REMIT Rulebook

ICE Trade Vault Europe

3 November 2021

Version History

Version	Date	Description of change
1.0	19 December 2017	Clarification as to how user IDs and passwords are issued.
2.0	25 May 2018	Update to paragraph 8 - Data Confidentiality; Sensitive Information and Security
3.0	26 November 2020	Update to Key Terms & Definitions to include references to: ICE EMIR Data File Service, Transition Period, and Withdrawal Agreement Update to paragraph 2.4 - System Availability and Support; Hours of Operation Update to paragraph 3.1.4 to include provisions relating to the transfer of data in relation to Brexit
4.0	3 November 2021	V1 Remit Annex copied from TR rules to constitute free-standing REMIT Rulebook

Table of Contents

1 **KEY TERMS & DEFINITIONS** **5**

2 **GENERAL PROVISIONS** **6**

Overview of Regulatory Requirements 6
2.1 ICE RRM Rules; Conflicts with Applicable Law 7
2.2 System Availability and Support; Hours of Operation 7
2.3 Service, Commitment and Continuity 7
2.4 ICE RRM Service Pricing 7
2.5 Emergency Authority 7
2.5.1 Authority *7*
2.5.2 Circumstances Requiring Invocation of Emergency Authority *8*
2.5.3 Emergency Authority Procedures *8*
2.6 Violations 9
2.6.1 Jurisdiction *9*
2.6.2 Board of Directors' Powers *10*
2.6.3 Notice of Action; Right to Hearing *10*
2.6.4 Hearing on Alleged Violation; Failure to Request Hearing Deemed Acceptance of Alleged Violation. *10*
2.6.5 Liability for Expenses *10*
2.6.6 Effective Date of Remedial Actions *11*
2.7 Conflicts of Interest 11
2.7.1 Definitions *11*
2.7.2 Prohibition *11*
2.7.3 Disclosure *12*
2.7.4 Procedure and Determination *12*

3 **ACCESS, CONNECTIVITY AND SAFE GUARDING OF DATA** **12**

3.1 [Reserved] 12
3.1.1 ICE RRM Service Participant and Trusted Source Access *12*
3.1.2 [Reserved] *12*
3.1.3 Reporting to ACER *12*
3.1.4 Third-Party Service Providers; Transparency About Access *12*
3.2 Revocation of Access 13
3.3 Reinstatement of Access; Revocation or Modification of Other Actions; Termination of Status 13
3.4 Connectivity 13

4 **ACCEPTANCE OF DATA AND REPORTING PROCEDURES** **14**

4.1 Asset Classes 14
4.2 Trade Data and Data Processing 14
4.2.1 General *14*
4.2.2 Participants and Trusted Sources *14*
4.2.3 Wholesale Energy Market Data *14*
4.2.4 [Reserved] *15*
4.2.5 ICE RRM Non-Standard Contract Data *15*
4.3 Data Translation and Default Data 15
4.4 Trade Status 15
4.5 No Invalidation or Modification of Valid Derivative Contract Data 16
4.6 Correction of Errors in Trade Records 16

4.7 DUTY TO COLLECT AND MAINTAIN DERIVATIVE CONTRACT DATA 16
5 **UNIQUE IDENTIFIERS 16**
5.1 UNIQUE TRADE IDENTIFIERS (UTIS) 16
5.2 LEGAL ENTITY IDENTIFIERS (LEIS) 16
5.3 UNIQUE PRODUCT IDENTIFIERS (UPIS) 16
5.3.1 Creating New UPIs 17
6 **DATA RETENTION; BUSINESS CONTINUITY 17**
6.1 DATA RETENTION, ACCESS AND RECORDKEEPING 17
6.2 LEGAL ENTITY IDENTIFIERS (LEIS) OR ACER CODES 18
6.3 OUTSOURCING ICE RRM SERVICE FUNCTIONS 18
7 **DATA CONFIDENTIALITY; SENSITIVE INFORMATION AND SECURITY 18**

ICE Trade Vault Europe REMIT Rulebook

1 Key Terms & Definitions

- ACER Code: means a numerical unique identifier assigned by ACER to a wholesale energy market participant which registers with a National Regulatory Authority.
- API: application programming interface.
- Applicable Law: Any and all applicable national, federal, supranational, state, regional, provincial, local or other governmental statute, law, ordinance, regulation, rule, directive, technical standard , code, guidance, order, published practice or concession, judgment or decision as amended from time to time, and shall include for the avoidance of doubt REMIT.
- Applicable REMIT ITS:

  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 (or the "Implementing Acts").
- Appointed Reporting Entity: A third party to which a Participant or Trusted Source has delegated the reporting of certain details of derivative contracts pursuant to Applicable Law.
- Article 5 Information: The information set forth in Article 5 of the Implementing Acts.
- GLEIF: The Global Legal Entity Identifier Foundation.
- ICE: Intercontinental Exchange, Inc., a publicly traded company.
- ICE eConfirm Service: The electronic platform utilised by Participants and Trusted Sources to report Wholesale Energy Market data to the ICE RRM Service.
- ICE RRM Service: means the collection, storage and regulatory reporting of Wholesale Energy Market Data in respect of Wholesale Energy Contracts that ICE RRM is approved by ACER to offer.
- ICE Trade Vault Europe: ICE Trade Vault Europe Limited.
- Internal Policies and Procedures: The internal policies and procedures in place from time to time of ICE Trade Vault Europe, including but not limited to those relating to compliance, risk, conflicts of interest, controls, internal and external audits, ethics, and internal and external reporting, reasonably designed to prevent violations of Applicable Law by ICE Trade Vault Europe or by its managers and employees.
- Legal Entity Identifier ("LEI"): As defined in the Applicable Law, the assigned code used for unique identification of a counterparty to any derivative contract.
- Lifecycle Event Data: has the meaning assigned to that term in Rule 4.2.3 of the Rulebook.
- National Regulatory Authority: means a European Union Member State national energy regulator.
- Organised Market Place: has the meaning assigned to that term in Article 2(4) of the Implementing Acts.

- Participant: An entity that has validly enrolled in the ICE RRM Service with ICE Trade Vault Europe through a duly executed Participant Agreement in effect with ICE Trade Vault Europe.
- Registered Reporting Mechanism: A person that reports data on wholesale energy products directly to ACER under REMIT, as that term is defined in paragraph 3 of the RRM Requirements.
- Regulator: ACER and any relevant National Regulatory Authority.
- REMIT: Regulation (EU) No 1227/2011 of 25 October 2011 of the European Parliament and of the Council on wholesale energy market integrity and transparency.
- RRM Requirements: the ACER requirements for the registration of Registered Reporting Mechanisms.
- Rulebook: This ICE Trade Vault Europe REMIT Rulebook, as amended from time to time.
- RRM Information: As defined in the Applicable Law, any information that ICE Trade Vault Europe receives from Participants or maintains on their behalf, as part of the ICE RRM Service.
- Trusted Source: An Appointed Reporting Entity that has a duly executed Trusted Source Agreement in effect with ICE Trade Vault Europe.
- Unique Product Identifier ("UPI"): As defined in the Applicable Law, the assigned distinctive code used for categorisation of derivative contracts with respect to the underlying products referenced therein.
- Unique Trade Identifier ("UTI"): As defined in the Applicable Law, the distinctive code created and assigned to a derivative contract.
- "Wholesale Energy Contract": 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 EMIR and has been reported by Participant to ICE Trade Vault.
- Wholesale Energy Market Data: The data submitted to ICE RRM by Participant or Trusted Source in respect of Wholesale Energy Contracts and data relating to wholesale energy products reported to ICE Trade Vault Europe in accordance with Article 5 of the Implementing Acts.

2 General Provisions

Overview of Regulatory Requirements

The Implementing Acts require that all Article 5 Information concerning orders or trades in a Wholesale Energy Contract (or any modification or termination) is reported by a RRM to ACER. A RRM is required to register with ACER, comply with REMIT, the Implementing Acts, the RRM Requirements and other Applicable Law.

A RRM also interacts directly with a range of market participants and is required to engage in the following core duties: (i) ensure the security, confidentiality and completeness of information; (ii) enable the identification and correction of errors in data reports; (iii) enable the authentication of the source of information; and (iv) ensure business continuity.

2.1 ICE RRM Rules; Conflicts with Applicable Law

The rules of the ICE RRM Service consist of this REMIT Rulebook and all other documents incorporated by reference into this REMIT Rulebook. Any Applicable Law affecting (i) the duties or obligations of ICE RRM or (ii) the performance of any Participant or Trusted Source shall take precedence over the rules of the ICE RRM Service. In the event of a conflict between Applicable Law and the rules of the ICE RRM Service, Applicable Law shall prevail.

This REMIT Rulebook is the RRM Rulebook referred to in recent versions of the Trade Vault Participant Agreement. In earlier versions of the Trade Vault Participant Agreement it was referred to as the REMIT Annex to the ICE Trade Vault Europe TR Rulebook. It has since been re-drafted into standalone format, but references in the earlier agreements to the REMIT Annex now should be read as references to this RRM Rulebook.

2.2 System Availability and Support; Hours of Operation

ICE Trade Vault Europe reserves the right to take the services offline, only if necessary, between the hours of 11:00 PM London time and 6:00 AM London time on any weekday and from 11:00 PM London time on Friday through 3:00 AM London time on Monday, if more extensive maintenance or upgrades are necessary. ICE Trade Vault Europe will provide Participants with advanced notice of any scheduled maintenance. All data submitted during systemdown time is stored and processed once the service has resumed.

The ICE Trade Vault Europe help desk is available to receive customer calls in London from 8:00 AM London time to 6:00 PM London time, Monday through Friday, on all local business days, and in Atlanta, Georgia from 8:00 AM ET to 6:00 PM ET, on all local business days.

To reach the help desk, contact: TradeVaultSupport@theice.com or +44 (0)20 7488 5100 in London or 1.770.738.2102 in Atlanta.

2.3 Service, Commitment and Continuity

ICE Trade Vault Europe shall notify all Participants and Trusted Sources using the ICE RRM Service of its intention to cease operation of the ICE RRM Service for any reason at least three months in advance or, if ICE Trade Vault Europe intends to cease operations in fewer than three months, as soon as practicable.

2.4 ICE RRM Service Pricing

Any fees or charges imposed by ICE RRM in connection with the ICE RRM Service shall be equitable. Fees or charges shall not be used as an artificial barrier to access to the ICE RRM Service. Details of fees and charges imposed by ICE RRM in connection with the ICE RRM Service can be found at www.icetradevault.com.

2.5 Emergency Authority

2.5.1 Authority

As part of its Internal Policies and Procedures, ICE Trade Vault Europe maintains a business continuity policy and disaster recovery plan to ensure maintenance of its functions, systems and the ICE RRM Service, and to enable as far as possible the timely recovery of operations and back up facilities if necessary in the event of a loss or disruption of critical functions relating to the ICE RRM Service. However, in an emergency situation, it may not always be possible to maintain the ICE RRM Service and/or functions and systems.

ICE Trade Vault Europe retains the authority to determine, in its sole discretion and in accordance with the provisions of this Rulebook, whether an emergency exists with respect to or otherwise threatens the ICE RRM Service (an "Emergency") and whether emergency action is warranted to mitigate such circumstances. ICE Trade Vault Europe may also exercise emergency authority if ordered to do so by any regulatory agency of competent jurisdiction.

2.5.2 Circumstances Requiring Invocation of Emergency Authority

Circumstances requiring the invocation of emergency authority include: (i) any occurrence or circumstance which ICE Trade Vault Europe determines to constitute an Emergency; (ii) any "Physical Emergency" (such as a fire or other casualty, bomb threats, terrorist acts, substantial inclement weather, power failures, communications breakdowns, computer system breakdowns, or transportation breakdowns); (iii) any occurrence or circumstance which threatens or may threaten the proper functionality of the ICE RRM Service; (iv) any occurrence or circumstance which may materially affect the performance of the ICE Trade Vault Europe systems; (v) any action taken by any governmental body or any Regulator, Trusted Source or Participant which may have a direct impact on the ICE Trade Vault Europe systems or the ICE RRM Service; and (vi) any other circumstance which may impact ICE Trade Vault Europe in a materially adverse manner.

2.5.3 Emergency Authority Procedures

If the Executive Director, or any individual designated by the Executive Director or the Board of Directors (or otherwise in accordance with the Internal Policies and Procedures (including, but not necessarily limited to the business continuity policy and disaster recovery plan)), determines that an Emergency has arisen, the Executive Director or such designee, as the case may be, may, consistent with Internal Policies and Procedures (including, but not necessarily limited to, the business continuity policy and disaster recovery plan), and in consultation with the CCO and the Board of Directors where possible, declare an Emergency with respect to the ICE RRM Service or the systems and facilities of ICE Trade Vault Europe and take or place into immediate effect a temporary emergency action or rule. Any such action or rule may remain in effect for up to 30 business days, after which time it must be approved by the Board of Directors to remain in effect. The CCO will be consulted, where possible, in terms of the implementation of any emergency action or rule or any decision approving or disapproving the ongoing effectiveness of such action or rule. Any such action or rule may provide for, or may authorise ICE Trade Vault Europe, the Board of Directors or any committee thereof to undertake, actions deemed necessary or appropriate by the Executive Director or any designee to respond to the Emergency, including, but not limited to, the following:

- modifying or suspending any relevant provision of the ICE RRM Service rules;
- extending, limiting or changing the operating hours of the ICE RRM Service; or
- temporarily limiting or denying access to the ICE RRM Service, including access to any relevant ICE Trade Vault Europe system or facilities.

Any such action placed into effect in accordance with the preceding paragraph may be reviewed by the Board of Directors at any time and may be revoked, suspended or modified by the Board of Directors.

If, in the judgment of the Executive Director, or any designee, as appropriate, the physical functions of the ICE RRM Service are, or are threatened to be, materially adversely affected by a Physical Emergency, such person may take any action that he or she may deem necessary or appropriate to respond to such Physical Emergency, in consultation, where possible, with the CCO, including suspending the ICE RRM Service.

In the event the Emergency that gave rise to such action or rule has, in the view of the Executive Director, or any designee, as appropriate (in consultation with the CCO and the Board of Directors where possible and consistent with the Internal Policies and Procedures), sufficiently abated to permit the ICE RRM Service and/or its systems and facilities to operate again in an orderly manner, such action or rule may be ceased or removed upon determination by the Executive Director, or designee, as appropriate; provided that any cessation or removal pursuant to this paragraph will be subject to review, and may be subject to modification or reversal by the Board of Directors, in consultation, where possible, with the CCO.

ICE Trade Vault Europe will notify Participants and Trusted Sources via an appropriate email address as provided by Participant or Trusted Sources from time to time, or such other means of communication as is possible, as soon as practicable of any action taken or implemented, or proposed to be taken or implemented, pursuant to this paragraph.

2.6 Violations

2.6.1 Jurisdiction

ICE Trade Vault Europe retains the authority to conduct investigations and take action in respect of any violations of this Rulebook ("Violations") committed by Participants and Trusted Sources as provided in this paragraph 2.6.

CCO Powers and Duties

The CCO is responsible for enforcing the rules set forth in this paragraph 2.6 and he or she shall have the authority to inspect the books and records of all Participants or Trusted Sources that are reasonably relevant to any investigation carried out pursuant to this Rule 2.6.1. The CCO also has the authority to require any Participant or Trusted Source to appear before him or her to answer questions regarding alleged Violations. The CCO may also delegate such authority to ICE Trade Vault Europe employees, including officers, and such other individuals (who possess the requisite independence) as ICE Trade Vault Europe may hire on a contract basis.

The CCO shall have the power to initiate an investigation of any suspected Violation and conduct investigations of possible Violations, prepare written reports with respect to such investigations, furnish such reports to the Board of Directors and undertake action in response to such Violations in accordance with this paragraph 2.6.

If, in any case, the CCO (or another ICE Trade Vault Europe employee designated for this purpose by ICE Trade Vault Europe) concludes that a Violation may have occurred, he or she may:

- issue a warning letter to the Participant or Trusted Source informing it that there may have been a Violation and that such continued activity may result in further action by ICE Trade Vault Europe; or
- negotiate a written settlement agreement with the Participant or Trusted Source, whereby the Participant or Trusted Source may agree to a suspension or a termination of Participant or Trusted Source status or other remedial action to address the Violation.

Any settlement recommended by the CCO shall be subject to the approval of the Board of Directors and shall become final and effective pursuant to Rule 2.6.6.

2.6.2 Board of Directors' Powers

The Board of Directors shall have the power to direct that an investigation of any suspected Violation be conducted by the CCO and shall hear any matter referred to it by the CCO regarding a suspected Violation.

In any case where the Board of Directors concludes that a Violation has occurred, the Board of Directors shall advise the Participant or Trusted Source of that fact pursuant to Rule 2.6.3 and may: (i) refer or return the matter to the CCO with instructions for further investigation; (ii) approve a settlement agreement negotiated pursuant to this rule with such Participant or Trusted Source (which may provide for remedial action other than that recommended by the CCO); and/or (iii) take remedial actions that may include, but are not limited to, a warning or a suspension or a termination of Participant or Trusted Source status.

2.6.3 Notice of Action; Right to Hearing

Pursuant to instructions from the Board of Directors, the CCO shall serve a notice of action (a "Notice") on the Participant or Trusted Source responsible for a Violation (the "Respondent"). Such Notice shall state: (i) the acts, practices or conduct of the Respondent that are considered to be a Violation; (ii) how such acts, practices or conduct constitute a Violation; (iii) that the Respondent is entitled, upon written request filed with ICE Trade Vault Europe within twenty days of service of the Notice, to a formal hearing on the alleged Violation; (iv) that the failure of the Respondent to request a hearing within twenty days of service of the Notice, except for good cause shown, shall be deemed a waiver of its right to a hearing; (v) that the failure of the Respondent to file a written answer to the Notice with the CCO within twenty days of service of the Notice shall be deemed an admission of all of the acts, practices or conduct contained in the Notice; and (vi) that the failure of the Respondent to expressly deny a particular allegation contained in the Notice shall be deemed an admission of such acts, practices or conduct.

Any hearing requested by Respondent shall be conducted pursuant to rules and procedures adopted by the Board of Directors, which, in the judgment of the Board of Directors, are sufficient to give such Respondent an opportunity to fully and fairly present to the Board of Directors the Respondent's case. No member of the hearing panel shall hear a matter in which that member, in the determination of the CCO, has a direct financial, personal or other interest in the matter under consideration.

2.6.4 Hearing on Alleged Violation; Failure to Request Hearing Deemed Acceptance of Alleged Violation.

In the event (i) the Respondent fails to file an answer or admits to or fails to deny any allegation of a Violation contained in the Notice or (ii) after a hearing conducted pursuant to Rule 2.6.3 the Board of Directors determines that any alleged Violation did in fact occur with respect to a Respondent, the Board of Directors shall find the Respondent to have committed each such Violation and may suspend or terminate the Respondent’s Participant or Trusted Source status. The CCO shall promptly notify the Respondent of any such action and of the Respondent's right to a hearing on the action. Failure to request a hearing on the action in a timely manner, absent good cause shown, shall be deemed to be acceptance of the action.

2.6.5 Liability for Expenses

A Respondent found to have committed a Violation may, in the discretion of the Board of Directors, be required to pay to ICE Trade Vault Europe an amount equal to any and all out-of-pocket expenses incurred by ICE Trade Vault Europe in connection with the investigation and remedying of such Violations.

2.6.6 Effective Date of Remedial Actions

If a Respondent enters into a settlement agreement, the terms of which have been approved by the Board of Directors, any remedial actions included as a part of such settlement agreement shall become final and effective on the date that the Board of Directors approves or enters into such settlement agreement.

Any decision by the Board of Directors shall be the final decision of ICE Trade Vault Europe and shall become effective fifteen days, or such longer time as the Board of Directors may specify, after a copy of the written decision of the Board of Directors has been served on the Respondent; *provided*, *however*, that in any case where the user has consented to the action taken and to the timing of its effectiveness, the Board of Directors may cause the decision involving any action to become effective prior to the end of the fifteen day period.

2.7 Conflicts of Interest

Conflicts of interest, or potential conflicts of interest, can arise in many ways including but not limited to (i) conflicts between business considerations and compliance requirements or Applicable Law; (ii) conflicts between management, employees and/or members of the Board of Directors or any close links of such persons or between such persons and ICE Trade Vault Europe or any entity in its corporate group; (d) conflicts between ICE Trade Vault Europe and other entities in its corporate group.

As part of its Internal Policies and Procedures, ICE Trade Vault Europe has a conflicts of interest policy concerning the identification, management and disclosure of conflicts of interest, or potential conflicts of interest, as the case may be. ICE Trade Vault Europe also maintains an ongoing inventory of existing conflicts of interest and manages these on an ongoing basis. In addition to the Internal Policies and Procedures, this paragraph 2.7 shall apply to the Board of Directors, or any committee thereof, and any member of senior management of ICE Trade Vault Europe.

2.7.1 Definitions

For purposes of this Rule 2.7 the following definitions shall apply:

The term "Family Relationship" shall mean the person's spouse, former spouse, parent, stepparent, child, stepchild, sibling, stepbrother, stepsister, grandparent, grandchild, uncle, aunt, nephew, niece or in-law.

The term "Named Party in Interest" shall mean a person or entity that is identified by name as a subject of any matter being considered by the Board of Directors or a committee thereof.

2.7.2 Prohibition

No member of the Board of Directors or of any committee thereof which has authority to take action for and in the name of ICE Trade Vault Europe shall knowingly participate in such body's deliberations or voting in any matter involving a Named Party in Interest where such member (i) is a Named Party in Interest, (ii) is an employer, employee, or guarantor of a Named Party in Interest or an affiliate thereof, (iii) has a Family Relationship with a Named Party in Interest or (iv) has any other significant, ongoing business relationship with a Named Party in Interest or an affiliate thereof.

2.7.3 Disclosure

Prior to consideration of any matter involving a Named Party in Interest, each member of the deliberating body shall disclose to the CCO, or his designee, whether such member has one (1) of the relationships listed in Rule 2.7.2 with a Named Party in Interest.

2.7.4 Procedure and Determination

The CCO shall determine whether any member of the deliberating body is subject to a prohibition under Rule 2.7.2. Such determination shall be based upon a review of the following information: (i) information provided by the member pursuant to Rule 2.7.3, and (ii) any other source of information that is maintained by or reasonably available to ICE Trade Vault Europe.

3 Access, Connectivity and Safe Guarding of Data

3.1 [Reserved]

3.1.1 ICE RRM Service Participant and Trusted Source Access

Access to the ICE RRM Service is provided to parties that have a duly executed agreement in effect with ICE Trade Vault Europe.

When enrolling with ICE Trade Vault Europe, Participants and Trusted Sources must designate a master user ("Administrator"). The Administrator will create, permission and maintain all user IDs for their firm with regard to accessing the user interface ("UI"). Application Program Interface ("API") user IDs may be requested from ICE Trade Vault at tradevaultsupport@theice.com. Production user IDs for the APIs will be provided once the Participant has completed the applicable conformance testing plan within an ICE Trade Vault test environment.

Participants and Trusted Sources shall only have access to their own data.

Participants and Trusted Sources shall be entitled to access and correct in a timely manner any information on a contract to which they are a party.

3.1.2 [*Reserved*]

3.1.3 Reporting to ACER

ICE RRM will report Wholesale Energy Market Data to ACER in a standard form defined by ACER. The reported information must contain the information indicated in the Implementing Acts. ICE RRM has a mechanism in place to ensure that ACER's receipts detailing out what data was reported and on the outcome of the reporting are properly processed. ICE RRM also has proper procedures for rectification and re-submission of invalid reports are in place. In the event ACER identifies information reported by a Participant or Trusted Source as invalid, such Participant or Trusted Source will be informed of the invalid information and how they should correct it. Once corrected, the information should be resent to ICE RRM for re-submission to ACER.

3.1.4 Third-Party Service Providers; Transparency About Access

Each third-party service provider that provides a service of a particular nature (a "Relevant Service") in connection with ICE Trade Vault Europe will be subject to the same procedures governing access to information maintained

by ICE Trade Vault Europe as each other provider of the same Relevant Service. However, no third-party service provider will have access to any information maintained by ICE Trade Vault Europe unless and until the relevant counterparties have consented to such third-party service provider accessing the relevant data. The CCO will review and confirm that sufficient evidence of the relevant consents has been obtained.

As a condition to its access to information maintained by ICE Trade Vault Europe, each third-party service provider agrees that it will not, with respect to any such information, act or omit to act in any manner that would cause ICE Trade Vault Europe to be in breach of the confidentiality, integrity and data protection requirements that apply to trade repositories under Applicable Law. Each third-party service provider that provides a Relevant Service will, with respect to information maintained by ICE Trade Vault Europe, comply with the confidentiality terms prescribed by ICE Trade Vault Europe with respect to providers of that Relevant Service.

3.2 Revocation of Access

Revocation or limitation of access shall only be permitted to the extent necessary to control risk to data stored by ICE Trade Vault Europe. Prior to implementing any limitation or revocation of a Participant's or Trusted Source's access to the ICE RRM Service or data maintained by ICE Trade Vault Europe, the CCO shall review the basis for the limitation or revocation for compliance with Applicable Law, the Internal Policies and Procedures and the rules of the ICE RRM Service, and provide advance notice to the Participant or Trusted Source of such limitation or revocation. If the CCO determines that a Participant or Trusted Source would be discriminated against unfairly if the proposed revocation or limitation were implemented, the CCO shall take such actions as are necessary to ensure that Participant's or Trusted Source's access to such service or data remains unaffected.

3.3 Reinstatement of Access; Revocation or Modification of Other Actions; Termination of Status

A Participant or Trusted Source that has had access revoked or limited pursuant to Rule 3.2 may seek reinstatement, revocation or modification of such action by submitting an application to the Board of Directors in such form and accompanied by such information as ICE Trade Vault Europe may prescribe. Such application may be rejected or granted in whole or in part by the Board of Directors in its discretion. If a Participant or Trusted Source whose access has been so limited or revoked does not appeal within twenty (20) days after the commencement of such limitation or revocation, or if such Participant or Trusted Source shall have so applied and the Board of Directors shall have rejected the application, any decision to limit or revoke such access shall be upheld. The Board of Directors may terminate such Participant's or Trusted Source's user status after giving such user notice and an opportunity to be heard at a hearing before the Board of Directors. Any such hearing shall be conducted pursuant to the Internal Policies and Procedures and other rules and procedures adopted by the Board of Directors which, in the judgment of the Board of Directors, are sufficient to give such user an opportunity to fully and fairly present to the Board of Directors the user's reasons why the application should be granted.

3.4 Connectivity

Participants, Trusted Sources and Regulators may access the ICE RRM Service through a web-based front-end that requires user systems to (a) satisfy ICE Trade Vault Europe minimum computing system and web browser requirements, (b) support HTTP 1. 1 and 128-bit or stronger SSL data encryption, and (c) support the most

recent version of Adobe Flash Player. Trusted Sources may connect to the ICE RRM Service through direct electronic access via an API.

4 Acceptance of Data and Reporting Procedures

4.1 Asset Classes

The ICE RRM Service accepts all Wholesale Energy Market Data.

4.2 Trade Data and Data Processing

4.2.1 General

ICE RRM Participants and Trusted Sources reporting Wholesale Energy Market Data to the ICE RRM Service will be required to comply with Applicable Law.

4.2.2 Participants and Trusted Sources

Applicable Law requires that Participants and Trusted Sources report through a RRM prescribed details of any Wholesale Energy Contract concluded and any modification or termination of such contract.

A Trusted Source which is an Organised Market Place listed by ACER under Article 3(2) of the Implementing Acts agrees, in accordance with Article 6 thereof,

i) that ICE RRM shall be the reporting channel for Article 5 Information in respect of products executed or orders placed at such market place; and

ii) that the REMIT Supplement to the ICE Trade Vault Europe Participant Agreement or the ICE Europe RRM Agreement (as appropriate) constitutes the data reporting agreement which is offered by such market place to market participants.

The timing of reporting and the details to be reported are set out in Applicable Law, and will differ depending on whether a Wholesale Energy Contract is a standard contract or non-standard contract referred to in Article 7 of the Implementing Act.

ICE RRM recognises that Participants may need to update data submissions or correct data submissions that contain errors. ICE RRM data submissions may be corrected by Participants in a timely manner. Lifecycle Event Data (as described in Rule 4.2.3) will require reporting to ICE RRM within the time periods set out under Applicable Law. However, in all cases such corrections and Lifecycle Event Data submissions are required to conform to the applicable LEI, ACER Code, UPI and UTI requirements and any other requirements under Applicable Law. Disciplinary actions may be taken for ongoing and excessive corrections or where such corrections or Lifecycle Event Data submissions are not made in good faith by the relevant Participant.

4.2.3 Wholesale Energy Market Data

Participants and Trusted Sources must report details of Wholesale Energy Contracts and all Lifecycle Event Data for Wholesale Energy Contracts previously reported to the ICE RRM Service as prescribed by Applicable Law. “Lifecycle Event Data” is the set of data generated in connection with lifecycle events that occur prior to, and including, a Wholesale Energy Contract’s termination date as required by Applicable

Law. The term "lifecycle events" includes, but is not limited to, trade cancellations, modifications, and terminations.

4.2.4 [Reserved]

4.2.5 ICE RRM Non-Standard Contract Data

ICE RRM supports the submission of non-standard contract data, as defined in the Implementing Acts, for Wholesale Energy Contracts. Participants and Trusted Sources may submit non¬standard contract data for Wholesale Energy Contracts in the form prescribed by ACER.

ICE RRM's supports the reporting of bespoke products in line with ACER's guidance on the reporting of spreads.

4.3 Data Translation and Default Data

Proprietary trade data values submitted by Participants and Trusted Sources must be converted to ICE RRM Service standard data value(s) in order to process trade records in a standardised format. Participants and Trusted Sources may utilise the web-based front-end to map proprietary data values to a standard set of ICE RRM Service data values. Once defined, a Participant's, Appointed Reporting Entity's or Trusted Source's data map is applied to each trade record subsequently received and processed by the ICE RRM Service.

Participants and Trusted Sources may also utilise the default data value facility provided with the ICE RRM Service for certain product default fields. This facility allows Participants and Trusted Sources to utilise, within the ICE RRM Service, a default standard data value by product. Prior to processing the trade, all required fields of a trade record must contain a standard data value for that product type. In the event that the Participant or Trusted Source submits no data value for a required field for a trade record, the ICE RRM Service uses the agreed default data value for that field.

4.4 Trade Status

Trade Status identifies the current reported state of a trade submitted to ICE RRM:

- REPORTED - ORDER: an order which has passed validation and has been reported to ACER.
- REPORTED - TRADE: a trade which has passed validation and has been reported to ACER.
- CANCELED - ORDER: an order which has passed validation and has been reported to ACER, then was subsequently cancelled.
- CANCELED - TRADE: a trade which has passed validation and has been reported to ACER, then was subsequently cancelled.
- ERRORED - ORDER: an order which failed validation in either ICE Trade Vault's RRM Service or

ACER and has not been reported to ACER in a valid state.

- ERRORED - TRADE: a trade which failed validation in either ICE Trade Vault's RRM Service or ACER and has not been reported to ACER in a valid state.

4.5 No Invalidation or Modification of Valid Derivative Contract Data

Lifecycle Event status identifies an action taken with respect to a Wholesale Energy Contract submitted to ICE RRM Service:

- NEW: the submission of a contract or an order to trade (trade or order report) for the first time.
- MODIFY: the modification of details of a previous trade or order report.
- ERROR: the cancellation of a wrongly submitted trade or order report.
- CANCEL: the termination of an existing contract or order to trade.

4.6 Correction of Errors in Trade Records

Participants and Trusted Sources are responsible for the timely resolution of transaction record errors. ICE Trade Vault Europe provides Participants and Appointed Reporting Entities electronic methods to correct transaction record errors and to extract data for trade data reconciliation.

4.7 Duty to Collect and Maintain Derivative Contract Data

Consistent with the requirements of Applicable Law, ICE Trade Vault Europe has the capacity to collect and maintain all derivative contract data recorded as part of the ICE RRM Service in accordance with Applicable Law. In this regard the ICE RRM Service performs both (i) standard derivative contract data collection and maintenance and (ii) specific tasks based on ad hoc requests of Regulators in a manner consistent with Applicable Law.

5 Unique Identifiers

5.1 Unique Trade Identifiers (UTIs)

Applicable Law states that counterparties to a derivative contract are responsible for generating UTIs for that transaction.

The Participant, Appointed Reporting Entity or Trusted Source reporting derivative contract data to the ICE RRM Service must provide the relevant UTIs with their transaction data submissions.

5.2 Legal Entity Identifiers (LEIs)

ICE Trade Vault Europe has the ability to map entities to their LEIs. This allows Participants to submit the entity name as stored in their system and map to the correct LEI.

5.3 Unique Product Identifiers (UPIs)

Applicable Law requires UPIs to be created and processed in a centralised registry. ICE Trade Vault Europe shall, where necessary, issue UPIs (at no cost to Participants), maintain reference data

representation of each product, including schema definitions, and disseminate the representation to Participants. If the industry creates and adopts a UPI taxonomy and registry, or to the extent there is an applicable existing UPI, ICE Trade Vault will comply with published standards at that time.

5.3.1 Creating New UPIs

Entities requesting new products must provide the new product specifications to ICE Trade Vault Europe in order to receive a new UPI code and product schema.

6 Data Retention; Business Continuity

6.1 Data Retention, Access and Recordkeeping

In accordance with Internal Policies and Procedures, ICE RRM Service data is saved to a redundant, local database and a remote disaster recovery database in near real-time. The ICE RRM Service database is backed-up to tape daily with tapes moved offsite weekly.

With the exception of cleared futures trades reported by any entity of the ICE Group,[1] Participants' individual trade data records remain available to Participants and Trusted Sources at no charge for online access through the ICE RRM Service from the date of submission until five years after the end date of the trade (last day of delivery or settlement as defined for each product). During this time period, ICE RRM Service data will be available to Regulators at no cost via real-time electronic access. After the initial five-year period, Participants' trade data will be stored off-line and remain available to Participants, upon a three-day advance request to ICE Trade Vault Europe, at no cost until ten years following the termination of the relevant derivative contract. Participant will retain unimpaired access to its online and archived trade data even in the event of Participant's discontinued use of the ICE RRM Service.

I ICE Trade Vault Europe shall co-operate with Regulators in accordance with Applicable Law, including, where required by and in accordance with Applicable Law, taking such action as may be necessary to enable such Regulator to carry out investigations.

Nothing in this Rule 6.1 will require a Participant to pay fees associated with ICE Trade Vault Europe's standard regulatory reporting and access obligations. However, if a Participant or its Regulator requests or requires archived trade data from ICE Trade Vault Europe to be delivered other than via the web-based front-end or the API or in a non-standard format, ICE Trade Vault Europe reserves the right to require Participant to reimburse ICE Trade Vault Europe for its reasonable expenses in producing data in response to such request or requirement as such expenses are incurred. Similarly ICE Trade Vault Europe may require a Participant to pay all reasonable expenses associated with producing records relating to its transactions pursuant to a court order or other legal process, as those expenses are incurred by ICE Trade Vault Europe, whether such production is required at the instance of such Participant or at the instance of another party in relation to a Participant's data.

ICE Trade Vault Europe may retain copies of communications between officers, employees or agents of ICE Trade Vault Europe, on one hand, and Participants and Trusted Sources (including related parties), on the

[1] ICE Trade Vault Europe archives all cleared and cancelled futures trades reported by ICE exchanges and clearinghouses that are older than 45 days. A Participant or Trusted Source may request to retrieve these archived trades as needed by contacting TradeVaultSupport@theice.com.

other hand, in such manner and for such periods of time as ICE Trade Vault Europe may deem necessary and appropriate to comply with Applicable Law.

6.2 Legal Entity Identifiers (LEIs) or ACER Codes

ICE RRM Service has the ability to map entities to their assigned identifiers, including, but not limited to, LEIs or ACER Codes. This allows Participants to submit the entity name as stored in their system and map to the correct LEI or ACER Code.

6.3 Outsourcing ICE RRM Service Functions

ICE Trade Vault Europe may, from time to time, outsource to another entity in its group, or to a third party, one or more of its functions that enable it to carry out the ICE RRM Service. Any such outsourcing will be permitted only in accordance with Applicable Law and the Internal Policies and Procedures.

7 Data Confidentiality; Sensitive Information and Security

ICE RRM recognises its responsibility to ensure data confidentiality and dedicates significant resources to information security to prevent the misappropriation or misuse of Article 5 Information and any other information maintained in the ICE RRM systems.

ICE RRM uses a multi-tiered firewall scheme to provide network segmentation and access control to its services. Firewalls are deployed in redundant pairs and employ stateful-inspection technology. ICE RRM application servers are housed in a demilitarised zone behind external firewalls. A second set of internal firewalls further isolate ICE RRM database systems, an intrusion system provides added security to detect any threats, and network sensors analyse all internet and private line traffic for malicious patterns.

Tactical controls are regularly examined and tested by multiple tiers of internal and external test groups, auditors and independently contracted third-party security testing firms. The controls impose an accountable and standard set of best practices to protect the confidentiality of Article 5 Information and any other information maintained in the ICE RRM. ICE RRM will complete an internal audit upon request by ACER for adherence to the data security policies. The audit tests the following applicable controls, among others, to ICE RRM systems: (i) logical access controls; (ii) logical access to databases; (iii) physical and environmental controls; (iv) back-up procedures; and (v) change management.

In accordance with the Internal Policies and Procedures, ICE RRM has procedures in place to prevent natural persons who have a close link with ICE RRM, or legal persons who are in the same corporate group as ICE RRM, using confidential information recorded by ICE RRM, including Article 5 Information and any other RRM Information maintained in the ICE RRM systems. ICE RRM itself will also not use such information for commercial purposes.