

ICE Clear Europesm

Clearing Rules

~~29 October 2018~~



Exhibit 1: Customer-CM CDS Transaction Standard Terms

Exhibit 2: Customer-CM F&O Transaction Standard Terms

Exhibit 3: Customer-CM FX Transaction Standard Terms

Exhibit 4: Settlement and Notices Terms

Exhibit 5: Standard Contractual Clauses

(h) ~~(h)~~ To the extent that the Clearing House is established in a jurisdiction which the European Commission has not found to offer an adequate level of protection for Personal Data transferred from the European Union in accordance with Article 45 of the General Data Protection Regulation, the Clearing House and each Exporting Member agree that:

(A) ~~(A)~~ the Exporting Member's transfer of Personal Data to the Clearing House will be governed by the Standard Contractual Clauses incorporated into these Rules at Exhibit 5;

(B) ~~(B)~~ in relation to the Personal Data received from an Exporting Member, the Clearing House shall comply with the Standard Contractual Clauses as the Data Importer;

(C) ~~(C)~~ in relation to the Personal Data transferred by the Exporting Member to the Clearing House, the Exporting Member shall comply with the Standard Contractual Clauses as the Data Exporter;

(D) ~~(D)~~ the description of the Data Subjects, recipients of Personal Data, purpose of the transfer(s) and categories of Personal Data transferred by the Exporting Member is set out at Annex B to the Standard Contractual Clauses;

(E) ~~(E)~~ for the purposes of Clause I(d) of the Standard Contractual Clauses:

(1) ~~(1)~~ the Clearing House will respond to enquiries from Data Subjects and Supervisory Authorities concerning its Processing of Personal Data received from the Exporting Member under the Standard Contractual Clauses; and

(2) ~~(2)~~ notwithstanding Rule 106(f)(E)(1), the Exporting Member will respond to enquiries from Data Subjects and Supervisory Authorities to the extent reasonably possible and with the information reasonably available to it if the Clearing House notifies the Exporting Member that it is unwilling or unable to respond;

(i) ~~(i)~~ for the purposes of Clause II(e) of the Standard Contractual Clauses, the Clearing House's point of contact for matters relating to the Personal Data transferred under the Standard Contractual Clauses is:

Data Protection Officer
Legal Department
Intercontinental Exchange
Milton Gate
60 Chiswell Street
London EC1Y 4SA
Email: regulatory-dataprotection@theice.com
Phone: +44 (0)20 7065 7700

- (j) ~~(h)~~ for the purposes of Clause II(g) of the Standard Contractual Clauses:
- (i) ~~(g)~~ an Exporting Member's review, audit or certification of the Clearing House's Processing of Personal Data received from the Exporting Member under the Standard Contractual Clauses shall be carried out subject to the confidentiality obligations imposed on the Exporting Member as agreed by the Clearing House and the Exporting Member and may be satisfied by provision of Clearing House's most recent annual Service Organization Control (SOC) Report in accordance with the procedure described at www.theice.com/security;
 - (ii) ~~(g)~~ before the commencement of any audit, review or certification, the Clearing House and the Exporting Member shall mutually agree upon its scope, timing and duration, and on the reimbursement rate for which Exporting Member shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by Clearing House; and the Exporting Member shall promptly notify the Clearing House of any non-compliance discovered during the course of an audit, review or certification;
- (k) ~~(h)~~ for the purposes of Clause II(i) of the Standard Contractual Clauses, the Exporting Member acknowledges that Personal Data received from the Exporting Member under the Standard Contractual Clauses may be transferred to third party controllers as described in Rule 106(a); and
- (l) ~~(h)~~ in the event of conflict or inconsistencies between the provisions of the Standard Contractual Clauses and these Rules or the Clearing Membership Agreement on matters relating to the processing of Personal Data received by the Clearing House from an Exporting Member under the Standard Contractual Clauses, the Standard Contractual Clauses shall take precedence.
- (m) ~~(h)~~ For the purposes of Rule 106 only, the terms:
- (i) ~~(g)~~ the terms "Data Subject", "Process" (and derivations thereof), "Personal Data" and "Controller" and "Supervisory Authority" each have the meaning given to such terms in Regulation (EU) 2016/679 (General Data Protection Regulation) (including any relevant implementing measure or successor legislation thereto);
 - (ii) ~~(g)~~ "Exporting Member" shall mean a Clearing Member which:
 - (A) ~~(A)~~ is subject to Chapter V of the General Data Protection Regulation;
and
 - (B) ~~(B)~~ transfers Personal Data to the Clearing House;
 - (iii) ~~(g)~~ "Standard Contractual Clauses" means the Set II Standard Contractual Clauses for the transfer of personal data from the Community to third countries (controller to controller transfers) (Commission Decision C(2004)5721/5271) and reproduced in Exhibit 5; and
 - (iv) ~~(g)~~ "Data Importer" and "Data Exporter" shall each have the meaning given to them in the Standard Contractual Clauses.

~~EXHIBIT~~EXHIBIT 5

ICE CLEAR EUROPE LIMITED

~~ICE CLEAR EUROPE LIMITED~~ STANDARD CONTRACTUAL CLAUSES

Commission Decision C(2004)~~5721~~5271

SET II

Standard contractual clauses for the transfer of personal data from the Community to third countries (controller to controller transfers)

Definitions

For the purposes of the clauses:

- a) “personal data”, “special categories of data/sensitive data”, “process/processing”, “controller”, “processor”, “data subject” and “supervisory authority/authority” shall have the same meaning as in Directive 95/46/EC of 24 October 1995 (whereby “the authority” shall mean the competent data protection authority in the territory in which the data exporter is established);
- b) “the data exporter” shall mean the controller who transfers the personal data;
- c) “the data importer” shall mean the controller who agrees to receive from the data exporter personal data for further processing in accordance with the terms of these clauses and who is not subject to a third country’s system ensuring adequate protection;
- d) “clauses” shall mean these contractual clauses, which are a free-standing document that does not incorporate commercial business terms established by the parties under separate commercial arrangements.

The details of the transfer (as well as the personal data covered) are specified in Annex B, which forms an integral part of the clauses.

I. Obligations of the data exporter

The data exporter warrants and undertakes that:

- a) The personal data have been collected, processed and transferred in accordance with the laws applicable to the data exporter.

- b) It has used reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses.
- c) It will provide the data importer, when so requested, with copies of relevant data protection laws or references to them (where relevant, and not including legal advice) of the country in which the data exporter is established.
- d) It will respond to enquiries from data subjects and the authority concerning processing of the personal data by the data importer, unless the parties have agreed that the data importer will so respond, in which case the data exporter will still respond to the extent reasonably possible and with the information reasonably

available to it if the data importer is unwilling or unable to respond. Responses will be made within a reasonable time.

- e) It will make available, upon request, a copy of the clauses to data subjects who are third party beneficiaries under clause III, unless the clauses contain confidential information, in which case it may remove such information. Where information is removed, the data exporter shall inform data subjects in writing of the reason for removal and of their right to draw the removal to the attention of the authority. However, the data exporter shall abide by a decision of the authority regarding access to the full text of the clauses by data subjects, as long as data subjects have agreed to respect the confidentiality of the confidential information removed. The data exporter shall also provide a copy of the clauses to the authority where required.

II. Obligations of the data importer

The data importer warrants and undertakes that:

- a) It will have in place appropriate technical and organisational measures to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.
- b) It will have in place procedures so that any third party it authorises to have access to the personal data, including processors, will respect and maintain the confidentiality and security of the personal data. Any person acting under the authority of the data importer, including a data processor, shall be obligated to process the personal data only on instructions from the data importer. This provision does not apply to persons authorised or required by law or regulation to have access to the personal data.
- c) It has no reason to believe, at the time of entering into these clauses, in the existence of any local laws that would have a substantial adverse effect on the guarantees provided for under these clauses, and it will inform the data exporter (which will pass such notification on to the authority where required) if it becomes aware of any such laws.

- d) It will process the personal data for purposes described in Annex B, and has the legal authority to give the warranties and fulfil the undertakings set out in these clauses.
- e) It will identify to the data exporter a contact point within its organisation authorised to respond to enquiries concerning processing of the personal data, and will cooperate in good faith with the data exporter, the data subject and the authority concerning all such enquiries within a reasonable time. In case of legal dissolution of the data exporter, or if the parties have so agreed, the data importer will assume responsibility for compliance with the provisions of clause I(e).
- f) At the request of the data exporter, it will provide the data exporter with evidence of financial resources sufficient to fulfil its responsibilities under clause III (which may include insurance coverage).
- g) Upon reasonable request of the data exporter, it will submit its data processing facilities, data files and documentation needed for processing to reviewing, auditing and/or certifying by the data exporter (or any independent or impartial inspection agents or auditors, selected by the data exporter and not reasonably objected to by the data importer) to ascertain compliance with the warranties and undertakings in these clauses, with reasonable notice and during regular business hours. The request will be subject to any necessary consent or approval from a regulatory or supervisory authority within the country of the data importer, which consent or approval the data importer will attempt to obtain in a timely fashion.
- h) It will process the personal data in accordance with the data processing principles set forth in Annex A.
- i) It will not disclose or transfer the personal data to a third party data controller located outside the European Economic Area (EEA) unless it notifies the data exporter about the transfer and
 - i. the third party data controller processes the personal data in accordance with a Commission decision finding that a third country provides adequate protection, or
 - ii. the third party data controller becomes a signatory to these clauses or another data transfer agreement approved by a competent authority in the EU, or
 - iii. data subjects have been given the opportunity to object, after having been informed of the purposes of the transfer, the categories of recipients and the fact that the countries to which data is exported may have different data protection standards, or
 - iv. with regard to onward transfers of sensitive data, data subjects have given their unambiguous consent to the onward transfer

III. Liability and third party rights

- a) Each party shall be liable to the other parties for damages it causes by any breach of these clauses. Liability as between the parties is limited to actual damage suffered. Punitive damages (i.e. damages intended to punish a party for its outrageous conduct) are specifically excluded. Each party shall be liable to data subjects for damages it causes by any breach of third party rights under these clauses. This does not affect the liability of the data exporter under its data protection law.
- b) The parties agree that a data subject shall have the right to enforce as a third party beneficiary this clause and clauses I(b), I(d), I(e), II(a), II(c), II(d), II(e), II(h), II(i), III(a), V, VI(d) and VII against the data importer or the data exporter, for their respective breach of their contractual obligations, with regard to his personal data, and accept jurisdiction for this purpose in the data exporter's country of establishment. In cases involving allegations of breach by the data importer, the data subject must first request the data exporter to take appropriate action to enforce his rights against the data importer; if the data exporter does not take such action within a reasonable period (which under normal circumstances would be one month), the data subject may then enforce his rights against the data importer directly. A data subject is entitled to proceed directly against a data exporter that has failed to use reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses (the data exporter shall have the burden to prove that it took reasonable efforts).

IV. Law applicable to the clauses

These clauses shall be governed by the law of the country in which the data exporter is established, with the exception of the laws and regulations relating to processing of the personal data by the data importer under clause II(h), which shall apply only if so selected by the data importer under that clause.

V. Resolution of disputes with data subjects or the authority

- a) In the event of a dispute or claim brought by a data subject or the authority concerning the processing of the personal data against either or both of the parties, the parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.
- b) The parties agree to respond to any generally available non-binding mediation procedure initiated by a data subject or by the authority. If they do participate in the proceedings, the parties may elect to do so remotely (such as by telephone or other electronic means). The parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.
- c) Each party shall abide by a decision of a competent court of the data exporter's country of establishment or of the authority which is final and against which no further appeal is possible.

VI. Termination

- a) In the event that the data importer is in breach of its obligations under these clauses, then the data exporter may temporarily suspend the transfer of personal data to the data importer until the breach is repaired or the contract is terminated.
- b) In the event that:
- i. the transfer of personal data to the data importer has been temporarily suspended by the data exporter for longer than one month pursuant to paragraph (a);
 - ii. compliance by the data importer with these clauses would put it in breach of its legal or regulatory obligations in the country of import;
 - iii. the data importer is in substantial or persistent breach of any warranties or undertakings given by it under these clauses;
 - iv. a final decision against which no further appeal is possible of a competent court of the data exporter's country of establishment or of the authority rules that there has been a breach of the clauses by the data importer or the data exporter; or
 - v. a petition is presented for the administration or winding up of the data importer, whether in its personal or business capacity, which petition is not dismissed within the applicable period for such dismissal under applicable law; a winding up order is made; a receiver is appointed over any of its assets; a trustee in bankruptcy is appointed, if the data importer is an individual; a company voluntary arrangement is commenced by it; or any equivalent event in any jurisdiction occurs

then the data exporter, without prejudice to any other rights which it may have against the data importer, shall be entitled to terminate these clauses, in which case the authority shall be informed where required. In cases covered by (i), (ii), or (iv) above the data importer may also terminate these clauses.

- c) Either party may terminate these clauses if (i) any Commission positive adequacy decision under Article 25(6) of Directive 95/46/EC (or any superseding text) is issued in relation to the country (or a sector thereof) to which the data is transferred and processed by the data importer, or (ii) Directive 95/46/EC (or any superseding text) becomes directly applicable in such country.
- d) The parties agree that the termination of these clauses at any time, in any circumstances and for whatever reason (except for termination under clause VI(c)) does not exempt them from the obligations and/or conditions under the clauses as regards the processing of the personal data transferred.

VII. Variation of these clauses

The parties may not modify these clauses except to update any information in Annex B, in which case they will inform the authority where required. This does not preclude the parties from adding additional commercial clauses where required.

VIII. Description of the Transfer

The details of the transfer and of the personal data are specified in Annex B. The parties agree that Annex B may contain confidential business information which they will not disclose to third parties, except as required by law or in response to a competent regulatory or government agency, or as required under clause I(e). The parties may execute additional annexes to cover additional transfers, which will be submitted to the authority where required. Annex B may, in the alternative, be drafted to cover multiple transfers.

ANNEX A

DATA PROCESSING PRINCIPLES

1. Purpose limitation: Personal data may be processed and subsequently used or further communicated only for purposes described in Annex B or subsequently authorised by the data subject.
2. Data quality and proportionality: Personal data must be accurate and, where necessary, kept up to date. The personal data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.
3. Transparency: Data subjects must be provided with information necessary to ensure fair processing (such as information about the purposes of processing and about the transfer), unless such information has already been given by the data exporter.
4. Security and confidentiality: Technical and organisational security measures must be taken by the data controller that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process the data except on instructions from the data controller.
5. Rights of access, rectification, deletion and objection: As provided in Article 12 of Directive 95/46/EC, data subjects must, whether directly or via a third party, be provided with the personal information about them that an organisation holds, except for requests which are manifestly abusive, based on unreasonable intervals or their number or repetitive or systematic nature, or for which access need not be granted under the law of the country of the data exporter. Provided that the authority has given its prior approval, access need also not be granted when doing so would be likely to seriously harm the interests of the data importer or other organisations dealing with the data importer and such interests are not overridden by the interests for fundamental rights and freedoms of the data subject. The sources of the personal data need not be identified when this is not possible by reasonable efforts, or where the rights of persons other than the individual would be violated. Data subjects must be able to have the personal information about them rectified, amended, or deleted where it is inaccurate or processed against these principles. If there are compelling grounds to doubt the legitimacy of the request, the organisation may require further justifications before proceeding to rectification, amendment or deletion. Notification of any rectification, amendment or deletion to third parties to whom the data have been disclosed need not be made when this involves a disproportionate effort. A data subject must also be able to object to the processing of the personal data relating to him if there are compelling legitimate grounds relating to his particular situation. The burden of proof for any refusal rests on the data importer, and the data subject may always challenge a refusal before the authority.

6. Sensitive data: The data importer shall take such additional measures (e.g. relating to security) as are necessary to protect such sensitive data in accordance with its obligations under clause II.
7. Data used for marketing purposes: Where data are processed for the purposes of direct marketing, effective procedures should exist allowing the data subject at any time to “opt-out” from having his data used for such purposes.
8. Automated decisions: For purposes hereof “automated decision” shall mean a decision by the data exporter or the data importer which produces legal effects concerning a data subject or significantly affects a data subject and which is based solely on automated processing of personal data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. The data importer shall not make any automated decisions concerning data subjects, except when:
 - a)
 - i. such decisions are made by the data importer in entering into or performing a contract with the data subject, and
 - ii. the data subject is given an opportunity to discuss the results of a relevant automated decision with a representative of the parties making such decision or otherwise to make representations to that parties.
 - or
 - b) where otherwise provided by the law of the data exporter.

ANNEX B DESCRIPTION OF THE TRANSFER

(To be completed by the parties)

Data subjects

The personal data transferred concern the following categories of data subjects:

- — past and present personnel (including employees, directors, officers, shareholders, beneficial owners, temporary employees, agents, contractors, secondees, interns and volunteers) of the data exporter and the data exporter's clients;
- — advisors, consultants, delivery facilities and other professional experts engaged by the data exporter.

Purposes of the transfer(s)

The transfer is made for the following purposes:

Business operations – management of business operations generally, including: the management and operation of the Clearing House in accordance with the Rules, the Clearing Membership Agreement and any such other agreements entered into between the data exporter and the data importer relating to the operation of the Clearing House; the safeguarding, promotion, maintenance, administration, support and development of the Clearing House; the administration and management of the data exporter's membership of the Clearing House; the fulfilment of contractual obligations; and

Compliance - compliance with legal, regulatory and self-regulatory requirements, such as: compliance with the data importer and data exporters' record-keeping and reporting obligations; enabling the data importer to conduct audits, comply with governmental inspections and other requests from governments or other public authorities, respond to legal process, pursue legal rights and remedies, defend litigation and manage complaints or claims; compliance with data importer's policies and procedures; ensuring compliance with laws, rules and regulations applicable to the data importer and/or the data exporter; market monitoring; preventing or detecting crime; conducting investigations.

Categories of data

The personal data transferred concern the following categories of data:

Personal details relating to the data subjects described above, including: name; date of birth; e-mail and telephone details; address; language preference; identification documents; national identification number; ITM;

Trading and usage information to the extent that it relates to a data subject in a personal capacity, including: details of trades cleared by the Clearing House; details of positions held; user IDs; watch list status; information concerning a data exporter's affairs (such as Matched Transactions, Contracts, positions, accounts, customers and clients, deliveries and settlement); usage logs for the Clearing House;

Call records to the extent that they relate to a data subject in a personal capacity, including: recordings of calls made in relation to the supervision of the Clearing House.

Recipients

The personal data transferred may be disclosed only to the following recipients or categories of recipients:

As described in Rule 106(a)

Sensitive data (if appropriate)

The personal data transferred concern the following categories of sensitive data:

Not applicable

Data protection registration information of data exporter (where applicable)

Not applicable

Additional useful information (storage limits and other relevant information)

Not applicable

Contact points for data protection enquiries

Data importer

Data Protection Officer
Legal Department
Intercontinental Exchange
Milton Gate, 60 Chiswell Street
London
EC1Y 4SA

Email: regulatory-dataprotection@theice.com
Phone: +44 (0)20 7065 7700

APPENDIX

ADDITIONAL SAFEGUARDS TO STANDARD CONTRACTUAL CLAUSES

1. The data importer will assess whether the laws applicable to it provide adequate protection under European Union ("EU") data protection law. To the extent that any such laws are likely to have a substantial adverse effect on the level of data protection offered by the Standard Contractual Clauses and required under EU data protection law, it will comply with the safeguards set out in paragraphs 2 and 3 below.
2. The data importer will adopt supplementary measures to protect the personal data received under the Standard Contractual Clauses from the data exporter ("SCC Personal Data") in accordance with the requirements of EU data protection law, including by implementing appropriate technical and organizational safeguards, such as encryption or similar technologies, access controls or other compensating controls, to protect personal data against any interference that goes beyond what is necessary in a democratic society to safeguard national security, defence and public security.
3. In the event that the data importer receives a legally binding request for access to the SCC Personal Data by a public authority, the data importer will:
 - (a) promptly notify the data exporter of such request to enable the data exporter to intervene and seek relief from such disclosure, unless the data importer is otherwise prohibited from providing such notice, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation. If the data importer is so prohibited:
 - (i) It will use its 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.
 - (ii) In the event that, despite having used its best efforts, the data importer is not permitted to notify the data exporter, it will make available on an annual basis general information on the requests it received to the data exporter and the competent supervisory authority of the data exporter.
 - (iii) Oppose any such request for access and contest its legal validity to the extent legally permitted under applicable law.
 - (b) comply with the data importer's internal policies governing the disclosure of personal data in response to requests from public authorities that conform to this Appendix
 - (c) not make any disclosures of the SCC 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

(d) upon request from the data exporter, provide general information on the requests from public authorities it received in the preceding 12 month period relating to SCC Personal Data.