicable Data Subjects of the Utilization Purposes to the extent required by Applicable Laws.
- C. ICE and Subscriber agree that Subscriber shall collect all consents from Data Subjects required by Applicable Laws, including without limitation for (1) the collection of any “**Special Care-Required Personal Information**” (as defined by Applicable Laws) and (2) any disclosures of Personal Data made by Subscriber to third parties, subject to Clause G, below.
- D. ICE shall keep the Personal Data accurate and up-to-date within the scope necessary to achieve the Utilization Purposes, and shall delete any Personal Data that becomes unnecessary to achieve a Utilization Purpose or other legitimate business purpose. For the avoidance of doubt, it is not necessary to delete Personal Data where Applicable Laws require ICE to retain it.
- E. ICE shall have in place appropriate technical and organizational measures to protect the Personal Data against accidental or unlawful destruction or accidental loss, leakage, alteration, and unauthorized disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.
- F. ICE shall exercise the necessary and appropriate control and supervision over its officers, employees, and vendors to securely manage the Personal Data received.
- G. ICE shall not disclose Personal Data to any third party except: (i) where such disclosure, transfer or access is mandated by Applicable Law; or (ii) where Subscriber consents to the disclosure of Personal Data to the third party; or (iii) as permitted in Clause H, below. In the event that ICE discloses Personal Data to a third party, ICE shall impose contractual obligations upon the third party that are no less restrictive than the terms set forth in this Agreement.
- H. In the case where ICE entrusts the handling of the Personal Data to a third party pursuant to this Clause H, ICE shall exercise necessary and appropriate control and supervision over the trustees to ensure the safety of such Personal Data, as stated in Clause G above, and ICE shall require the trustees comply with obligations equivalent to ICE’s obligations under the Additional Terms, including the obligations in this Schedule 11. ICE Importers shall be responsible for any breach by the trustees (and any subsequent trustees) of the obligations above. For clarity, this Clause H shall apply to all third party trustees and subsequent third party trustees.

- 
- I. To the extent required by the APPI, upon request of the Data Subject, ICE shall correct, add, or delete certain Personal Data if the Data Subject can show the contents of the Personal Data are incorrect. ICE shall promptly inform the Data Subject if it has corrected, added, or deleted Personal Data, or if it has determined it does not have to do so.
- J. To the extent required by the APPI, upon request of the Data Subject, ICE shall disclose the information on the Personal Data stipulated under the APPI, including (i) the contents of the retained Personal Data; (ii) the name of the Data Importer; (iii) the purpose of use of the Personal Data; (iv) the procedures for responding to a request for the Personal Data; and (v) the contact information Data Subjects should use to make claims regarding the handling of the Personal Data. Each Data Importer shall promptly inform the Data Subject if it has determined it does not have to provide requested information on the contents and/or the purpose of use of the Personal Data.
- K. To the extent required by the APPI, ICE shall delete or stop utilizing the Personal Data if the Data Subject can show that ICE is using or has used such Personal Data outside of the designated Utilization Purposes or has acquired it by improper means; provided, however, that it is not required where it would be unreasonably expensive or unreasonably difficult to do so and where alternative action which would protect the Data Subject's interests can be taken. ICE shall promptly inform the Data Subject if it has deleted or stopped utilizing the Personal Data, or if it has determined it does not have to do so.
- L. To the extent required by the APPI, ICE shall stop providing Personal Data to a third party, if ICE has provided it to a third party in violation of the restrictions related to the provisions of the Personal Data to a third party under the APPI; provided, however, that it is not required where would be unreasonably expensive or unreasonably difficult to do so and where alternative action which would protect the Data Subject's interests can be taken. ICE shall promptly inform the Data Subject if it has stopped providing the Personal Data, or if it has determined it does not have to do so.
- M. If ICE knows or should know that any Personal Data has been or is likely to be leaked, disclosed, accessed, destroyed, altered, lost, used without authorization, or otherwise handled in any way not permitted under the Agreement, regardless of whether or not ICE is liable for such incidents, ICE shall immediately inform Subscriber of the same in writing, and shall take any appropriate measures to prevent such incident from occurring, expanding, and recurring.



SCHEDULE 12

Additional terms for Singapore

The following provisions apply to all transfers of Personal Data from Subscriber to ICE subject to Singapore Data Protection Laws.

- A. For the avoidance of doubt, “Applicable Laws” includes the Personal Data Protection Act 2012 (PDPA), which shall include implementing measures to comply with that Act, as may be amended or supplemented from time to time. Subscriber shall ensure appropriate express consent from Data Subjects has been obtained for the transfer of Personal Data to ICE and/or its subcontractors, unless the purpose of such transfer falls within an exception to the PDPA’s consent requirements (e.g., transfers that are reasonable for the purpose of managing or terminating an employment relationship).



ANNEX C - REMIT SUPPLEMENT TO THE

ICE TRADE VAULT EUROPE PARTICIPANT AGREEMENT

THIS REMIT SUPPLEMENT WILL ONLY APPLY TO PARTICIPANTS THAT HAVE EXECUTED THIS ANNEX C – REMIT SUPPLEMENT TO THE ICE TRADE VAULT EUROPE PARTICIPANT AGREEMENT WITH ICE TRADE VAULT EUROPE LIMITED.

This REMIT Supplement (the “**Supplement**”), shall, effective as of the date below, amend, supplement and form part of the ICE Trade Vault Europe Participant Agreement (the “**ICE European TR Agreement**”) between the participant identified below (the “**Participant**”) and ICE Trade Vault Europe Limited (“**ICE Trade Vault**”).

I. PURPOSE

This Supplement has been published to enable Participant to submit data with respect to Wholesale Energy Contracts (as defined below) to ICE RRM (as defined below) for reporting to the Agency for the Cooperation of Energy Regulators (“**ACER**”) as further described below. Participants are not required to execute this Supplement.

ICE Trade Vault is registered with ACER as a Registered Reporting Mechanism (as defined below). ICE Trade Vault in its capacity as a Registered Reporting Mechanism subject to registration with ACER shall be referred to hereunder as “**ICE RRM**”.

The terms of this Supplement shall apply solely with respect to ICE RRM and the data submitted to ICE RRM by Participant, on Participant’s behalf or via a Reporting Broker (as defined below) in respect of Wholesale Energy Contracts and Fundamental Data. Notwithstanding anything to the contrary in the ICE European TR Agreement, in the event of any inconsistency between the terms of the ICE European TR Agreement and the terms of this Supplement, this Supplement shall prevail with respect to Wholesale Energy Contracts and Fundamental Data and the rights and obligations of the parties in respect thereof.

Unless otherwise specified in this Supplement, all capitalized terms used herein shall have the meanings assigned in the ICE European TR Agreement.

II. ACER SUPPLEMENT TERMS

The ICE European TR Agreement shall be amended and supplemented as follows:

A. Definitions

“**ACER Data**” means the data submitted to ICE RRM by Participant or on Participant’s behalf in respect of a Wholesale Energy Contract or REMIT reportable Fundamental Data and shall replace the term “ICE Europe TR Service Data” wherever used in the ICE European TR Agreement.

“**Applicable Law**” has the meaning assigned to it in the ICE European TR Agreement, including without limitation, REMIT and the Implementing Acts.



“**UK EMIR**” means the UK legislation onshoring the European Market Infrastructure Regulation cited as Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on derivatives, central counterparties and trade repositories.

“**ICE Europe RRM Service**” means the collection, storage and regulatory reporting of data in respect of Wholesale Energy Contracts and Fundamental Data that ICE RRM is approved to offer and shall replace the term “ICE Europe TR Service” wherever used in the ICE European TR Agreement.

“**ICE Trade Vault Europe TR Rulebook**” has the meaning assigned to it in the ICE European TR Agreement as amended to include the REMIT Annex thereto but no other jurisdictional annex and as may otherwise be amended from time to time.

“**Implementing Acts**” means the Commission Implementing Regulation (EU) No 1348/2014 of 17 December 2014 laying down implementing technical standards with regard to data reporting implementing Article 8(2) and Article 8(6) of REMIT.

“**Registered Reporting Mechanism**” or “**RRM**” means a person that reports data on Wholesale Energy Contracts and Fundamental Data directly to ACER under REMIT.

“**REMIT**” means Regulation (EU) No 1227/2011 of the European Parliament and of the Council of 25 October 2011 on wholesale energy market integrity and transparency.

“**Reporting Broker**” means a broker or other third party that has entered into an ICE Trade Vault Europe Reporting Broker Agreement or Trusted Source Agreement with ICE Trade Vault pursuant to which ICE Trade Vault has agreed to provide the Reporting Broker with access to and use of the ICE Trade Vault Europe Platform in connection with the Reporting Broker’s reporting of ACER Data (as appropriate under Applicable Law).

“**Reporting Broker’s Facility**” means the reporting of ACER Data in respect of trading activity occurring in a Reporting Broker’s marketplace.

“**Wholesale Energy Contract**” means a wholesale energy transaction, including matched and unmatched orders to trade, required to be reported to ACER in accordance with the Implementing Acts and excluding any derivatives data with respect to a wholesale energy transaction which is reportable under UK EMIR, has been reported by Participant to ICE Trade Vault and is not being reported to ICE RRM.

“**Fundamental Data**” means the data prescribed in Article 2(1) of REMIT.

B. Additional Terms

1. **Preamble.** The preamble of the ICE European TR Agreement shall be amended by deleting the terms “derivatives trades” in the third line thereof and replacing them with “Wholesale Energy Contracts and Fundamental Data”.

2. **Participant’s Representations, Warranties and Covenants.** Section 3(k) of the ICE European TR Agreement shall be deleted in its entirety and replaced with the following:



“Participant represents that any ACER Data submitted to the ICE Europe RRM Service by Participant or on Participant’s behalf has been submitted in compliance with Applicable Law and that Participant has used due care to ensure the completeness, accuracy and timely submission of such ACER Data. Participant further agrees that it will report any errors or omissions in respect of the ACER Data as soon as practicable after discovery of any such error or omission in accordance with the ICE Trade Vault Europe TR Rulebook”.

3. **Confidentiality.** Section 7(b) of the ICE European TR Agreement shall be amended by deleting the following parenthetical in the fifth line thereof: “(including, without limitation, provisions of Applicable Law that mandate the publication of aggregate trade data)”.

4. **Governing Law.** Section 13 of the ICE European TR Agreement is amended by deleting the second sentence thereof and replacing it with the following: “ICE Trade Vault’s ICE Europe RRM Service is subject to the ACER requirements for the registration of Registered Reporting Mechanisms.”

5. **Whole Agreement.** Section 17 of the ICE European TR Agreement shall be amended by adding the word “applicable” between “any” and “annexes” in the first line thereof.

C. **Reporting Via Reporting Brokers**

The terms in this Section D apply where ACER Data in respect of Participant are reported to ICE Trade Vault by a Reporting Broker.

1) **ACER Data.**

- a) Participant will provide to Reporting Broker all data reasonably requested by Reporting Broker to allow Reporting Broker to conduct the reporting required under the Implementing Acts with respect to Participant’s Wholesale Energy Contracts and Fundamental Data Participant will, subject to Applicable Law, cooperate reasonably with Reporting Broker to allow Reporting Broker to respond to requests from ACER for additional information relating to ACER Data reported by Reporting Broker through the Reporting Broker’s Facility.
- b) Participant agrees that Participant remains solely responsible for the accuracy of all ACER Data reported to ICE Trade Vault via Reporting Broker except to the extent that any such inaccuracy results solely from an act or omission on the part of Reporting Broker. Participant represents and warrants that ACER Data submitted by Participant to Reporting Broker is accurate. Participant agrees that it will take reasonable steps to verify the completeness, accuracy and timeliness of all ACER Data submitted to ICE Trade Vault through the Reporting Broker’s Facility and will report all errors and omissions in ACER Data to Reporting Broker in a timely manner after discovery of such errors or omissions.
- c) Participant will remain liable for any delay in the reporting of ACER Data except to the extent that such delay is due solely to an act or omission on the part of Reporting Broker.
- d) Participant acknowledges that, unless otherwise agreed with Reporting Broker, Reporting Broker will only report orders and initial trade records that occur in Reporting Broker’s marketplace (including historical data as required by the Implementing Acts) and will not report lifecycle data required under Article 7(6) of the Implementing Acts to ICE Trade Vault.



- e) Participant acknowledges and agrees that Reporting Broker may be required to provide ICE Trade Vault with information related to the activities of Participant that is reasonably requested by ICE Trade Vault in order to enable ICE Trade Vault to maintain the integrity of the ICE Europe System or to comply with Applicable Law.
- 2) **Delegation by Reporting Broker.** ICE Trade Vault will procure that Reporting Broker will not delegate its reporting obligations in respect of Participant's ACER Data to any third party (other than an affiliate or legal successor) without the prior written consent of ICE Trade Vault, and ICE Trade Vault will not issue any such consent without the prior written approval of Participant.
- 3) **Reporting by Reporting Brokers; Force Majeure.** Participant agrees that a Reporting Broker will not be held liable for any failure to report ACER Data as a result of any delay, failure in performance, or interruption of service resulting directly or indirectly from acts of God, civil or military authority, civil disturbance, war, strikes, fires, other catastrophes, power failure or any other cause beyond its reasonable control.
- 4) **Termination of Reporting Broker's Facility by ICE Trade Vault.** Participant acknowledges that ICE Trade Vault may, in its sole discretion, immediately and without notice to Participant or Reporting Broker, but subject to compliance with Applicable Law, suspend or terminate Reporting Broker's ability to report ACER Data to ICE Trade Vault through the Reporting Broker's Facility. Participant further acknowledges that ICE Trade Vault may, in its sole discretion, temporarily or permanently cease to provide the ICE Europe RRM Service to Reporting Broker. Participant also acknowledges that Reporting Broker's access to and utilization of the ICE Trade Vault Europe Platform may be monitored by ICE Trade Vault for its own purposes (including, without limitation, for purposes of monitoring levels of activity and for purposes of maintaining the functional and operational integrity of the ICE Europe System and for purposes of complying with Applicable Law). Participant acknowledges that the ICE Trade Vault Europe TR Rulebook available at <https://www.theice.com/technology/post-trade/ice-trade-vault-europe>, sets forth additional terms and conditions under which ICE Trade Vault may temporarily or permanently suspend the ICE Europe RRM Service.
- 5) **LIMITATION OF REPORTING BROKER'S LIABILITY**
 - a) PARTICIPANT ACKNOWLEDGES AND AGREES THAT NEITHER REPORTING BROKER NOR ITS MANAGERS, OFFICERS, AFFILIATES, SUBSIDIARIES, SHAREHOLDERS, EMPLOYEES OR AGENTS MAKE ANY WARRANTY WITH RESPECT TO, AND NO SUCH PARTY SHALL HAVE ANY LIABILITY TO PARTICIPANT (i) FOR THE ACCURACY, TIMELINESS, COMPLETENESS, RELIABILITY, PERFORMANCE OR CONTINUED AVAILABILITY OF THE ICE EUROPE RRM SERVICE, OR (ii) FOR DELAYS, OMISSIONS OR INTERRUPTIONS THEREIN. EXCEPT AS REQUIRED BY APPLICABLE LAW, REPORTING BROKER SHALL HAVE NO DUTY OR OBLIGATION TO PARTICIPANT TO VERIFY ANY INFORMATION SUBMITTED TO OR DISPLAYED VIA THE ICE EUROPE RRM SERVICE. PARTICIPANT ACKNOWLEDGES AND AGREES THAT REPORTING BROKER IS NOT AN ADVISOR OR FIDUCIARY OF PARTICIPANT.
 - b) PARTICIPANT AGREES THAT IN NO EVENT WILL REPORTING BROKER BE RESPONSIBLE OR LIABLE (WHETHER IN CONTRACT, OR TORT (INCLUDING NEGLIGENCE), FOR BREACH OF STATUTORY DUTY OR OTHERWISE) FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, EXEMPLARY, PUNITIVE OR OTHER LOSSES OR DAMAGES (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS, LOSS OF BUSINESS, USE, DATA OR OTHER INTANGIBLE



DAMAGES OR OTHERWISE) EVEN IF IT HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

- c) THE LIMITATIONS AND EXCLUSIONS OF LIABILITY SET OUT HEREIN SHALL NOT APPLY TO LIABILITY FOR: (I) DEATH OR PERSONAL INJURY CAUSED BY REPORTING BROKER'S NEGLIGENCE; (II) FRAUD OR FRAUDULENT MISREPRESENTATION; OR (III) ANY OTHER LIABILITY THAT CANNOT BE EXCLUDED OR LIMITED BY APPLICABLE LAW.

6) **THIRD PARTY RIGHTS**

- a) Subject to clause b) below, a person who is not a party to this Supplement has no right under the Contracts (Rights of Third Parties) Act 1999 or otherwise to enforce any term of this Supplement.
- b) All agreements, acknowledgments, representations and warranties made or given by Participant in this Supplement are made and given for the express benefit of ICE Trade Vault and Reporting Broker, and Participant acknowledges that such agreements, acknowledgments, representations and warranties are a material inducement to Reporting Broker to offer its Reporting Broker's Facility to Participant.
- c) The parties to this Supplement do not require the consent of any third party to rescind or vary this Supplement at any time.
- d) Participant agrees that ICE Trade Vault may confirm to Participant's Reporting Broker that Participant has agreed to the above provisions with respect to the Reporting Broker's Facility.



Date: _____, 20__

PARTICIPANT:

[Insert Participant's Full Legal Company Name Below]

ICE Trade Vault Europe Limited

5th Floor, Milton Gate, 60 Chiswell Street Address: _____

London EC1Y 4SA _____

United Kingdom

Signature: _____

Signature: _____

Name: Stuart Williams

Name: _____

Title: Executive Director

Title: _____



ANNEX D - ICE eCONFIRM® TRADE VAULT REPORTING CONNECTIVITY

The ICE eConfirm Trade Vault Reporting Connectivity, as further described in Section 1(a) below, is provided by Intercontinental Exchange Holdings, Inc. ("ICE"), an affiliate of ICE Trade Vault, independently of the ICE Europe TR Service, and will be provided to Participants who have (i) entered into a separate agreement with ICE eConfirm, LLC governing Participant's use of ICE eConfirm's electronic platform for the matching of previously executed trades with other participants, and the matching of Trade data with a third party responsible for arranging the Trade, collectively known as the ICE eConfirm Service (the "ICE eConfirm Agreement"), and (ii) executed this ICE Trade Vault Agreement, which includes this Annex D.

This Annex D (a) addresses Participant's access to additional functionality available within the ICE eConfirm Service for the purpose of submitting Participant's ICE eConfirm Service Data to the ICE Europe TR Service, and (b) authorizes ICE to provide the Participant's ICE eConfirm Service Data to ICE Trade Vault in connection with the ICE Europe TR Service. This Annex D supplements the ICE Trade Vault Agreement as well as the ICE eConfirm Agreement by setting forth the terms governing Participant's use of and access to the ICE eConfirm Trade Vault Reporting Connectivity. Unless amended in this Annex D, all terms and conditions contained in the ICE eConfirm Agreement shall remain in effect.

Defined terms used herein but not otherwise defined herein shall have the same meaning set forth elsewhere in this ICE Trade Vault Agreement. In the event of a conflict between this ICE Trade Vault Agreement and the ICE eConfirm Agreement, with respect to Participant's use of and access to the ICE eConfirm Trade Vault Reporting Connectivity only, the terms and conditions of this ICE Trade Vault Agreement shall prevail.

1. ICE'S PROVISION OF TRADE VAULT REPORTING CONNECTIVITY

- a. ICE eConfirm Trade Vault Reporting Connectivity Definition. "ICE eConfirm Trade Vault Reporting Connectivity" means ICE's proprietary connectivity and electronic messaging system that provides two-way communication of ICE eConfirm Service Data in respect of certain trade data to ICE Trade Vault for the purpose of meeting a Participant's regulatory reporting obligations as required under Applicable Law. The term "ICE eConfirm Trade Vault Reporting Connectivity" includes all written documentation and specifications provided to Participant related thereto.
- b. Subject to Participant's compliance with the terms of the (i) ICE Trade Vault Agreement (including this Annex D), as it relates to the use of the ICE Europe TR Service, and (ii) ICE eConfirm Agreement, as it relates to Participant's use and access to the ICE eConfirm Service, Participant may access and use the ICE eConfirm Trade Vault Reporting Connectivity functionality in order to submit ICE eConfirm Service Data to the ICE Europe TR Service. Participant may use the ICE eConfirm Trade Vault Reporting Connectivity solely in connection with the ICE Europe TR Service.

2. DISCLAIMER OF WARRANTIES; LIMITATION OF LIABILITY; INDEMNITY

- a. PARTICIPANT ACKNOWLEDGES, UNDERSTANDS AND ACCEPTS THAT NEITHER ICE NOR ICE TRADE VAULT MAKES ANY WARRANTY WHATSOEVER TO PARTICIPANT AS TO THE ICE eCONFIRM TRADE VAULT REPORTING CONNECTIVITY, EXPRESS OR IMPLIED, AND THAT THE ICE eCONFIRM TRADE VAULT REPORTING CONNECTIVITY IS PROVIDED ON AN "AS IS" BASIS AT PARTICIPANT'S SOLE RISK. BOTH ICE AND ICE TRADE VAULT EXPRESSLY DISCLAIM ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A

PARTICULAR PURPOSE. ICE, ICE TRADE VAULT AND THEIR RESPECTIVE MANAGERS, OFFICERS, AFFILIATES, SUBSIDIARIES, SHAREHOLDERS, EMPLOYEES OR AGENTS MAKE NO WARRANTY WITH RESPECT TO, AND NO SUCH PARTY SHALL HAVE ANY LIABILITY TO PARTICIPANT FOR, (i) THE ACCURACY, TIMELINESS, COMPLETENESS, RELIABILITY, PERFORMANCE OR CONTINUED AVAILABILITY OF THE ICE eCONFIRM TRADE VAULT REPORTING CONNECTIVITY, OR (ii) DELAYS, OMISSIONS OR INTERRUPTIONS THEREIN. ICE SHALL HAVE NO DUTY OR OBLIGATION TO VERIFY ANY INFORMATION SUBMITTED TO OR DISPLAYED VIA THE ICE EUROPE TR SERVICE. PARTICIPANT ACKNOWLEDGES AND AGREES THAT ICE IS NOT AN ADVISOR OR FIDUCIARY OF PARTICIPANT. WITHOUT LIMITATION OF THE FOREGOING, PARTICIPANT ACKNOWLEDGES, AGREES AND ACCEPTS THAT ICE SHALL HAVE NO LIABILITY OR RESPONSIBILITY WHATSOEVER FOR ANY MATTERS RELATED TO PARTICIPANT'S RELATIONSHIP OR DEALINGS WITH ICE TRADE VAULT, INCLUDING BUT NOT LIMITED TO THE ACCURACY OF ANY INFORMATION SUBMITTED BY ICE ON THE PARTICIPANT'S BEHALF TO ICE TRADE VAULT IN CONNECTION WITH PARTICIPANT'S USE OF THE ICE EUROPE TR SERVICE, ALL OF WHICH SHALL BE THE SOLE RESPONSIBILITY OF PARTICIPANT.

- b. TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, NEITHER ICE NOR ICE TRADE VAULT SHALL BE RESPONSIBLE OR LIABLE FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, EXEMPLARY, PUNITIVE OR OTHER LOSSES OR DAMAGES (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS, LOSS OF BUSINESS, USE, DATA OR OTHER INTANGIBLE DAMAGES, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES), WHETHER ARISING OUT OF BREACH OF CONTRACT, TORT (INCLUDING, WITHOUT LIMITATION, NEGLIGENCE AND STRICT LIABILITY) OR OTHER LEGAL THEORY, HOWSOEVER CAUSED, ARISING OUT OF OR RELATING IN ANY WAY TO ICE eCONFIRM TRADE VAULT REPORTING CONNECTIVITY AND/OR PARTICIPANT'S USE OF, OR INABILITY TO USE, OR RELIANCE ON, THE ICE eCONFIRM TRADE VAULT REPORTING CONNECTIVITY.
- c. With respect to Participant's use of the ICE eConfirm Trade Vault Reporting Connectivity, Participant agrees that it shall indemnify, protect, and hold harmless ICE, its directors, officers, affiliates, employees and agents, from and against any and all losses, liabilities, judgments, suits, actions, proceedings, claims, damages, or costs (including attorneys' fees) resulting from or arising out of any act or omission by any person obtaining access to the ICE eConfirm Trade Vault Reporting Connectivity (other than through the fault or negligence of ICE), whether or not Participant has authorized such access.
- d. Participant acknowledges and agrees that any and all information submitted by Participant to ICE Trade Vault utilizing the ICE eConfirm Trade Vault Reporting Connectivity may be disclosed to applicable regulators or other entities, including but not limited to relevant derivatives clearing organizations, as reasonably necessary to satisfy applicable regulatory reporting obligations.
- e. Notwithstanding the terms of Section 2(a), in no event shall ICE's aggregate liability to the Participant or any other person or entity for damages under any provision of this Annex D, and regardless of the form of action, whether arising out of or related to breach of contract, tort (including negligence) or otherwise, exceed ten thousand dollars (\$10,000). The foregoing limitations shall apply even if the Participant's remedies under this Annex D fail of their essential purpose.



3. **TERMINATION.**

Termination of this ICE Trade Vault Agreement shall automatically terminate Participant's access to the ICE eConfirm Trade Vault Reporting Connectivity.

5. **DISPUTE RESOLUTION.** Any dispute, controversy or claim (or any and every type, whether based on contract, tort, statute, regulation or otherwise) arising out of, in relation to or in connection with the ICE eConfirm Trade Vault Reporting Connectivity shall be resolved in accordance with clause 14 (Arbitration) of this ICE Trade Vault Agreement.

6. **ICE AS THIRD PARTY BENEFICIARY.** Participant acknowledges and agrees that ICE is a third party beneficiary of the terms of this Annex D.



ANNEX E - ETD UK EMIR TRADE REPORTING SERVICE

The ETD UK EMIR Trade Reporting Service, as further described in section 1(a) below, is provided by ICE Trade Vault to Participants who have elected to receive the service and executed this Annex E to the ICE European TR Agreement.

This Annex supplements and amends the ICE European TR Agreement by setting forth certain additional terms governing Participant's use of and access to the ETD UK EMIR Trade Reporting Service (as defined below).

Defined terms used but not otherwise defined herein shall have the same meaning as set forth elsewhere in the ICE European TR Agreement. Notwithstanding anything to the contrary in the ICE European TR Agreement, in the event of any inconsistency between the terms of the ICE European TR Agreement and the terms of this Annex E, this Annex E shall prevail with respect to the ETD UK EMIR Trading Reporting Service and the rights and obligations of the parties in respect thereof.

1. PROVISION OF UK EMIR TRADE REPORTING SERVICE

- a. ETD UK EMIR Trade Reporting Service Definition. "ETD UK EMIR Trade Reporting Service" means the service offering forming part of the ICE Europe TR Service which provides communication of ETD UK EMIR Trade Reporting Service Data (as defined below) to ICE Trade Vault for collection, storage and regulatory reporting purposes in order to satisfy a Participant's [(and, where applicable, its customers')] regulatory reporting obligations as set forth in Article 9(1) of the European Markets and Infrastructure Regulation ("UK EMIR").
- b. ETD UK EMIR Trade Reporting Service Data Definition. "ETD UK EMIR Trade Reporting Service Data" means all required trade, counterparty and common data for futures and options trades executed on, or pursuant to the rules of, ICE Futures Europe ("IFEU") or ICE Endex Markets B.V. ("ICE Endex")(together, the "Exchanges" and each an "Exchange") by a Participant [(and, where applicable, its customers)] with a reporting obligation under UK EMIR which are made available to ICE Trade Vault in accordance with the ICE European TR Agreement (including this Annex E). For the avoidance of doubt, ETD UK EMIR Trade Reporting Service Data shall be ICE Europe TR Service Data for the purposes of the ICE European TR Agreement.
- c. A Participant that wishes to receive the ETD UK EMIR Trade Reporting Service shall, in addition to executing the ICE European TR Agreement and this Annex E, submit an service election form to ICE Trade Vault in the form and manner prescribed from time to time and notified by ICE Trade Vault to Participants via circular or other form of notification ("Service Election Form"). Submission of the Service Election Form to ICE Trade Vault authorizes the the ETD UK EMIR Trade Reporting Service Data relevant to that Participant (and, if applicable, its customers) to be made available to ICE Trade Vault in connection with the provision of the ETD UK EMIR Trading Reporting Service and to satisfy the aforementioned reporting obligations.

2. PARTICIPANT'S REPRESENTATIONS, WARRANTIES AND COVENANTS.

- a. Participant represents and warrants to ICE Trade Vault that, where applicable, Participant has been duly granted authority enabling it to act on each client's behalf pursuant to this Annex E, and has full power and legal authority, on each client's behalf and for each client's account, to use the ETD UK EMIR Trade Reporting Service and to accept this Annex E.

3. **DISCLAIMER OF WARRANTIES; LIMITATION OF LIABILITY; INDEMNITY**

- a. PARTICIPANT ACKNOWLEDGES, UNDERSTANDS AND AGREES THAT NEITHER ICE TRADE VAULT NOR ANY EXCHANGE MAKES ANY WARRANTY WHATSOEVER TO PARTICIPANT AS TO THE ETD UK EMIR TRADE REPORTING SERVICE, EXPRESS OR IMPLIED, AND THAT THE ETD UK EMIR TRADE REPORTING SERVICE IS PROVIDED ON AN “AS IS” BASIS AT PARTICIPANT’S SOLE RISK. EACH OF ICE TRADE VAULT AND THE EXCHANGES EXPRESSLY DISCLAIM ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. NEITHER ICE TRADE VAULT NOR ANY EXCHANGE, NOR ANY OF THEIR RESPECTIVE MANAGERS, OFFICERS, AFFILIATES, SUBSIDIARIES, SHAREHOLDERS, EMPLOYEES OR AGENTS, MAKES ANY WARRANTY WITH RESPECT TO, AND NO SUCH PARTY SHALL HAVE ANY LIABILITY TO PARTICIPANT FOR, (i) THE ACCURACY, TIMELINESS, COMPLETENESS, RELIABILITY, PERFORMANCE OR CONTINUED AVAILABILITY OF THE ETD UK EMIR TRADE REPORTING SERVICE, OR (ii) DELAYS, OMISSIONS OR INTERRUPTIONS THEREIN. NEITHER ICE TRADE VAULT NOR ANY EXCHANGE SHALL HAVE ANY DUTY OR OBLIGATION TO VERIFY ANY INFORMATION SUBMITTED TO OR DISPLAYED VIA OR IN CONNECTION WITH THE ETD UK EMIR TRADE REPORTING SERVICE. PARTICIPANT ACKNOWLEDGES AND AGREES THAT EACH OF ICE TRADE VAULT AND THE EXCHANGES IS NOT AN ADVISOR OR FIDUCIARY OF PARTICIPANT. WITHOUT LIMITATION OF THE FOREGOING, PARTICIPANT ACKNOWLEDGES, AGREES AND ACCEPTS THAT NEITHER ICE TRADE VAULT NOR ANY EXCHANGE SHALL HAVE ANY LIABILITY OR RESPONSIBILITY WHATSOEVER FOR ANY MATTERS RELATED TO PARTICIPANT’S RELATIONSHIP OR DEALINGS WITH ICE TRADE VAULT OR THE EXCHANGES, INCLUDING BUT NOT LIMITED TO THE ACCURACY OF ANY INFORMATION MADE AVAILABLE, OR CAUSED TO BE MADE AVAILABLE, TO ICE TRADE VAULT ON PARTICIPANT’S INSTRUCTION BY THE EXCHANGES OR ONE OR MORE OF THEIR AFFILIATES, IN CONNECTION WITH PARTICIPANT’S USE OF THE ETD UK EMIR TRADE REPORTING SERVICE, ALL OF WHICH SHALL BE THE SOLE RESPONSIBILITY OF PARTICIPANT.
- b. TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, NEITHER ICE TRADE VAULT NOR ANY EXCHANGE SHALL BE RESPONSIBLE OR LIABLE FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, EXEMPLARY, PUNITIVE OR OTHER LOSSES OR DAMAGES (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS, LOSS OF BUSINESS, USE, DATA OR OTHER INTANGIBLE DAMAGES, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES), WHETHER ARISING OUT OF BREACH OF CONTRACT, TORT (INCLUDING, WITHOUT LIMITATION, NEGLIGENCE AND STRICT LIABILITY) OR OTHER LEGAL THEORY, HOWSOEVER CAUSED, ARISING OUT OF OR RELATING IN ANY WAY TO THE ETD UK EMIR TRADE REPORTING SERVICE.
- c. With respect to Participant’s use of the ETD UK EMIR Trade Reporting Service, Participant agrees that it shall indemnify, protect, and hold harmless each of ICE Trade Vault and the Exchanges, and their respective directors, officers, affiliates, employees and agents, from and against any and all losses, liabilities, judgments, suits, actions, proceedings, claims, damages, or costs (including attorneys’ fees) resulting from or arising out of any act or omission by any person obtaining access to the ETD UK EMIR Trade Reporting



Service (other than through the fault or negligence of ICE Trade Vault or any Exchange), whether or not Participant has authorized such access.

- d. Participant acknowledges and agrees that any and all information submitted by Participant to ICE Trade Vault utilizing the ETD UK EMIR Trade Reporting Service may be disclosed to applicable regulators or other entities, including but not limited to relevant derivatives clearing organizations, as reasonably necessary to satisfy, or otherwise in connection with, applicable regulatory reporting obligations.
- e. Notwithstanding the terms of section 3(a), in the event that ICE Trade Vault is determined to be liable to Participant for any cause arising out of or in any way related to the ETD UK EMIR Trade Reporting Service, Participant expressly agrees that ICE Trade Vault's aggregate liability, for all causes of action (whether in contract, or tort (including negligence), for breach of statutory duty, or otherwise), will not exceed the total fees and other amounts (excluding any applicable taxes or duties) paid to ICE Trade Vault by Participant in respect of the provision of the ETD UK EMIR Trade Reporting Service in the previous six months from the date of the occurrence of the liability.

4. **TERMINATION.**

Termination of the ICE European TR Agreement in accordance with section 5 of that agreement shall automatically terminate Participant's access to the ETD UK EMIR Trade Reporting Service under this Annex E.

5. **DISPUTE RESOLUTION.**

Any dispute, controversy or claim (or any and every type, whether based on contract, tort, statute, regulation or otherwise) arising out of, in relation to or in connection with the ETD UK EMIR Trade Reporting Service shall be resolved in accordance with clause 14 (Arbitration) of the ICE European TR Agreement.

6. **IFEU AND ICE ENDEX AS THIRD PARTY BENEFICIARIES.**

Participant acknowledges and agrees that each of IFEU and ICE Endex is a third party beneficiary of the terms of this Annex E.

In consideration of the mutual covenants and agreements set forth herein and for other good and valuable consideration (the receipt and sufficiency of which are hereby acknowledged), the parties below covenant and agree to the terms set out in the ICE European TR Agreement as supplemented and amended by this Annex E.



Date: _____, 20__

ICE Trade Vault Europe Limited

Signature: _____

Name:

Title:

Signature:

Name:

Title:

Signed on behalf of [Participant Full Legal Company Name]

Signature:

Name:

Title:

Participant Legal Entity Identifier: