ANNEX B - DATA PROTECTION

Where Participant is incorporated in any member state of the European Economic Area ("**EEA**") or in the United Kingdom, the following additional terms in this Annex B ("**Additional Terms**") 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, and, 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;

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

"**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 clause 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 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.

2.5 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.

2.6 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 all Applicable Laws.

3.2 Where clause 3.1 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 Data, 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 Data, 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 the Agreement shall be considered as a signature to the Transfer Clauses.

3.4 Where clause 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 clause 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, 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 so that they fulfil the intention for them to provide the appropriate safeguards as required under UK 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.

3.6 For the purposes of UK Data Protection Laws:

(a) Clause 6 Description of the transfer(s) is replaced with: "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred are those specified in Schedule 1 or Schedule 3, as applicable, where UK Data Protection Laws apply to the Processing".

(b) References to "Regulation (EU) 2016/679" or "that Regulation" are replaced by "UK Data Protection Laws" and references to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws. For the purposes of UK Data Protection Laws references to the "Union", "EU" and "EU Member State" are all replaced with the "UK".

(c) References to Regulation (EU) 2018/1725 are removed.

(d) References to the “Union”, “EU” and “EU Member State” are all replaced with the “UK”.

(e) Clause 13(a) and Part C of Schedules 1 and 3 are not used; the "competent supervisory authority" is the “Information Commissioner".

(f) Clause 17 of the Transfer Clauses is replaced to state "These Clauses are governed by the laws of England and Wales".

(i) The Parties may agree to change Clause 17 and/or 18 to refer to the laws and/or courts of Scotland or Northern Ireland.

(g) Clause 18 of the Transfer Clauses is replaced to state: "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."

(h) The footnotes to the Transfer Clauses do not apply.

3.7 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 clause 3.6, the provisions that provide the most protection to data subjects shall prevail.

3.8 Save for the provisions in clause 3 the terms of this Agreement shall not vary the Transfer Clauses in any way.

3.9 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 as separate documents setting out the proposed transfers of Personal Data in such manner as may be required.

3.10 In the event that the Transfer Clauses or any of the specific provisions set forth at clause 3.6 are amended, replaced or repealed by the European Commission, 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 and signature are incorporated per clause 3 of the Additional Terms. Date shall be the date on which the Agreement is executed.

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):

Signature is incorporated per clause 3 of the Additional Terms. Date shall be the date on which the Agreement is executed.

Name: ICE Trade Vault Europe Limited

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

Contact person's name, position and contact details: Data Protection Officer, Milton Gate, 60 Chiswell Street, London EC1Y 4SA (*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.A. (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.A. (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 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

---

([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.

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 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 1.B.

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.B. 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.

(b) 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. 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

([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.

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.

(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:

(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.

([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.

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.

([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.

(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.

(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.C, 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.C, 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.C, 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).

(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.

([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 and signature are incorporated per clause 3 of the Additional Terms. Date shall be the date on which the Agreement is executed.

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]*

Signature is incorporated per clause 3 of the Additional Terms. Date shall be the date on which the Agreement is executed.

Name: ICE Trade Vault Europe Limited

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

Contact person's name, position and contact details: Data Protection Officer, Milton Gate, 60 Chiswell Street, London EC1Y 4SA (*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 recognises its responsibilities 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

(i) 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.

(ii) Computer Operations

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

(iii) 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.

(iv) 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.A. (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.A. (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

---

([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.

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 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.B.

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.B, 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.B. 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.B.

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.

([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.

(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.

(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

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

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.

(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.C, 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.C, 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.C, 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.

(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.

([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.

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.