

Data Processing and Guarantee Agreement

This Data Processing and Guarantee Agreement ("DPGA") is entered into by and between the data exporters (each a "**Data Exporter**") and the data importers (each a "**Data Importer**") listed on the Signature Page (each a "**Party**" and collectively the "**Parties**").

Preamble

- WHEREAS, Commerzbank AG, headquartered in Frankfurt/Main Germany, is an internationally active business bank, represented in numerous countries inside and outside of the European Union ("EU") and the European Economic Area ("EEA") through a network of branches and legal entities;
- WHEREAS, in certain circumstances, it may become necessary that Commerzbank AG, its branches and/or affiliates transfer personal data relating to customers and individual representatives, directors, contact persons, authorized signatories and authorized traders of its corporate customers as well as ultimate beneficial owners that are natural persons (together "**Data Subjects**"), to other branches and/or legal entities outside the EU/the EEA. Some countries in which the Commerzbank Group does business and to which personal data are transferred, may not provide for the same standard of data protection which applies in Germany or in the EU/the EEA;
- WHEREAS, the Parties wish to provide appropriate safeguards in connection with such transfers of personal data with respect to the protection of privacy and fundamental rights and freedoms of the data subjects;
- WHEREAS, European data protection laws require data exporters in EU/EEA countries to provide appropriate safeguards for transfers of personal data to controllers in non-EU/EEA countries and such appropriate safeguards can be adduced by requiring the Data Importers to enter into the Standard Contractual Clauses for the Transfer of Personal Data to Third Countries ("**Model Contract C2C**") pursuant to Commission Decision 2004/915/EC of 27 December 2004;
- WHEREAS, European data protection laws require data exporters in EU/EEA countries to provide appropriate safeguards for transfers of personal data to processors in non-EU/EEA countries and such appropriate safeguards can be adduced by requiring the Data Importers to enter into the Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries ("**Model Contract C2P**") pursuant to Commission Decision 2010/87/EU of 5 February 2010;
- WHEREAS, the Model Contract C2C as well as the Model Contract C2P are usually incorporated in an agreement between the legal entity transferring and the legal entity receiving the personal data. In the case of a transfer between a legal entity and its legally dependent branch, some data protection authorities have taken the view that a unilateral guarantee declaration, to be made available to the Data Subjects shall be used instead;
- WHEREAS, for transfers of personal data by a Data Exporter being a legal entity to one of its branches, the Data Exporter and the Data Importer guarantee to the Data Subjects that they assume the data exporter's and the data importer's obligations, respectively, as if they had entered into the Model Contract C2C respectively the Model Contract C2P as set out in Exhibit 1 respectively Exhibit 2 ("**Guarantee**"). Under this Guarantee, the Data Subjects shall have the same rights against the relevant Data Exporter as if its branch office was located in the EU/the EEA;
- WHEREAS, the Parties agree that the bundling of the Data Exporters and the Data Importers (as listed on the Signature Page) within this single DPGA is only undertaken for efficiency purposes (i.e., to avoid a multitude of different contract documents) and (i) shall result in legally separate agreements between each Data Exporter and each Data Importer and (ii) shall not create any legal or other relationship whatsoever between the "bundled" Parties other than between each Data Exporter and each Data Importer separately;

WHEREAS, the Model Contract C2C and the Model Contract C2P have to be supplemented by certain amendments required by the 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 the free movement of such data, and repealing Directive 95/46/EC ("**General Data Protection Regulation**") and/or local law amendments where required to address additional local law requirements;

WHEREAS, the Commerzbank Group wishes to apply a consistent set of rules to all transfers of personal data covered under this DPGA and therefore want to use the Model Contract C2C and Model Contract C2P regardless of the location of the Parties, whether within or outside the EU/the EEA;

WHEREAS, this DPGA is concluded only for those processing activities that are not covered by another "transfer vehicle", i.e. another option to comply with the rules on international data transfers.

WHEREAS, each particular data transfer or set of transfers shall be described in a separate Annex B to Exhibit 1 (in case of a controller to controller transfer) or in a separate Appendix 1 to Exhibit 2 (in case of a controller to processor transfer);

NOW, THEREFORE, in order to enable the Parties to exchange personal data in compliance with applicable laws and for other good and valuable consideration, the receipt of which is hereby acknowledged, the Parties enter into this DPGA as follows:

Main Body of the DPGA

1. Document structure and hierarchy

1.1 This DPGA consists of the various parts as follows:

| | |
|----------------------------------|--|
| This main body of the DPGA: | contains overarching provisions for all types of data transfers; |
| Exhibit 1: Model Contract C2C | contains the unmodified body document of the Model Contract C2C for controller to controller transfers (as per Commission Decision 2004/915/EC of 27 December 2004); |
| Annex A of Exhibit 1 | contains the data processing principles applicable to all controller to controller transfers of personal data covered hereunder according to Annex A of the Model Contract C2C; |
| Annex B.1 to B.5 of Exhibit 1 | contain descriptions of transfers of personal data according to Annex B of the Model Contract C2C; |
| Annex C of Exhibit 1 | contains local law Amendments to supplement (but not change) the Model Contract C2C in light of national requirements that go beyond the clauses of the Model Contract C2C and in light of the decision of the Court of Justice of the European Union C-311/18 ("Schrems II"); |
| Exhibit 2: Model Contract C2P | contains the unmodified body document of the Model Contract C2P for controller to processor transfers (as per Commission Decision 2010/87/EU of 5 February 2010); |
| Appendix 1.1 to 1.3 of Exhibit 2 | contains a description of the Data Importer's processing activities according to Appendix 1 of the Model Contract C2P; |
| Appendix 2 of Exhibit 2 | contains a description of the Data Importer's technical and organizational measures, which are applied consistently in connection with all processing activities described in Appendix 1.1 according to Appendix 2 of the Model Contract C2P; |
| Appendix 3 of Exhibit 2 | contains local law amendments to supplement (but not change) the Model Contract C2P in light of national requirements that go beyond |

the clauses of the Model Contract C2P and in light of the decision of the Court of Justice of the European Union C-311/18 ("Schrems II");

Signature Page

Page with Signatures of Data Exporters and Data Importers whereby the Parties declare to be bound by this DPGA.

- 1.2 Each Party hereby enters into this DPGA and the Model Contract C2C and/or Model Contract C2P (as applicable) with each other Party (as applicable).
- 1.3 For controller to controller transfers from an EU/EEA country to a non-EU/EEA country the clauses of Exhibit 1 and its Annexes shall prevail over any conflicting clauses in the remainder of the DPGA, unless expressly called out otherwise in Annex C of Exhibit 1 (Local Law Amendments). For the avoidance of doubt, any provisions in this DPGA that do not contradict the Model Contract C2C shall remain valid.
- 1.4 For controller to processor transfers from an EU/EEA country to a non-EU/EEA country the clauses of Exhibit 2 and its Appendices shall prevail over any conflicting clauses in the remainder of the DPGA, unless expressly called out otherwise in Appendix 3 of Exhibit 2 (Local Law Amendments). For the avoidance of doubt, any provisions in this DPGA that do not contradict the Model Contract C2P shall remain valid.
- 1.5 For transfers of personal data by a Data Exporter being a legal entity to one of its branches as Data Importer, the Data Exporter and the Data Importer guarantee to the Data Subjects that they assume the data exporter's and the data importer's obligations, respectively, as if they had entered into the Model Contract C2C respectively the Model Contract C2P as set out in Exhibit 1 respectively Exhibit 2. In particular, Data Subjects shall have the same rights against the relevant Data Exporter as if its branch office was located in the EU/the EEA.
- 1.6 In the event of inconsistencies between the provisions of this DPGA and any other agreement between the Parties in relation to the subject-matters addressed herein, the provisions of this DPGA shall prevail as it relates to the Parties' data protection obligations in connection with data transfers.
- 1.7 In relation to any transfers of personal data from an EU/EEA country to the United Kingdom, clauses 1.2 to 1.6 shall apply and the Model Contract C2C or Model Contract C2P (as applicable) shall apply if the United Kingdom:
 - (a) is not a White-List Country; and
 - (b) there are no other arrangements (including without limitation transitional arrangement) or legislation in place permitting the transfer of personal data from the EU/EEA to the United Kingdom for the purposes of the General Data Protection Regulation and/or local data protection laws.

2. Definitions

The following terms defined and used in this DPGA shall be interpreted as follows (also in the main body document of the Model Contract C2C in Exhibit 1 and the Model Contract C2P in Exhibit 2, where defined terms are not capitalized):

- 2.1 "Adequate Subprocessor" shall mean a Subprocessor located in the EU/EEA or a White-List Country;
- 2.2 The term "Clauses", as used herein, shall be interpreted as meaning all provisions of this DPGA, unless provided otherwise in the relevant context;
- 2.3 The term "Data Exporter", as used herein, shall be interpreted as meaning each entity specified as a Data Exporter in the relevant Annex B of Exhibit 1 (for controller to controller transfers) or Appendix 1 of Exhibit 2 (for controller to processor transfers), regardless of the country in which such entity is located and irrespective of the term being used in singular form (i.e., Data Exporter) or plural form (i.e., Data Exporters);
- 2.4 The term "Data Importer", as used herein, shall be interpreted as meaning each entity specified as a Data Importer in the relevant Annex B of Exhibit 1 (for controller to controller transfers) or Appendix 1 of Exhibit 2 (for controller to processor transfers), regardless of the country in which such entity is located and irrespective of the term being used in singular form (i.e., Data Importer) or plural form (i.e., Data Importers);

- 2.5 The term "**Member State**", as used herein, shall be interpreted as meaning any country in which a Party is located, whether this is a EU/EEA country or a non-EU/EEA country;
- 2.6 The term "**Service**" or "**Services**", as used herein, shall mean the (processing) services rendered by the Data Importer, as described in Annexes B to Exhibit 1 and Appendices 1 to Exhibit 2 (also if used with additions or in variations, for instance "processing Services");
- 2.7 The term "**Service Provider**" shall mean any Subprocessor (i.e., a processor without a contractual relationship with the Data Exporter) of the Data Importer or further processor (i.e., a processor with a direct contractual relationship with the Data Exporter) of the Data Exporter;
- 2.8 The term "**Commerzbank Group**", as used herein, shall be interpreted as meaning all legal entities and branches that jointly form the Commerzbank group of companies (i.e., the Data Importers and Data Exporters under this DPGA);
- 2.9 The terms "**Subprocessor**" or "**Sub-processor**" shall mean any processor, located within or outside the EU/EEA, who agrees to receive from the Data Importer personal data exclusively intended for processing activities to be carried out on behalf of the Data Exporter after the transfer in accordance with the Data Exporter's instructions and in accordance with the terms of this DPGA and a service agreement with the Data Importer;
- 2.10 "**White-List Country**" shall mean a country which is found by decision of the EU Commission to ensure an adequate level of data protection within the meaning of Article 45 (1) (9) General Data Protection Regulation.

3. Local law compliance

- 3.1 In order to comply with mandatory local law requirements, the Parties agree on the local law amendments contained in the Annex C of Exhibit 1 (for controller to controller transfers) and Appendix 3 of Exhibit 2 (for controller to processor transfers). These amendments shall apply to any data transfer or set of transfers described in Annexes B of Exhibit 1 or – as the case may be – Appendices 1 of Exhibit 2 (as applicable).
- 3.2 If and to the extent necessary to comply with mandatory provisions regarding data protection under the national laws applicable to the Data Exporter, Data Exporter may communicate any necessary requested changes (including amendments and/or replacements) to the provisions of this DPGA to Commerzbank AG, designating the Data Importer concerned. Commerzbank AG will communicate such changes to the Data Importer concerned. Such changes are deemed accepted by the Data Importer if it does not reject the changes within four weeks after having received a notification of the changes in writing (including electronic form).

4. Changes to this Agreement

Commerzbank AG shall be entitled to amend this DPGA from time to time, unless such amendments are prohibited by applicable law or the terms of this DPGA. Additional entities may be included by Commerzbank AG in the name and on behalf of the entities party to this agreement. Further data processing activities may be added or amended by Commerzbank AG unilaterally subject to its reasonable discretion. Commerzbank AG shall inform the Parties to this DPGA of such amendments (e.g. by adding the new entity to the signature page, by providing new annexes/appendices) thirty (30) days prior to their entry into force. At the end of such notice period, each legally separate agreement between each Data Exporter and each Data Importer will be deemed amended.

5. Term and termination

- 5.1 This DPGA shall have an indefinite term, it being understood that the participation in this DPGA may be terminated by a Party pursuant to section 5.2.
- 5.2 Without prejudice to any other termination rights that a Party may have under this DPGA and/or applicable law, each Party may terminate its participation in this DPGA by providing three (3) months' prior written notice to the other Party or Parties concerned. For the avoidance of doubt, the termination of its participation in this DPGA by a Party does not affect the other separate and divisible contractual relationships between the other Parties construed by this DPGA.

6. Miscellaneous

- 6.1 The Parties agree that the "bundling" of various Parties and data transfers in a single DPGA serves only efficiency purposes (i.e., to avoid a multitude of agreements) but shall result in separate and divisible relationships between the Data Exporters and Data Importers. Relatedly, and save as provided otherwise in Exhibit 1 or 2, nothing in this DPGA is intended or shall be construed to establish joint and several liability between the Parties. No Party shall be liable for acts or omissions of another Party.
- 6.2 This DPGA inures to the benefit of the Parties only and no third party shall have any rights hereunder, except as otherwise stated herein.
- 6.3 The main body document of this DPGA shall be governed by the laws of the country in which the Data Exporter is established except for those parts of the body document relating to the Parties' data protection obligations where the choice of law shall follow Clause IV of Exhibit 1 and Clause 9 of Exhibit 2. For the avoidance of doubt for Exhibit 1 and its Annexes the choice of law according to Clause IV of Exhibit 1 applies and for Exhibit 2 and its Appendices the choice of law according to Clause 9 of Exhibit 2 applies. As a minimum requirement the Parties must comply with the General Data Protection Regulation.
- 6.4 This DPGA may be executed in one or more counterparts, each of which shall be deemed an original and all of which together shall constitute one and the same instrument.
- 6.5 A determination that any provision of the DPGA is invalid or unenforceable shall not affect the other provisions of the DPGA. In such case the invalid or unenforceable provision shall automatically be replaced by a valid and enforceable provision that comes closest to the purpose of the original provision. The same shall apply if the DPGA contains an unintended gap.

Signatures: See Signature Page

Exhibit 1: Model Contract C2C

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

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, at its option, in accordance with:
 - (i) the data protection laws of the country in which the data exporter is established, or
 - (ii) the relevant provisions of any Commission decision pursuant to Article 25(6) of Directive 95/46/EC, where the data importer complies with the relevant provisions of such an authorisation or decision and is based in a country to which such an authorisation or decision pertains, but is not covered by such authorisation or decision for the

purposes of the transfer(s) of the personal data, or

- (iii) the data processing principles set forth in Annex A.

Data importer to indicate which option it selects: (iii)

Initials of data importer: _____

- (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 of 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.

Signatures: See Signature Page

**Annex A
of Exhibit 1
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 organization 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 - 1
of Exhibit 1
Know Your Customer Data Sharing**

Description of the transfer

Data Exporter(s)

The Commerzbank AG entities and branches listed in Signature Page.

Data Importer(s)

The Commerzbank AG entities and branches listed in Signature Page.

Data subjects

The personal data transferred concern, in particular, the following categories of data subjects:

1. Customers
2. Contact persons of (corporate) customers and of potential (corporate) customers.
3. Individual representatives/ authorized signatories and/or authorized traders/directors (Senior Executives, Members of the Board or Governing Body) of (corporate) customers or of potential corporate customers.
4. Ultimate beneficial owners/Shareholders of (corporate) customers and of potential corporate customers.

Purposes of transfer

The transfer is made, in particular, for the following purpose:

Global customer database and sharing KYC information serves the purpose to facilitate the onboarding process (avoid duplications of onboarding process) and to fulfil group wide AML-obligations.

The personal data will only be transferred if and to the extent in compliance with applicable law and used only on a need-to-know basis.

Categories of data

The personal data transferred concern, in particular, the following categories of data:

1. Customers, e.g.
 - Full name / first names
 - Title
 - Function
 - email-address
 - phone, fax
 - Date and place of birth (depending on local requirements of Sales location)
 - Passport/identity card details (copy of document normally provided)
 - Private address / Country of residence
 - Citizenship
 - PEP information
 - Tax ID
 - Results of screening and negative news search
2. Contact persons of (corporate) customers and of potential (corporate) customers, e.g.
 - Name
 - function,

- phone, fax
 - e-mail address
3. Individual representatives/ Authorized signatories and/or authorized traders/directors (Senior Executives, Members of the Board or Governing Body) of (corporate) customers or potential (corporate) customers, e.g.
- Full name / first names
 - Title
 - Function
 - email-address
 - phone, fax
 - Date and place of birth (depending on local requirements of Sales location)
 - Passport/identity card details (copy of document normally provided)
 - Private address / Country of residence
 - Citizenship
 - PEP information
 - Tax ID
 - Results of screening and negative news search
4. Ultimate Beneficial Owners/Shareholders of corporate customers and of potential corporate customers, e.g.
- Full name / first names
 - Title
 - Date and place of birth (depending on local requirements of Sales location)
 - Passport/identity card details (copy of document if exceptionally required)
 - Private address / Country of residence
 - investment percentage
 - Citizenship
 - PEP status and PEP information
 - Position/function in company
 - Tax residency
 - Tax Identification No. (TIN)
 - PEP information
 - Source of wealth, if required
 - Results of screening and negative news search

Recipients

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

- Commerzbank entities and branches listed in Signature Page.

The global customer database includes, whether the internationally operating (corporate) customer is already onboarded/has a relationship with one of the Commerzbank entities, and if so, certain details regarding the (corporate) customer (i.e. the name of the (corporate) customer, legal address, status of KYC (on-boarded, in process, rejected, prospect) as well as the risk rating result including reason why risk rating was manually changed,

KYC result and next review data, where the client is onboarded already and the fact that full KYC documentation already exists). Access to the global customer database is granted in two steps: Firstly, only the name of the (corporate) customer can be found by the German head office, all branches and all subsidiaries worldwide in the global customer database to ensure that new customers can be linked to existing customers. Secondly, if access to further information, including the abovementioned data categories of the above mentioned data subjects is needed, i.e. if the (corporate) customer needs to be onboarded again, access management checks upon request of the recipient mentioned on the Signature Page, whether there is a need-to-know and depending on the outcome, grants access or not.

Sensitive data (if appropriate) (only where applicable and permitted under national law)

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

N/A.

Data protection registration information of data exporter (where applicable)

N/A.

Additional Useful Information (storage limits and other relevant information)

The above categories of data will not be stored for longer than necessary for the legally permissible purpose(s) for which they were collected and as required under applicable retention policies and/or in accordance with applicable law.

Contact point for data protection enquiries:

as set out in the Information on Data Protection issued by the respective entity

**Annex B - 2
of Exhibit 1
Audit/Reporting**

Description of the transfer

Data Exporter(s)

The Commerzbank AG entities and branches listed in Signature Page.

Data Importer(s)

The Commerzbank AG entities and branches listed in Signature Page.

Data subjects

The personal data transferred concern, in particular, the following categories of data subjects:

1. Customers
2. Contact persons of corporate customers and potential corporate customers.
3. Individual representatives/ authorized signatories and/or authorized traders/directors (Senior Executives, Members of the Board or Governing Body) of corporate customers or potential corporate customers.

Purposes of transfer

The transfer is made, in particular, for the following purpose:

For internal audit purposes and reporting purposes.

The personal data will only be transferred if necessary for auditing and reporting reasons and to the extent in compliance with applicable law. It will be used on a need-to-know basis only.

Categories of data

The personal data transferred concern, in particular, the following categories of data:

1. Customers, e.g.
 - Full name / first names
 - Title
 - Function
 - email-address
 - phone, fax
 - concerned data of business relationship
2. Contact persons of (corporate) customers and of potential (corporate) customers, e.g.
 - Name
 - function,
 - phone, fax
 - e-mail address
3. Individual representatives/ Authorized signatories and/or authorized traders/directors (Senior Executives, Members of the Board or Governing Body) of (corporate) customers or of potential (corporate) customers, e.g.
 - Full name / first names
 - Title
 - Function

- email-address
- phone, fax

Recipients

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

- Commerzbank AG (Head office)
- Entities and branches listed in Signature Page if necessary for audit and/or reporting purposes (e.g. due to a matrix structure).

Sensitive data (if appropriate) (only where applicable and permitted under national law)

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

N/A.

Data protection registration information of data exporter (where applicable)

N/A.

Additional Useful Information (storage limits and other relevant information)

The above categories of data will not be stored for longer than necessary for the legally permissible purpose(s) for which they were collected and as required under applicable retention policies and/or in accordance with applicable law.

Contact point for data protection enquiries:

as set out in the Information on Data Protection issued by the respective entity

**Annex B - 3
of Exhibit 1
Global Trade Surveillance**

Description of the transferData Exporter(s)

The Commerzbank AG entities listed in Signature Page.

Data Importer(s)

The Commerzbank AG entities listed in Signature Page.

Data subjects

The personal data transferred concern, in particular, the following categories of data subjects:

Trade surveillance:

- Customers

Communication surveillance:

- Customers
- Potential customers

Purposes of transfer

The transfer is made for the following purpose:

For both, Trade and Communication Surveillance, the purpose is to adhere to legal requirements. Both systems have the purpose of preventing, detecting and identifying insider dealing, market manipulation and other suspicious trades and orders.

Categories of data

The personal data transferred concern, in particular, the following categories of data (only where applicable and permitted under national law):

- Trade Surveillance, e.g.
 - Order data
 - Trade data
 - Customer data data (e.g. Client or counterparty data, decision maker (asset management mandates, algo trade responsables, legal representative)
 - Market data
 - Research data
 - Static data (e.g. Portfolio hierarchy, instrument data)
 - Additional Compliance data (e.g. Watch List, Restricted List)
- for Communication Surveillance, e.g.
 - E-Mail data (e.g. sender, receiver, subject, text body)
 - Phone recordings (e.g. audio file, participant phone numbers)
 - Chat communication data (e.g. participants, messages)
 - Customer data

Recipients

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

The Commerzbank AG entities listed in Signature Page on a need-to-know basis. The alerts are analysed for suspicious activities within the respective local entity/branch. For trade surveillance further locations can be involved in the investigation process. For communication surveillance the results of the alerts may be provided to other Commerzbank AG entities listed in the Signature Page.

Sensitive data (if appropriate)

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

It is not anticipated to process special categories of personal data.

Data protection registration information of data exporter (where applicable)

N/A.

Additional Useful Information (storage limits and other relevant information)

The above categories of data will not be stored for longer than necessary for the legally permissible purpose(s) for which they were collected and as required under applicable retention policies and/or in accordance with applicable law.

Contact point for data protection enquiries:

as set out in the Information on Data Protection issued by the respective entity

**Annex B - 4
of Exhibit 1
Prevention of Anti-Money-Laundering and Counter-Terrorist-Financing**

Description of the transfer

Data Exporter(s)

The Commerzbank entities and branches listed in Signature Page.

Data Importer(s)

The Commerzbank entity listed in Signature Page.

Data subjects

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

1. Global PNG List:

- Customers, contact persons, representatives/authorized persons, keycontrollers and ultimate beneficial owners of corporate customers
- Persons included on local external lists

2. Information sharing via the Financial Crime Unit at Head Office: Customers, contact persons, representatives/authorized persons, keycontrollers and ultimate beneficial owners of corporate customers

3. Internal Reporting and Escalation: Customers, contact persons, representatives/authorized persons, keycontrollers and ultimate beneficial owners of corporate customers

Purposes of transfer

The transfer is made for the following purposes:

1. Global PNG List: Development and subsequent implementation and maintenance of global PNG List and AML/CTF prevention

2. Information sharing via the Financial Crime Unit (FCU) located at the compliance department of the Head Office: The purpose of FCU is to act as a centralized and dedicated unit for receiving, tracking, analysing and reporting financial crime events. The aim is to improve the group's capability to detect financial crime and to encounter adequate measures on a global level.

3. Internal Reporting and Escalation: As part of Internal Reporting and Escalation, certain information (e.g. information included in SARs, case escalation metrics, Subpoenas) may be required to be shared between Head Office, the branches and/or entities and business units (if necessary) pursuant to legal and regulatory requirements and/or internal policies and procedures. Internal reporting of metrics may be periodic or on an ad-hoc basis. Escalation may require transferring or remotely accessing data and/or client files (KYC file, Alerts, Cases) across locations and legal-entities.

Categories of data

The personal data transferred concern the following categories of data (only where applicable and permitted under national law):

1. PNG List:

- Customers and contact persons, representatives/authorized persons, keycontrollers and ultimate beneficial owners of (corporate) customers

- Name
- Address
- Nationality

- Birthplace
 - Birthdate
 - Position
 - Reason for inclusion on Global PNG List (if possible)
 - Commerzbank branch/entity which included the customer to Global PNG List
 - Persons included in local external lists
 - Name
 - Address
 - Nationality
 - Birthplace
 - Birthdate
 - Position
 - Reason for inclusion on Global PNG List (if possible)
2. Information sharing via the Financial Crime Unit
- KYC Customer data and supporting documentation;
 - Transaction Monitoring – transactional data and supporting documentation;
 - Suspicious Activity Reporting – including reports (SARs) reported to regulators;
 - Sanctions Hits – customer data, transactional data;
 - External data – e.g. Sanctions lists, high risk industry/entities list
 - Reports of Findings from Internal Audit, Regulator/Examiner or Compliance Desk reviews;
 - Whistleblowing data;
 - Latest personal client contact;
 - Name of relationship manager, operations/services officer, or compliance/regulatory officer;
 - FI Regulatory Services, Relationship Manager, Regional Head or Group Compliance input, approval, status and comments;
 - Watchlists, blacklists etc.;
 - Risk ratings (clients, countries, products);
 - Free text:
 - Descriptions of major risk issues that are related to money laundering, terrorist financing or sanctions, or any other aspect of the AML / CTF/Sanctions compliance program;
 - AML / CTF / Sanctions investigations undertaken by any branches / subsidiaries or regulatory body;
 - Information regarding "de-risked" / denied customers and products / services for compliance reasons from other locations;
 - Control gaps (e.g., categories of transactions that should be alerting the monitoring system but are not);
 - Material internal or external audit findings; and regulatory breaches
3. Internal Reporting and Escalation:
- Customer data (e.g. Customer name, Party information, address information, tax identifier information, transacting counterparty data)
 - Account data (e.g. Account details, activity limits)
 - Products and services data (e.g. Types of products and services used, Risk ratings, expected activity)
 - Transaction data
 - Reference data (e.g. Country risk rating)
 - External request data (e.g. Subpoena, third-party requests)
 - Data regarding ultimate beneficial ownership, PEP status or authorized persons
 - Alert-level per customer: No. of closed alerts, trigger of alert (standardized reasons for case/no details)
 - Case-level per customer: No. of closed cases, trigger of case (standardized reasons for case/no details)
 - Regulatory reports files (e.g. SAR) (y/n; no details shared unless legally permissible), and action taken (i.e. no action, conditioned action, or termination)
 - RFI: No. of outgoing/incoming RFI's, Evaluation RFI response (Analyst evaluates response via score)

Recipients

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

1. Global PNG List:

- Commerzbank AG Head office for creation of Global PNG List for its purposes
- Global PNG List to be provided to other entities and branches listed in Signature Page for their purposes on a need-to-know-basis

2. Information sharing via the Financial Crime Unit at Head Office:

All relevant branches and group entities/subsidiaries report relevant AML/Sanctions events to Financial Crime Unit at Head Office in a structured process. Financial Crime Unit at Head Office to monitor and analyze global developments and changing patterns regarding financial crimes. Financial Crime Unit at Head Office may share relevant information within GM-CO, Frankfurt (Germany) as well as the individual compliance departments in all relevant branches and group entities/subsidiaries on a need-to-know-basis

3. Internal Reporting and Escalation: Commerzbank AG Head office, other branches and entities listed in Signature Page**Sensitive data (if appropriate)**

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

N/A.

Data protection registration information of data exporter (where applicable)

N/A.

Additional Useful Information (storage limits and other relevant information)

The above categories of data will not be stored for longer than necessary for the legally permissible purpose(s) for which they were collected and as required under applicable retention policies and/or in accordance with applicable law.

Contact point for data protection enquiries:

as set out in the Information on Data Protection issued by the respective entity

**Annex B - 5
of Exhibit 1
Risk Assessments**

Description of the transfer

Data Exporter(s)

The Commerzbank AG entities and branches listed in Signature Page.

Data Importer(s)

The Commerzbank AG entities and branches listed in Signature Page.

Data subjects

The personal data transferred concern, in particular, the following categories of data subjects:

- Existing and/or potential new customers for credit risk (risk assessment/risk management) i.e. credit analysis, credit decision and credit monitoring

Purposes of transfer

The transfer is made for the following purposes:

In order to check all credits concerning the customer, including credits of the customer's group companies and shareholders

Categories of data

The personal data transferred concern, in particular, the following categories of data (only where applicable and permitted under national law):

- for credit risk of customers [assessment/management], e.g.
 - Credit risk assessment relevant data (financial information, Balance Sheet, Rating, etc.)
 - Market data
 - Research data
 - Static data (e.g. KYC data)
 - Additional Compliance data (e.g. Watch List, Restricted List)
 - Credit Risk data (Credit Agreement data, credit line and exposure data)

Recipients

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

The Commerzbank AG entities and branches listed in Signature Page on a need-to-know basis.

Sensitive data (if appropriate)

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

N/A.

Data protection registration information of data exporter (where applicable)

N/A.

Additional Useful Information (storage limits and other relevant information)

The above categories of data will not be stored for longer than necessary for the legally permissible purpose(s) for which they were collected and as required under applicable retention policies and/or in accordance with applicable law.

Contact point for data protection enquiries:

as set out in the Information on Data Protection issued by the respective entity

**Annex C
of Exhibit 1
Local Law Amendments**

The below local law amendments apply if the Data Exporter is subject to the jurisdiction of the respective country:

I. Country specific

| # | Country | Amendments |
|----|--|--|
| 1. | Hungary | <p>Power of Attorney</p> <p>To the extent the Data Importer or Data Exporter is located in Hungary, Data Importer/Data Exporter hereby grants, to the extent permitted by law, pursuant to this clause, a power of attorney to Commerzbank AG to act as the party's authorized representative for the purposes of executing (i) any amendments to this DPGA, including without limitation additions of further or amendments to existing data processing activities; and (ii) any agreements to include additional entities or branches as Data Exporter and/or Data Importer to this DPGA. Commerzbank AG shall, within a reasonable time, notify in writing the relevant party of any documents signed by it pursuant to the authorization granted to this DPGA.</p> |
| 2. | Italy | <p>Clause 4 sentences 4 and 5 of the Main Body of the DPGA are replaced by the following: "Commerzbank AG will communicate the above amendments to the entities party to this agreement by written notice with confirmation of receipt (including electronic form) - sent at least fifteen (15) days before the effective date of the proposed amendments. Such amendments will be deemed accepted by the entities party to this agreement, if the respective entity does not withdraw in writing from the agreement within thirty (30) days after having received the above notice."</p> |
| 3. | China (which, when referring to jurisdiction, does not include Hong Kong, Macau and Taiwan) | <p>In case the Data Exporter is located in China, Exhibit 1 shall be amended as follows:</p> <ol style="list-style-type: none"> The term "Community" and "European Economic Area (EEA)" in Exhibit 1 shall be replaced with the term "PRC". The term "Directive 95/46/EC of 24 October 1995", "Article 25(6) of Directive 95/46/EC", "Directive 95/46/EC" and "Article 12 of Directive 95/46/EC" in Exhibit 1 and its Annex A shall be replaced with the term "the applicable data protection law". The term "special categories of data/sensitive data", "sensitive data", "categories of sensitive data and "special categories of personal data" in Exhibit 1 and its Annexes shall be replaced with the term "sensitive personal data". Paragraph (a) under the section "Definitions" shall be restated as follows: <ol style="list-style-type: none"> "personal data", "sensitive personal data", "process/processing", "controller", "processor", "data subject" and "supervisory authority/authority" shall have the same meaning as ascribed to it under the applicable data protection law (whereby "the authority" shall mean the competent data protection authority in the People's Republic of China ("PRC")); The following paragraph shall be added to the section "Definitions" as the new Paragraph (e): <ol style="list-style-type: none"> "the applicable data protection law" shall mean the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the PRC in which the data exporter is established. |

| | | |
|----|-----------|---|
| | | <p>6. Subparagraph (ii) of Paragraph (h) of Clause II (<i>Obligations of the data importer</i>) shall be deleted in its entirety and the subparagraph thereafter shall be renumbered sequentially and all cross-references in Exhibit 1 shall be renumbered accordingly.</p> <p>7. Paragraph (i) of Clause II (<i>Obligations of the data importer</i>) shall be restated as follows:</p> <p>(i) It will not disclose or transfer the personal data to a third party data controller unless:</p> <p>(i) it notifies the data exporter of the disclosure or transfer; and</p> <p>(ii) the relevant data subjects have been informed of the purposes, manner and scope of the disclosure or transfer of personal data, the categories of recipients and the fact that the countries to which data is exported may have different data protection standards, and have consented to the same prior to the disclosure or transfer.</p> <p>8. Paragraph (c) of Clause VI (<i>Termination</i>) shall be deleted in its entirety and the paragraph thereafter shall be renumbered sequentially and all cross-references in Exhibit 1 shall be renumbered accordingly.</p> <p>9. Paragraph (c) (the original Paragraph (d)) of Clause VI (<i>Termination</i>) shall be restated as follows:</p> <p>(c) The parties agree that the termination of these clauses at any time, in any circumstances and for whatever reasons, does not exempt them from the obligations and/or conditions under the clauses as regards the processing of the personal data transferred.</p> <p>10. Data Processing Principle 7 of Annex A of Exhibit 1 shall be restated as follows:</p> <p>7. Data used for marketing purposes: The data importer may only process the personal data for the purposes of direct marketing provided that the data subject has consented to such processing. Where data is processed for the purposes of direct marketing, effective procedures should exist to allow the data subject to "opt-out" at any time from having his/her data used for such purposes.</p> |
| 4. | Hong Kong | <p>In case the Data Exporter is located in Hong Kong, Exhibit 1 shall be amended as follows:</p> <p>1. The terms "Community", "European Economic Area (EEA)" and "EU" shall be replaced with the term "Hong Kong Special Administrative Region of the People's Republic of China".</p> <p>2. The term "Commission" shall be replaced with the term "authority".</p> <p>3. The terms "Directive 95/46/EC of 24 October 1995", "Directive 95/46/EC", "Article 25(6) of Directive 95/46/EC", and "Article 12 of Directive 95/46/EC" shall be replaced with the term "Personal Data (Privacy) Ordinance (Cap. 486 of Laws of Hong Kong)", except for where it is used in the definition of "special categories of data/sensitive data".</p> <p>4. The following definitions shall replace those set out in Exhibit 1:</p> <ul style="list-style-type: none"> "controller" shall have the meaning given to "data user" in the Personal Data (Privacy) Ordinance (Cap. 486 of Laws of Hong Kong). |

| | | |
|----|-------|---|
| | | <ul style="list-style-type: none"> • "processor" shall have the meaning given to "data processor" in the Personal Data (Privacy) Ordinance (Cap. 486 of Laws of Hong Kong). • "data subject" shall have the same meaning given in the Personal Data (Privacy) Ordinance (Cap. 486 of Laws of Hong Kong). • "supervisory authority/authority" shall have the same meaning given to "Commissioner" in the Personal Data (Privacy) Ordinance (Cap. 486 of Laws of Hong Kong). <p>5. In Clause 5 of Annex A of Exhibit 1, replace "Rights of access, rectification, deletion and objection: ... The burden of proof for any refusal rests on the data importer, and the data subject may always challenge a refusal before the authority." with:</p> <p>"Rights of access and rectification: Data subjects must, whether directly or via a third party, be provided with the personal information about them that an organization holds, except for requests for which access need not be granted under the applicable data protection law. Data subjects must be able to have the personal information about them rectified where it is inaccurate."</p> |
| 5. | Japan | <p>In case the Data Exporter is located in Japan, Exhibit 1 shall be amended as follows:</p> <ol style="list-style-type: none"> 1. The term "Community" and "EU" shall be replaced with the term "Japan", the term "European Economic Area ("EEA") shall be replaced with the term Japan, EEA and UK. 2. The term "Commission" shall be replaced with the term "authority". 3. The term "Directive 95/46/EC of 24 October 1995", "Directive 95/46/EC" and "Article 25(6) of Directive 95/46/EC" in the Agreement shall be replaced with the term "Act on the Protection of Personal Information (Act No. 57 of May 30, 2003, as amended) and all related regulations". 4. The following definitions shall replace those set out in Exhibit 1: "special categories of data/sensitive data (要配慮個人情報)", "controller (個人情報取扱事業者)", "data subject (本人)", and "supervisory authority/authority (個人情報保護委員会)" shall have the same meaning as in the Act on the Protection of Personal Information (Act No. 57 of May 30, 2003, as amended) and all related regulations (whereby "the authority" shall mean the competent data protection authority in the territory in which the data exporter or data importer is established). 5. The Data Importer shall take all reasonable measures to ensure its employees comply with all necessary and appropriate security measures under the Act on the Protection of Personal Information (Act No. 57 of May 30, 2003, as amended) and all related regulations, and implement necessary and appropriate monitoring of employees activities. "all reasonable measures" include providing quality and frequent training for employees on company rules and practices relating to the security measures and conducting audits of employees" compliance with the company rules and practices on a regular basis. 6. Where the Data Importer transfers the personal data to a third party regardless of whether the third party is located in Japan or outside Japan, the Data Importer shall do this using a means compliant with the Act on the Protection of Personal Information (Act No. 57 of May 30, 2003, as amended) and all related regulations, but where uncertain, shall default to obtaining consent for the data transfers from data subjects. |

| | | |
|----|-------------|--|
| 6. | Singapore | <p>In case the Data Exporter is located in Singapore,</p> <ul style="list-style-type: none"> • Exhibit 1 shall be amended as follows: <ol style="list-style-type: none"> 1. The term "Community" and "European Economic Area (EEA)" in Exhibit 1 shall be replaced with the term "Singapore". 2. The term "Commission" shall be replaced with the term "authority". 3. The terms "Directive 95/46/EC", "Article 25(6) of Directive 95/46/EC", and "Article 12 of Directive 95/46/EC" shall be replaced with the term "Personal Data Protection Act", except for where it is used in the definition of "special categories of data/sensitive data", "controller" and "processor". 4. The term "EU" shall be replaced with the term "Singapore". 5. The following definitions shall replace those set out in Exhibit 1: <ol style="list-style-type: none"> a) "personal data" shall have the same meaning given in the Personal Data Protection Act. b) "process/processing" shall have the same meaning given in the Personal Data Protection Act. c) "supervisory authority/authority" shall have the same meaning given to "Commissioner" in the Personal Data Protection Act. 6. The following definition shall be included in Exhibit 1 as paragraph (e) under "Definitions": <p style="margin-left: 40px;">"Personal Data Protection Act" shall mean Singapore's Personal Data Protection Act including all subsidiary legislation enacted thereunder, whether now or in the future.</p> • and, clause 1.6 of this DPGA notwithstanding, <p>For the avoidance of doubt, it will not be considered an inconsistency with this DPGA if the provisions in any other agreement between the Parties in relation to the subject-matters addressed herein serve as a clarification or extension of the provisions in this DPGA and/or imposes a stricter obligation on a Party.</p> |
| 7. | Switzerland | <p>In case the Data Exporter is located in Switzerland, Exhibit 1 shall be amended, as follows:</p> <ol style="list-style-type: none"> 1. "personal data", "special categories of data/sensitive data", "personality profiles", "process/processing", "controller", "processor", "data subject" and "supervisory authority/authority" shall have the meaning assigned to them by the Swiss Federal Act on Data Protection of June 19, 1992 ("DPA") including the relevant amendments and its implementing ordinances, (whereby "the authority" shall mean the competent data protection authority in the territory in which the data exporter is established); 2. 'the applicable law' shall mean the legislation protecting the fundamental rights and freedoms of natural and legal persons, including the Swiss Federal Data Protection Act of June 19, 1992 including the relevant amendments and its implementing ordinances; 3. 'White-List Country' shall mean a country, which is found by decision of the Swiss Federal Data Protection and Information Commissioner to ensure an adequate level of data protection according to Swiss standards; |

| | | |
|----|----------------|--|
| | | <p>4. The Data Importer acknowledges and agrees that the personal data transferred to Data Importer by Data Exporter may include personal data of legal persons and personality profiles of natural persons. The Data Importer shall process personal data of legal persons in the same manner as other personal data as long as this requirement exists under Swiss data protection law and personality profiles in the same manner as special categories of data;</p> <p>5. The DPA requires equal to the European law Data Exporters in Switzerland to provide appropriate safeguards for transfers of personal data to controllers in non-EU/EEA countries and outside Switzerland. Such appropriate safeguards can be adduced by requiring the Data Importers to enter into the Standard Contractual Clauses for the Transfer of Personal Data to Third Countries ("Model Contract C2C") pursuant to Commission Decision 2004/915/EC of 27 December 2004.</p> |
| 8. | United Kingdom | <p>In relation to any transfers of personal data from the United Kingdom to outside of the United Kingdom, clauses 1.2 to 1.5 of the Main Body of the DPGA shall apply and the Model Contract C2C shall apply to the extent permissible under data protection laws in the United Kingdom if personal data is transferred to a jurisdiction which is</p> <p>(a) not subject to an arrangement with the United Kingdom (or transitional arrangements under the laws of the United Kingdom) permitting the transfer of personal data from the United Kingdom to the jurisdiction in which the Data Importer is located; or</p> <p>(b) not subject to an adequacy decision or similar decision (or transitional arrangement) under the laws of the United Kingdom permitting the transfer of personal data to jurisdictions outside of the United Kingdom.</p> |

II. Supplementary Measures for Data Exporters located in the EU

| | |
|----|--|
| 1. | Unless prohibited by applicable law, data importer shall inform the data exporter in general terms about requests, orders or similar demands by a court, competent authority, law enforcement or other government body ("Judicial or Governmental Information Request) relating to the processing of personal data under these Clauses. |
| 2. | Data importer shall object to and challenge any "Judicial or Governmental Information Request by taking legal remedies to the extent they are reasonable given the circumstances. If compelled to disclose personal data transferred under these Clauses by a "Judicial or Governmental Information Request, data importer will give data exporter reasonable notice to allow data exporter to seek a protective order or other appropriate remedy unless data importer is legally prohibited from doing so. |
| 3. | Should a new/updated version of the Clauses become available, data importer shall upon data exporter's request agree to the new/amended version of the Clauses. |
| 4. | Notwithstanding other restrictions, in case data importer makes personal data available to processors, data importer will select processors in a third country only after a due diligence that entails (i) a review of any transparency reports made available by processor, (ii) and carrying out a transfer risk assessment prior to the engagement of processor. |
| 5. | In case data importer makes personal data available to a third party data controller, data importer will obligate the third party data controller to comply with the aforementioned sections 1. to 4. |

Exhibit 2: Model Contract C2P

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

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Clause 1 Definitions

For the purposes of the Clauses:

- (a) "personal data", "special categories of data", "process/processing", "controller", "processor", "data subject" and "supervisory authority" shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
- (b) "the data exporter" means the controller who transfers the personal data;
- (c) "the data importer" means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
- (d) "the sub-processor" means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
- (e) "the applicable data protection law" means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
- (f) "technical and organisational security measures" means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration,

unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2 Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3 Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4
Obligations of the data exporter

The data exporter agrees and warrants:

- (a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
- (b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
- (c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
- (d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
- (e) that it will ensure compliance with the security measures;
- (f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
- (g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection

supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

- (h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
- (i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
- (j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5
Obligations of the data importer

The data importer agrees and warrants:

- (a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
- (d) that it will promptly notify the data exporter about:
 - (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve

the confidentiality of a law enforcement investigation,

- (ii) any accidental or unauthorised access, and
 - (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
- (e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
- (f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
- (g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
- (h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;
- (i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;
- (j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 6 Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7 Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
 - (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
 - (b) to refer the dispute to the courts in the Member State in which the data exporter is established.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance

with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

Signatures: See Signature Page

**Appendix 1.1
of Exhibit 2
Centralization of Onboarding/Offboarding**

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Data Exporter

Commerzbank entity and/or branch listed in Signature Page.

Data Importer

The Data Importers are:

- **Commerzbank AG, Germany**, the head office and parent company. Receives personal data from all Commerzbank entities and branches listed in Signature Page.
- 3 Hubs:
 - **Commerzbank AG, New York Branch** receives personal data from Commerz Markets LLC and from Commerzbank entity in Brazil
 - **CERI International Sp. Z.o.o., Poland** receives personal data from the entities/branches in Austria, Belgium, Czech Republic, France, Germany, Hungary, Italy, Luxembourg, the Netherlands, Slovakia, Spain, UK, Switzerland
 - **Singapore Branch** receives personal data from Dubai Branch in UAE

Data subjects

The personal data transferred concern, in particular, the following categories of data subjects (please specify):

1. Customers
2. Contact persons of corporate customers and of potential corporate customers.
3. Individual representatives/ Authorized signatories and/or authorized traders/directors (Senior Executives, Members of the Board or Governing Body) of (corporate) customers or of potential (corporate) customers
4. Ultimate beneficial owners/Shareholders of (corporate) customers and of potential (corporate) customers.

Categories of data

The personal data transferred concern, in particular, the following categories of data (please specify) (only where applicable and permitted under national law):

1. Customers, e.g.
 - Full name / first names
 - Title
 - Date and place of birth (depending on local requirements of Sales location)
 - Passport/identity card details (copy of document if exceptionally required normally provided).
 - Private address / Country of residence
 - investment percentage
 - Citizenship
 - PEP status and PEP information
 - Position/function in company
 - Tax residency
 - Tax Identification No. (TIN)
 - PEP information
 - Source of wealth, if required
 - Results of screening and negative news search

2. Contact persons of (corporate) customers and of potential (corporate) customers, e.g.
 - Name
 - function,
 - phone, fax
 - e-mail address
3. Individual representatives/ authorized signatories and/or authorized traders/directors (Senior Executives, Members of the Board or Governing Body) of (corporate) customers or of potential (corporate) customers, e.g.
 - Full name / first names
 - Title
 - Function
 - email-address
 - phone, fax
 - Date and place of birth (depending on local requirements of Sales location)
 - Passport/identity card details (copy of document normally provided)
 - Private address / Country of residence
 - Citizenship
 - PEP information
 - Tax ID
 - Results of screening and negative news search
4. Ultimate Beneficial Owners/Shareholders of (corporate) customers or potential (corporate) customers, e.g.
 - Full name / first names
 - Title
 - Date and place of birth (depending on local requirements of Sales location)
 - Passport/identity card details (copy of document if exceptionally required)
 - Private address / Country of residence
 - investment percentage
 - Citizenship
 - PEP status and PEP information
 - Position/function in company
 - Tax residency
 - Tax Identification No. (TIN)
 - PEP information
 - Source of wealth, if required
 - Results of screening and negative news search

Special categories of data (if appropriate and only where applicable and permitted under national law)

N/A

Processing operations

The personal data transferred will be subject to the following basic processing activities:
Collection and transfer, as well as storage.

Subject matter of the processing

The local client owner of the local Commerzbank legal entity or local branch office collects all relevant customer data (see above) directly from the customer and transfers it electronically to the respective Hub (if applicable). The central data storage of all relevant customer data will be with the head office in Germany. On-boarding, customer due diligence and off-boarding process for corporate client segment is performed by specialists and centralized in three Hubs (if applicable). In this context the Hub will check completeness of data and documents, verify against supporting documents and start the screening process (PEP, sanction lists, etc.). The Hub will also have access to risk evaluations and KYC scores. The final decision will remain with local client owner.

Nature and purpose of the processing

Centralization of onboarding process, customer due diligence and off-boarding process in order to have an aligned approach worldwide.

Signatures: See Signature Page

**Appendix 1.2
of Exhibit 2
Global Trade Surveillance**

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Data Exporter

Commerzbank entity and/or branch listed in Signature Page.

Data Importer

The Data Importer is:

- **Commerzbank AG, Germany**, as the host provider for the system for Trade Surveillance and for Communication Surveillance and where the Global Control Room is located

Data subjects

The personal data transferred concern, in particular, the following categories of data subjects (please specify):

Trade surveillance:

- Customers

Communication surveillance:

- Customers
- Potential customers

Categories of data

The personal data transferred concern, in particular, the following categories of data (please specify) (only where applicable and permitted under national law):

Trade surveillance, e.g.

- o Order data
- o Trade data
- o Customer data (e.g. Client or counterparty data, decision maker (asset management mandates, algo trade reponsibles, legal representative)
- o Market data
- o Research data
- o Static data (e.g. Portfolio hierarchy, instrument data)
- o Additional Compliance data (e.g. Watch List, Restricted List)

Communication Surveillance (for trade staff, customers and potential customers), e.g.

- o E-Mail data (e.g. sender, receiver, subject, text body)
- o Phone recordings (e.g. audio file, participant phone numbers)
- o Chat communication data (e.g. participants, messages)
- o Customer data/Potential customer data (e.g. E-Mail address, phone number, name, content of communication)

Special categories of data (if appropriate and only where applicable and permitted under national law)

It is not anticipated to process special categories of personal data.

Processing operations

- Processing operation #1 (= generating alert by system): Commerzbank AG Frankfurt is hosting the system that analyses the communication and the trades from entities and branches worldwide automatically. If there is a suspicious hit, an alert will be created automatically by the system. Commerzbank AG Frankfurt is acting as a data processor on behalf of the respective entities/branch and in particular analyses based on rules specified by each branch/entity.
- Processing operation #2 (= review and analysis of alert): Following an alert under processing operation #1 above, the process for trade surveillance is as follows :
- Global Control Room based in Frankfurt will review and analyse the alert (on behalf of the respective entity or branch). If the alert cannot be resolved, it will be handed over to the second level review - the Local Control Room which is the respective local compliance officer

Subject matter of the processing

Surveillance of trade and communication pursuant to legal requirements.

Nature and purpose of the processing

For both, Trade and Communication Surveillance, the purpose is to adhere to legal requirements. Both systems have the purpose of preventing, detecting and identifying insider dealing, market manipulation and other suspicious trades and orders.

Signatures: See Signature Page

**Appendix 1.3
of Exhibit 2
Anti-Money-Laundering and Counter Terrorism Prevention**

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Data Exporter

Commerzbank entity and/or branch listed in Signature Page.

Data Importer

The Data Importer is Commerzbank AG, Head Office

Data subjects

The personal data transferred concern, in particular, the following categories of data subjects (please specify):

1. Name Screening: customer, ultimate beneficial owner, authorized person, keycontroller of (corporate) customer
2. Customer Risk Rating: customer ultimate beneficial owner, authorized person, keycontroller of (corporate) customer
3. Transaction Monitoring and Sanction Screening: customer, ultimate beneficial owner, authorized person, keycontroller of corporate customer

Categories of data

The personal data transferred concern, in particular, the following categories of data (please specify) (only where applicable and permitted under national law):

1. Name Screening, e.g.:
 - name,
 - address,
 - birthdate,
 - birthplace
 - nationality
 - position
2. Customer Risk Rating, e.g.:
 - Country information (legal address, country of incorporation/nationality)
 - Customer type
 - Industry type
 - Legal form
 - Product and services types
 - Distribution channels / communication, e.g. online
 - Specific (or pre-defined) risk scenarios
 - Transaction activity (actual and expected)
 - PEP status
 - Information on material negative news
 - Behaviour of the customer, e.g. in context with case management,
 - Transaction monitoring and SAR filing
 - Information on Sanctions, e.g. OFAC SDN
 - Risk Rating Result (e.g. risk score and / or rating: low, medium, high)
3. Transaction Monitoring and Sanctions Screening, e.g.

- Client data (e.g. Customer and Party information, address details, risk-rating, tax identifier information, transacting counterparty data, beneficial ownership, PEP status)
- Account data (e.g. Account details, activity limits, settlement accounts, settlement instructions, lifecycle dates)
- Products and services data (e.g. Risk ratings, expected activity, interest rates, security identifiers and details)
- Transaction data (Transactions, trades, transfers, change of addresses, audit events, cancellations/amendments, asset balances, loan information etc.)
- Reference data (e.g. Bank data, Country risk rating, whitelists, prior alerts, prior SARs)
- External data (e.g. Subpoena, third-party requests, sanction lists)
- Financial crime event related Alert and Case data (Historical alerts, alert disposition details, alert escalation, documentation, regulatory reporting etc.)

Special categories of data (if appropriate and only where applicable and permitted under national law)

N/A.

Processing operations

Centralizing of the processes:

1. Name Screening:

- Comparison of personal customer information with
 - Global PNG List
 - Other internal Persona non Grata lists which are not included Global PNG List
 - External lists provided by external vendor, e.g. Factiva (PEP, Sanctions, other lists)
- Hit: Head Office provides relevant information to requesting branch/entity.

2. Customer Risk Rating: Calculate risk

3. Transaction Monitoring and Sanctions Screening: Consistently monitoring of client activity across several countries worldwide. The Compliance team at Head Office conducting the review of client activity and alerts may need to remotely access data (view, edit, extract, store etc.).

Subject matter of the processing

1. Name screening: Name Screening against lists.
2. Customer Risk Rating: Calculation of risk rating.
3. Transaction Monitoring and Sanctions Screening: Monitoring of activities, review, analysing and handling of alerts; viewing transactional history and previous alerts, cases and documentation.

Nature and purpose of the processing

1. Name Screening: Name Screening against this Global PNG List, other internal (local) Persona non Grata lists and external lists (sanction, PEP/relatives/associates and negative information) for Anti-Money-Laundering and Counter Terrorism Prevention).

2. Customer Risk Rating: In order to determine the risk rating of the customer, customer attributes such as country of incorporation, product usage, PEP status, transactional behavior etc. are used in order to determine the risk rating of the customer. Head Office calculates the risk rating, and sends the results back to Data Exporter.

3. Transaction Monitoring and Sanction Screening: Development and implementation of Global Transaction Monitoring (1st level AML transaction monitoring) including Alert and Case management and sanctions screening which includes the screening of domestic and international payments against global and local sanctions lists.

Signatures: See Signature Page

| |
|--|
| <p style="text-align: center;">Appendix 2 of Exhibit 2 Technical and Organizational Security Measures</p> |
|--|

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organizational security measures implemented by the Data Importer in accordance with Clauses 4(d) and 5(c):

A. General

Sec. 1 Technical and organisational security measures to ensure an adequate data protection level

| |
|---|
| (1a) Measures to pseudonymise and anonymise personal data: |
| <ul style="list-style-type: none"> • Development of data protection concepts for IT systems or a group of IT systems if personal data of natural persons are processed within the scope of application of the GDPR (within the EU). • As a matter of principle, production data will not be transferred to and used in development and test environments of the IT system. If this should be mandatory, however, any data will be anonymised sufficiently before transfer. The methods of anonymisation are decided case-by-case. Any deviations must undergo a standardised exception process. |

Explanation:

Pseudonymisation means processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. An anonymisation takes place if such additional information does not exist or is erased irrevocably.

An existing documentation (e.g. in a data protection or security concept) can also be indicated.

| |
|--|
| 1b) Measures to encrypt personal data: |
| <ul style="list-style-type: none"> • Development of safety concepts via a centralised safety analysis application of Commerzbank for IT applications that process personal data and for IT infrastructures. • Encoding measures as set forth in the policy of the bank (Information Security Control Framework). Depending on the data classification determined by the centralised safety analysis application of Commerzbank (confidentiality level of the data) of the IT applications and the type of processing (such as storing, transmitting), the data shall be encoded in accordance with the defined encoding matrix by the cryptographic processes allowed in the bank in accordance with the technical standard. |

Explanation:

Encryption of personal data is a common practice to protect such data from disclosure to unauthorised individuals.

An existing documentation (e.g. in a data protection or security concept) can also be indicated.

| |
|---|
| (1c) Measures to ensure ongoing confidentiality: |
|---|

- Development of data protection concepts for IT systems or a group of IT systems if personal data are processed within the scope of application of the GDPR (within the EU).
- Development of safety concepts via a centralised safety analysis application of Commerzbank for IT applications that process personal data and for IT infrastructures.
- Identification of IT applications which are likely to have a high risk pursuant to article 35 GDPR within the framework of the safety analysis process.
- In addition, these applications will undergo a standardised process for the Privacy Impact Assessment the result of which, in turn, will be taken into account when developing the safety concept.
- Encoding measures; see Sec. 1 (1b).
- The assignment of authorisations to IT application will be done via a standardised process according to the principle of minimum rights ("need-to-know").
- Measures regarding admission control; see sec. 2 (2b).
- Measures regarding access control; see sec. 2 (2c).
- Measures regarding transfer control; see sec. 2 (2d).

Explanation:

This means measures ensuring adequate security of the personal data including protection against unauthorised unlawful processing as well as unintentional loss, unintentional destruction or unintentional damages. These measures must be designed to ensure ongoing confidentiality.

An existing documentation (e.g. in a data protection or security concept) can also be indicated.

| (1d) Measures to ensure ongoing integrity: |
|--|
| <ul style="list-style-type: none"> • Development of data protection concepts for IT systems or a group of IT systems if personal data of natural persons are processed within the scope of application of the GDPR (within the EU). • Development of safety concepts via a centralised safety analysis application of Commerzbank for IT applications that process personal data and for IT infrastructures. • Conditions applicable to the development of software for the IT system for input validation. • Any changes to software, hardware and other IT infrastructure used in production shall be made in accordance with a centralised/standardised Change Management Process. • Security Logging and Monitoring shall be carried out in accordance with the method of Security Information and Event Management (SIEM) within the framework of operating a Security Operation Centre (SOC). • Measures regarding input control; see Sec. 2 (2e). • Measures regarding transfer control; see Sec. 2 (2d) |

Explanation:

This means measures ensuring adequate security of the personal data including protection against unauthorised or unlawful processing as well as unintentional loss, unintentional destruction or

unintentional damages as well as unauthorised changes. These measures must be designed to ensure ongoing integrity.

An existing documentation (e.g. in a data protection or security concept) can also be indicated.

| (1e) Measures to ensure ongoing availability: |
|---|
| <ul style="list-style-type: none">• Use of fire protection devices (smoke and fire detectors, fire extinguishers, fire doors, fire extinguishing systems) in the computing centre and the IT technology rooms.• Use of a system to detect a break in.• Use of the failsafe electricity supply (FES).• Air conditioning in the computing centre and the IT technology rooms.• System detecting damages caused by water.• Data backup and data export (redundant data management).• Threat and risk analysis per application with preventive measures.• Use of backup processes.• Use of antivirus systems (centralised and decentralised).• Use of SPAM and content filters.• Having an emergency, work-around and restart concept in place.• Training, instructions, and annual exercises.• Monitoring the availability of infrastructure components and application/databases through the system in accordance with the criticality of the data to be processed.• Possible production failures will be documented, processed and, if necessary, escalated by a centralised incident/problem management process. |

Explanation:

This means measures ensuring that personal data are protected against accidental destruction or loss. These measures must be designed to ensure ongoing availability.

An existing documentation (e.g. in a data protection or security concept) can also be indicated.

| (1f) Measures to ensure ongoing resilience of the systems and services: |
|--|
| <ul style="list-style-type: none">• Centralised capacity management (load balancing; for important applications, key performance indicators will be defined and monitored).• Conducting penetration tests for web applications. |

Explanation:

This includes measures, for example, which have to be taken before data processing is carried out by the controller and the processor (cf. 2i). However, continuous monitoring of the systems may also be required.

An existing documentation (e.g. in a data protection or security concept) can also be indicated.

(1g) Measures for timely restoring availability in case of a physical or technical incident:

- Written emergency plan in accordance with the BCM framework (acc. to ISO 22301) for all processes and units applicable throughout the Group.
- Regular emergency tests for critical processes including the necessary resources (IT products).
- Resilient attachment to the IT infrastructure/IT systems (backup for the computing centre and server) so as to realise the brief storage times defined by the criticality of the processes.
- A control function to ensure compliance with policy is integrated into the emergency plan and test.

Explanation:

In order to ensure restorability sufficient safeguards on the one hand and plans of measures on the other are conceivable which are capable of restoring operations in case of disaster scenarios (and if necessary the foundation of the backup).

An existing documentation (e.g. in a data protection or security concept) can also be indicated.

(1h) Measures for regular testing, assessing and evaluating of the effectiveness of technical and organisational measures:

- Continuous improvement process in the information safety management system (ISMS).
- Regular compliance checks for IT systems processing personal data within the scope of the centralised safety analysis process of Commerzbank. The results of these checks will be included in existing risk analyses for modification of the safety concepts.
- Verification of compliance with the conditions on information safety by risk-oriented tests (on the basis of the relevant security compliance checks) by a second line of defence.
- Control measures within the framework of the internal control system (ICS).

Explanation:

Measures especially designed to keep the measures for data security described here up to date.

An existing documentation (e.g. in a data protection or security concept) can also be indicated.

Sec. 2 Additional technical and organisational measures unless stated under Sec. 1

(2a) Measures to deny unauthorised individuals access to data processing facilities (admission control through physical security measures):

- Classification of the buildings/areas in different safety and protection zones.
- Using a system to detect break in.
- Camera surveillance of the grounds and entrance areas.
- The buildings of Commerzbank AG have electronic admission systems. These systems permit employees free access to the building during the regular working hours. Extraordinary assignments and associated admission to the buildings need to be applied for separately.

- Visitors, suppliers and other third parties must first register with reception. Their presence will be recorded in writing. Any visitors' passes must be worn openly and returned when leaving the building.
- In addition to safeguarding the buildings by the general electronic admission control, the entrances to the rooms of the computing centres are partly secured biometrically and by badge readers.
- Access to the computing centre by individual admission systems.
- External individuals will be accompanied by authorised employees in the special protection zones (such as, among others, the computing centre, the technology rooms).
- Special authorisation processes for access to certain special protection zones.
- Transparency and the possibility of analysing admissions.

Explanation:

This means measures denying unauthorised individuals access to buildings and computing centres where personal data are processed. In this connection, measures are taken to ensure that only individuals with proper authorisation are admitted to the buildings and computing centres.

An existing documentation (e.g. in a data protection or security concept) can also be indicated.

(2b) Measures to **prevent unauthorised individuals from using data processing systems** (controlling access to data processing systems):

- Access to Commerzbank systems through a personalised user ID and password.
- Administration of authorisation systems for use of the Commerzbank systems.
- Application and change management for granting or withdrawing access authorisations, logging of all activities performed.
- Sealing-off of the bank's internal networks by firewalls.
- Manual and automatic screen lock.
- Separation between development, test and production environments.
- Protection of transmission lines and the data stream, for example by encoding via VPN.
- Annual checking of identifications (for example, are they up-to-date or inactive).
- Logging user activities (the logging in and logging out, failed attempts).
- Security Logging and Monitoring will be conducted in accordance with the method of Security Information and Event Management (SIEM) in connection with the operation of a Security Operation Centre (SOC).

Explanation:

This means measures preventing unauthorised individuals from using data processing facilities and processes. In this connection, measures are taken to ensure that only individuals with proper authorisation have access to the data processing facilities. These include, for example, suitable password rules and firewall configurations.

An existing documentation (e.g. in a data protection or security concept) can also be indicated.

(2c) Measures to prevent access to personal data by unauthorised individuals (access control by authorisation management):

- Use of personal user IDs and passwords.
- Authorisation management (rights and roles concept).
- Granting authorisations to IT applications will be done in accordance with the standardised process according to the principle of minimum rights ("need-to-know").
- Annual check of authorisations or the scope of authorisation (are they up-to-date, are they necessary).
- Disposal of data carriers, lists, etc. no longer required in accordance with data protection rules by qualified providers of disposal services in connection with the contract data processing arrangements.
- Logging of the assignment of authorisations.
- Logging of user activities in the Commerzbank systems.
- Separation between development, test and production environments.

Explanation:

This means measures to ensure that individuals authorised to use the data processing processes have access only to personal data for which they have access authorisation. In this connection, measures are taken to ensure that individuals working in data processing have access only to those data for which they have the appropriate authorisation and that personal data cannot be read, copied, changed or erased without authority during processing, use and after saving.

An existing documentation (e.g. in a data protection or security concept) can also be indicated.

(2d) Measures to prevent unauthorised perusal and to ensure accountability and protection of data integrity during data transmission (transfer control by safe transmission):

- Data carriers and confidential documents are either stored or destroyed by Commerzbank itself or by certified service providers.
- Documentation of the transport route.
- Use of sealed transport containers.
- Checking the admissibility of transferring data to third parties.
- Logging of transfer to the respective recipient of the data.
- Depending on the confidentiality of the data, encoding processes are used.
- Sealing-off of the internal network through firewalls.
- Protecting transmission lines and the data stream, for example by encoding via VPN.
- All employees all associates will be asked to sign a confidentiality clause or data protection declaration and will be instructed on a regular basis.

Explanation:

This means measures to ensure that personal data cannot be read, copied, changed or erased without authority during electronic transmission, transport or while being saved on data carriers, and that it can be verified and examined where transmission of personal data by data transmission facilities is intended.

An existing documentation (e.g. in a data protection or security concept) can also be indicated.

(2e) Measures for the **subsequent examination and accountability of input, changes and erasures** (input control by creating a protocol):

- Unambiguous matching of users to their user ID.
- Logging the collection of, changes to and erasure of data.
- Explicit access rules with regard to journal files.
- Rules for the erasure of personal data in accordance with applicable retention periods.

Explanation:

This means measures to ensure that it can be examined and determined subsequently whether and by whom personal data in data processing systems or applications were entered, changed or erased.

An existing documentation (e.g. in a data protection or security concept) can also be indicated.

(2f) Measures to **restore personal data in case of failure** (availability control by Business Continuity Management):

- Centrally managed data safety and restoring concepts of the individual IT applications and IT infrastructures (DR Tracking Tool).
- Use of backup processes depending on the classification of the information/data regarding availability and the parameters Recovery Time Objective (RTO) and Recovery Point Objective (RPO).
- Work-around and response concepts for possible network failures.

Explanation:

This means measures ensuring that personal data are protected against accidental destruction or loss.

An existing documentation (e.g. in a data protection or security concept) can also be indicated.

(2g) Measures for **keeping processing of personal data collected for different purposes separate** (separation control by keeping clients separate and by authorisation management):

- Logical separation of client data by participant numbers and other unambiguous identification criteria or physical separation (separate hardware surface).
- Separation between development, testing and production.
- Separation between test and production data.

Explanation:

This means measures to ensure that data collected for different purposes can be processed separately.

An existing documentation (e.g. in a data protection or security concept) can also be indicated.

(2h) Measures for data erasure and restriction of processing

- Development of data protection concepts including erasure and restrictions for IT systems or a group of IT systems if personal data of natural persons are processed within the scope of application of the GDPR (within the EU).
- Use of automated erasure routines if possible.
- Data from earlier, completed transactions/customer relations which, among other things, only need to be retained by Commerzbank AG in accordance with statutory provisions, for example retention periods under commercial law, are restricted (archived).

Explanation:

If personal data are no longer needed for the purposes for which they were collected or processed otherwise, they shall be erased whether requested by the data subject or not. This is the case especially if there is no basis for processing the data any more or if the basis has lapsed in the meantime.

In certain cases, a restriction of data processing must be arranged instead of complete erasure (called blocking so far).

An existing documentation (e.g. in a data protection or security concept) can also be indicated.

B. Additional country specific measures

For Switzerland:

The measures set out under this Appendix 2 of Exhibit 2 for the processing of personal data within the scope of application of the GDPR, shall also apply for the processing of personal data within the scope of application of the Swiss Data Protection Act ("DPA"). For avoidance of doubt, these measures shall apply for all processing of personal data within Switzerland, as well as for processing of personal data where the Data Exporter is located within Switzerland.

Signatures: See Signature Page

Appendix 3 to Exhibit 2 - Local Law Amendments

The below local law amendments apply if the Data Exporter is subject to the jurisdiction of the respective country:

I. Country specific

| # | Country | Amendment |
|----|---|---|
| 1. | Hungary | <p>Power of Attorney</p> <p>To the extent the Data Importer or Data Exporter is located in Hungary, Data Importer/Data Exporter hereby grants grants, to the extent permitted by law, pursuant to this clause, a power of attorney to Commerzbank AG to act as the party's authorized representative for the purposes of executing (i) any amendments to this DPGA, including without limitation additions of further or amendments to existing data processing activities; and (ii) any agreements to include additional entities or branches as Data Exporter and/or Data Importer to this DPGA. Commerzbank AG shall, within a reasonable time, notify in writing the relevant party of any documents signed by it pursuant to the authorization granted to this DPGA.</p> |
| 2. | Italy | <p>Clause 4 sentences 4 and 5 of the Main Body of the DPGA are replaced by the following:</p> <p>"Commerzbank AG will communicate the above amendments to the entities party to this agreement by written notice with confirmation of receipt (including electronic form) - sent at least 15 days before the effective date of the proposed amendments. Such amendments will be deemed accepted by the entities party to this agreement, if the respective entity does not withdraw in writing from the agreement within thirty (30) days after having received the above notice."</p> |
| 3. | China (which, when referring to jurisdiction, does not include Hong Kong, Macau and Taiwan) | <p>In case the Data Exporter is located in China, Exhibit 2 shall be amended as follows:</p> <ol style="list-style-type: none"> 1. The term "Community", "Member State" and "that State" in Exhibit 2 shall be replaced with the term "PRC". 2. The term "Article 26(2) of Directive 95/46/EC", "Directive 95/46/EC" and "Article 25(1) of Directive 95/46/EC" in Exhibit 2 shall be replaced with the term "the applicable data protection law". 3. The term "special categories of data" and "special categories of personal data" in Exhibit 2 and its Annexes shall be replaced with the term "sensitive personal data". 4. Paragraph (a) under the section "Definitions" shall be restated as follows: <ol style="list-style-type: none"> (a) "personal data", "sensitive personal data", "process/processing", "controller", "processor", "data subject" and "supervisory authority" shall have the same meaning as ascribed to each of them under the applicable data protection law (whereby "supervisory authority" shall mean the competent data protection authority in the People's Republic of China ("PRC")); 5. Paragraph (f) of Clause 4 (<i>Obligations of the data exporter</i>) shall be restated as follows: <ol style="list-style-type: none"> (f) data subjects have been informed of the purposes, manner and scope of the disclosure of transfer of personal data, the categories of recipients and the fact that the countries to which data is exported may have different data protection standards, and have consented to the same prior to the disclosure or transfer; |

| | | |
|----|-----------|---|
| | | <p>6. The following paragraph shall be added to Clause 11 (<i>Subprocessing</i>) as the new Paragraph 5:</p> <p>5. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without notifying the relevant data subjects of the same. Data subjects shall be informed of the purposes, manner and scope of the subprocessing of personal data.</p> |
| 4. | Hong Kong | <p>In case the Data Exporter is located in Hong Kong, Exhibit 2 shall be amended as follows:</p> <ol style="list-style-type: none"> 1. The term "Community" shall be replaced with the term "Hong Kong Special Administrative Region of the People's Republic of China". 2. The terms "Directive 95/46/EC", "Article 25(1) of Directive 95/46/EC" and "Article 26(2) of Directive 95/46/EC" shall be replaced with the term "Personal Data (Privacy) Ordinance (Cap. 486 of Laws of Hong Kong)", except for where it is used in the definition of "special categories of data/sensitive data". 3. The following definitions shall replace those set out in Clause 1 of Exhibit 2: <ul style="list-style-type: none"> • "controller" shall have the meaning given to "data user" in the Personal Data (Privacy) Ordinance (Cap. 486 of Laws of Hong Kong). • "processor" shall have the meaning given to "data processor" in the Personal Data (Privacy) Ordinance (Cap. 486 of Laws of Hong Kong). • "data subject" shall have the same meaning given in the Personal Data (Privacy) Ordinance (Cap. 486 of Laws of Hong Kong). • "supervisory authority/authority" shall have the same meaning given to "Commissioner" in the Personal Data (Privacy) Ordinance (Cap. 486 of Laws of Hong Kong). • "the applicable data protection law" shall mean the Personal Data (Privacy) Ordinance (Cap. 486 of Laws of Hong Kong). • "technical and organizational security measures" shall mean "those measures aimed at protecting personal data against unauthorized or accidental access, processing, erasure, loss or use of the data transferred." 4. In Clause 4(d) of Exhibit 2, replace "accidental or unlawful... and against all other unlawful forms of processing" with "unauthorized or accidental access, processing, erasure, loss or use of the data transferred." 5. At the end of Clause 6(1) of Exhibit 2, insert "in accordance with local law". |
| 5. | Japan | <p>In case the Data Exporter is located in Japan, Exhibit 2 shall be amended as follows:</p> <ol style="list-style-type: none"> 1. The term "Article 26(2) of Directive 95/46/EC", "Directive 95/46/EC" and "Article 25 (1) of Directive 95/46/EC" in the Exhibit 2 shall be replaced with the term "Act on the Protection of Personal Information (Act No. 57 of May 30, 2003, as amended) and all related regulations". 2. The following definitions shall replace those set out in Exhibit 2: "special categories of data (要配慮個人情報)", "controller (個人情報取扱事業者)", "data subject (本人)", and "supervisory authority (個人情報保護委員会)" shall have the same meaning as in the Act on the Protection of Personal Information (Act No. 57 of May 30, 2003, as amended) and all related regulations (whereby "the authority" shall mean the competent data protection authority in the territory in which the data exporter or data importer is established). |

| | | |
|----|--------|---|
| | | <p>3. Personal data transferred shall only be processed for purposes described in Appendix 1.1 to 1.3 of Exhibit 2 or for purposes subsequently authorised by the data subject.</p> <p>4. Clause I (a) and Clause II (i) in Exhibit 1 shall apply to controller to processor transfers from Japan to a country outside Japan and outside the EEA and the UK.</p> <p>5. Clause II (h) (iii) in Exhibit 1 and particularly Clause 2 and Clause 3 in Annex A of Exhibit 1 shall apply to controller to processor transfers from Japan to a country outside Japan and outside the EEA and the UK.</p> <p>6. The Data Importer shall take all reasonable measures to ensure its employees comply with all necessary and appropriate security measures under the Act on the Protection of Personal Information (Act No. 57 of May 30, 2003, as amended) and all related regulations, and implement necessary and appropriate monitoring of employees activities. "all reasonable measures" include providing quality and frequent training for employees on company rules and practices relating to the security measures and conducting audits of employees' compliance with the company rules and practices on a regular basis.</p> <p>7. Where the Data Importer transfers the personal data to a third party regardless of whether the third party is located in Japan or outside of Japan, the Data Importer shall do this using a means compliant with the Act on the Protection of Personal Information (Act No. 57 of May 30, 2003, as amended) and all related regulations, but where uncertain, shall default to obtaining consent for the data transfers from data subjects.</p> |
| 6. | Russia | <p>1. <u>Application of the clauses:</u> Russian Data Exporters enter into the clauses, together with the "Descriptions of Transfers of Personal Data" (Appendix 1.1 to 1.3 of Exhibit 2), with any Data Importer (irrespective of whether such Data Importer is established in a country that ensures an adequate level of protection of data subjects' rights or not). Clause 4 of the Russia Local Law Amendments shall also apply to all transfers of Personal Information to Russia. For the avoidance of doubt, the clauses shall also apply where the Data Exporter and the Data Importer are located in the Russian Federation (to the extent appropriate).</p> <p>2. <u>Obligations of the Data Importer:</u> For the purposes of clause 5(c) of the Standard Contractual Clauses (Controller to Processor) the Data Importer warrants and undertakes that before processing the personal data it has implemented and will have in place the appropriate legal, technical and organizational measures to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, and such additional legal, technical and organizational measures as may be required under the Russian Personal Data Law, in particular under Article 19 of the Russian Personal Data Law (to the extent applicable), which provide a level of security appropriate to the risk represented by the processing and the nature of the personal data to be protected, and will ensure confidentiality of the personal data, as well as observe, where applicable, the regime of medical secrecy.</p> <p>The Data Importer, when it receives personal data for processing without use of automation tools, hereby represents that it is aware of (1) the fact that it processes personal data without use of automation tools, (2) categories of processed personal data and (3) special requirements to such personal data processing. The Data Importer shall comply with applicable requirements on personal data processing without use of automation tools, including to familiarize its employees and third parties that have access to the personal data with the information listed in this paragraph.</p> |

| | | |
|----|-----------|--|
| | | <p>3. <u>Confidentiality and security of data</u>: The data operator and data processor contracted by the data operator are obliged to ensure confidentiality and security of personal data. The data processor may only disclose to third parties or disseminate the personal data subject to data subjects' consents or otherwise in accordance with the Russian Personal Data Law.</p> <p>4. <u>Description of the transfer</u>: Unless otherwise specifically indicated by the Data Exporter to the Data Importer (e.g. due to the constraints of the data subject consents), the Data Importer shall be permitted to perform the following operations upon the personal data: collection, recording, systematization, accumulation, storage, (update, alteration), retrieval, use, transfer (distribution, disclosure, access), blocking, removal, destruction of personal data, whether with or without means of automation.</p> |
| 7. | Singapore | <p>In case the Data Exporter is located in Singapore,</p> <ul style="list-style-type: none"> • Exhibit 2 shall be amended as follows: <ol style="list-style-type: none"> 1. The term "Community" in Exhibit 2 shall be replaced with the term "Singapore". 2. The opening paragraph in Exhibit 2 "For the purposes of Article 26(a)... adequate level of data protection" shall be deleted. 3. The following definitions shall replace those set out in Exhibit 2: <ol style="list-style-type: none"> a) "personal data" shall have the same meaning given in the Personal Data Protection Act. b) "process/processing" shall have the same meaning given in the Personal Data Protection Act. c) "supervisory authority" shall have the same meaning given to "Commissioner" in the Personal Data Protection Act. 4. The terms "in the Member State" in clauses 1(e) and 7(1)(b) in Exhibit 2 and "of the Member State" in clauses 4(a), 9 and 11(3) in Exhibit 2 shall be deleted. 5. The term "that State" in clause 4(a) in Exhibit 2 shall be replaced by "Singapore". 6. The following definition shall be included in Exhibit 1 as paragraph (g) under "Definitions": <p style="margin-left: 40px;">"Personal Data Protection Act" shall mean Singapore's Personal Data Protection Act including all subsidiary legislation enacted thereunder, whether now or in the future.</p> • and, clause 1.6 of this DPGA notwithstanding, <p>For the avoidance of doubt, it will not be considered an inconsistency with this DPGA if the provisions in any other agreement between the Parties in relation to the subject-matters addressed herein serve as a clarification or extension of the provisions in this DPGA and/or imposes a stricter obligation on a Party.</p> |

| | | |
|----|----------------|---|
| 8. | Switzerland | <p>In case the Data Exporter is located in Switzerland, Exhibit 2 shall be amended as follows:</p> <ol style="list-style-type: none"> 1. "personal data", "special categories of data/sensitive data", "personality profiles", "process/processing", "controller", "processor", "data subject" and "supervisory authority/authority" shall have the meaning assigned to them by the Swiss Federal Act on Data Protection of June 19, 1992 ("DPA") including the relevant amendments and its implementing ordinances, (whereby "the authority" shall mean the competent data protection authority in the territory in which the Data Exporter is established); 2. 'the applicable law' shall mean the legislation protecting the fundamental rights and freedoms of natural and legal persons, including the Swiss Federal Data Protection Act of June 19, 1992 including the relevant amendments and its implementing ordinances; 3. 'White-List Country' shall mean a country, which is found by decision of the Swiss Federal Data Protection and Information Commissioner to ensure an adequate level of data protection according to Swiss standards; 4. The Data Importer acknowledges and agrees that the personal data transferred to Data Importer by Data Exporter may include personal data of legal persons and personality profiles of natural persons. The Data Importer shall process personal data of legal persons in the same manner as other personal data as long as this requirement exists under Swiss data protection law and personality profiles in the same manner as special categories of data; 5. The DPA requires equal to the European laws Data Exporters in Switzerland to provide appropriate safeguards for transfers of personal data to processors in non-EU/EEA countries and outside Switzerland. Such appropriate safeguards can be adduced by requiring the Data Importers to enter into the Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries ("Model Contract C2P") pursuant to Commission Decision 2010/87/EU of 5 February 2010. |
| 9. | United Kingdom | <p>In relation to any transfers of personal data from the United Kingdom to outside of the United Kingdom, clauses 1.2 to 1.5 of the Main Body of the DPGA shall apply and the Model Contract C2P shall apply to the extent permissible under data protection laws in the United Kingdom if personal data is transferred to a jurisdiction which is</p> <p>(a) not subject to an arrangement with the United Kingdom (or transitional arrangements under the laws of the United Kingdom) permitting the transfer of personal data from the United Kingdom to the jurisdiction in which the Data Importer is located; or</p> <p>(b) not subject to an adequacy decision or similar decision (or transitional arrangement) under the laws of the United Kingdom permitting the transfer of personal data to jurisdictions outside of the United Kingdom.</p> |

II. Supplementary Measures for Data Exporters located in the EU

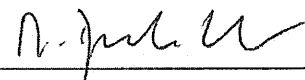

- | |
|---|
| <ol style="list-style-type: none"> 1. Unless prohibited by applicable law, data importer shall inform the data exporter in general terms about requests, orders or similar demands by a court, competent authority, law enforcement or other |
|---|

government body ("Judicial or Governmental Information Request) relating to the processing of personal data under these Clauses.

2. Data importer shall object to and challenge any "Judicial or Governmental Information Request by taking legal remedies to the extent they are reasonable given the circumstances. If compelled to disclose personal data transferred under these Clauses by a "Judicial or Governmental Information Request, data importer will give data exporter reasonable notice to allow data exporter to seek a protective order or other appropriate remedy unless data importer is legally prohibited from doing so.
3. Should a new/updated version of the Clauses become available, data importer shall upon data exporter's request agree to the new/amended version of the Clauses.
4. Notwithstanding clause 5 lit. h of the Clauses and other requirements in data processing agreements, in case data importer makes personal data available to sub-processors, data importer will select sub-processor in a third country only after a due diligence that entails (i) a review of any transparency reports made available by sub-processor, (ii) and carrying out a transfer risk assessment and provision of the same to the data exporter prior to the engagement of sub-processor.

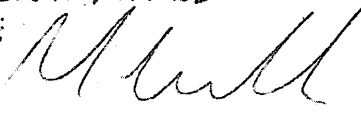
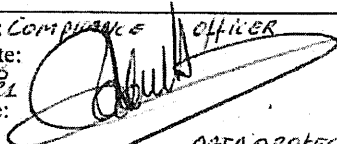
Signature Page

1. Commerzbank AG entities (including branch offices, located in the EU/EEA or the UK):

| # | Country | Name, legal form and address | Exporter | Importer | Signature 1 | Signature 2 |
|----|----------------|--|-------------------------------------|-------------------------------------|---|---|
| 1. | Austria | Commerzbank AG Vienna Branch Hietzinger Kai 101 – 105 1130 Wien, Austria | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: VIENNA, 17.8.2021 Signature:  | Capacity: Place, date: VIENNA, 17.8.2021 Signature:  |
| 2. | Belgium | Commerzbank AG Brussels Branch 29, Boulevard Louis Schmidt 1040 Bruxelles, Belgium | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |
| 3. | Bulgaria | Digital Technology Center Commerzbank AG Sofia Branch, Bulgaria, Sofia, district Mladost, zh.k. Mladost 4, 1715, str. Samara 2, Advance Business Center II, 3 rd floor | <input type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |
| 4. | Czech Republic | Commerzbank AG Acting through COMMERZBANK Aktiengesellschaft, Pobočka Praha Prague Branch Jugoslávská 1 120 21 Praha 2, Czech Republic | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |

Signature Page

I. Commerzbank AG entities (including branch offices, located in the EU/EEA or the UK):

| # | Country | Name, legal form and address | Exporter | Importer | Signature 1 | Signature 2 |
|----|----------------|--|-------------------------------------|-------------------------------------|---|--|
| 1. | Austria | Commerzbank AG Vienna Branch Hietzinger Kai 101 – 105 1130 Wien, Austria | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |
| 2. | Belgium | Commerzbank AG Brussels Branch 29, Boulevard Louis Schmidt 1040 Bruxelles, Belgium | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: COUNTRY LEO DE LUX Place, date: BRUSSELS 17/11/2024 Signature:  | Capacity: COMPLIANCE OFFICER Place, date: BRUSSELS 17/11/2024 Signature:  DATA PROTECTION CONTACT |
| 3. | Bulgaria | Digital Technology Center Commerzbank AG Sofia Branch, Bulgaria, Sofia, district Mladost, zh.k. Mladost 4, 1715, str. Samara 2. Advance Business Center II, 3 rd floor | <input type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |
| 4. | Czech Republic | Commerzbank AG Acting through COMMERZBANK Aktiengesellschaft, Pobočka Praha Prague Branch Jugoslávská 1 120 21 Praha 2, Czech Republic | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |



Signature Page

I. Commerzbank AG entities (including branch offices, located in the EU/EEA or the UK):

| # | Country | Name, legal form and address | Exporter | Importer | Signature 1 | Signature 2 |
|----|----------------|--|-------------------------------------|-------------------------------------|--|---|
| 1. | Austria | Commerzbank AG Vienna Branch Hietzinger Kai 101 – 105 1130 Wien, Austria | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |
| 2. | Belgium | Commerzbank AG Brussels Branch 29, Boulevard Louis Schmidt 1040 Bruxelles, Belgium | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |
| 3. | Bulgaria | Digital Technology Center Commerzbank AG Sofia Branch, Bulgaria, Sofia, district Mladost, zh.k. Mladost 4, 1715, str. Samara 2, Advance Business Center II, 3 rd floor | <input type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: <i>10 Oct. 2021</i> Signature: <i>[Signature]</i> | Capacity: <i>6-8-05-25</i> Place, date: <i>Sofia 12/10/21</i> Signature: <i>[Signature]</i> <i>Evaterina Maslaeska</i> |
| 4. | Czech Republic | Commerzbank AG Acting through COMMERZBANK Aktiengesellschaft, Pobočka Praha Prague Branch Jugoslávská 1 120 21 Praha 2, Czech Republic | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |

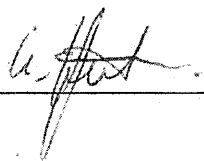
Signature Page

I. Commerzbank AG entities (including branch offices, located in the EU/EEA or the UK):

| # | Country | Name, legal form and address | Exporter | Importer | Signature 1 | Signature 2 |
|----|----------------|--|-------------------------------------|-------------------------------------|---|--|
| 1. | Austria | Commerzbank AG Vienna Branch Hietzinger Kai 101 – 105 1130 Wien, Austria | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |
| 2. | Belgium | Commerzbank AG Brussels Branch 29, Boulevard Louis Schmidt 1040 Bruxelles, Belgium | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |
| 3. | Bulgaria | Digital Technology Center Commerzbank AG Sofia Branch, Bulgaria, Sofia, district Mladost, zh.k. Mladost 4, 1715, str. Samara 2, Advance Business Center II, 3 rd floor | <input type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |
| 4. | Czech Republic | Commerzbank AG Acting through COMMERZBANK Aktiengesellschaft, Pobočka Praha Prague Branch Jugoslávská 934/1 120 00 Praha 2, Czech Republic | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Country CEO Place, date: Signature:  | Capacity: Local COO Place, date: Signature:  |

| | | | | | | |
|----|---------|---|-------------------------------------|-------------------------------------|--|---|
| 5. | France | Commerzbank AG Paris Branch 86 Boulevard Haussmann 75008 Paris France | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: Molenaar, Olivier <small>Digital unterscriben von Molenaar, Olivier Datum: 2021.07.21 09:31:36 +02'00'</small> | Capacity: Place, date: Signature: Maas, Erich <small>Signature numérique de Maas, Erich Date: 2021.07.21 09:07:24 +02'00'</small> |
| 6. | Germany | Commerzbank AG Kaiserstraße 16 (Kaiserplatz) 60311 Frankfurt/Main Germany | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |
| 7. | Hungary | Commerzbank Zrt. Széchenyi rakpart 8 1054 Budapest, Hungary Postal address: P.O. Box 1070 1245 Budapest, Hungary | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |
| 8. | Italy | Commerzbank AG Milan Branch Corso Europa 2 20122 Milan, Italy | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |

| | | | | | | |
|----|---------|---|-------------------------------------|-------------------------------------|---|---|
| 5. | France | Commerzbank AG Paris Branch 86 Boulevard Haussmann 75008 Paris France | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |
| 6. | Germany | Commerzbank AG Kaiserstraße 16 (Kaiserplatz) 60311 Frankfurt/Main Germany | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Vigelius, Sabine Signature: <small>Digital unterschrieben von Vigellus, Sabine DN: ou=Nur zur internen Verwendung!, cn=Vigellus, Sabine, email=sabine.vigellus@commerzbank.c om Datum: 2021.08.30 18:35:27 +0200'</small> |
| 7. | Hungary | Commerzbank Zrt. Széchenyi rakpart 8 1054 Budapest, Hungary Postal address: P.O. Box 1070 1245 Budapest, Hungary | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |
| 8. | Italy | Commerzbank AG Milan Branch Corso Europa 2 20122 Milan, Italy | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |

| | | | | | | |
|----|---------|---|-------------------------------------|-------------------------------------|---|---|
| 5. | France | Commerzbank AG Paris Branch 86 Boulevard Haussmann 75008 Paris France | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |
| 6. | Germany | Commerzbank AG Kaiserstraße 16 (Kaiserplatz) 60311 Frankfurt/Main Germany | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature:  |
| 7. | Hungary | Commerzbank Zrt. Széchenyi rakpart 8 1054 Budapest, Hungary Postal address: P.O. Box 1070 1245 Budapest, Hungary | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |
| 8. | Italy | Commerzbank AG Milan Branch Corso Europa 2 20122 Milan, Italy | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |

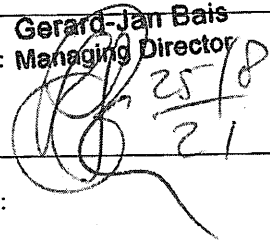
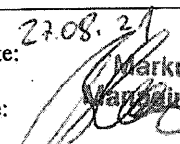
| | | | | | | |
|----|---------|---|-------------------------------------|-------------------------------------|--|--|
| 5. | France | Commerzbank AG Paris Branch 86 Boulevard Haussmann 75008 Paris France | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |
| 6. | Germany | Commerzbank AG Kaiserstraße 16 (Kaiserplatz) 60311 Frankfurt/Main Germany | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |
| 7. | Hungary | Commerzbank Zrt. Széchenyi rakpart 8 1054 Budapest, Hungary Postal address: P.O. Box 1070 1245 Budapest, Hungary | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: Fueloep Bogdan, Krisztina <small>Digitálisan aláírta: Fueloep Bogdan, Krisztina Dátum: 2021.08.31 17:31:34 +02'00'</small> | Capacity: Place, date: Signature: Kovacs, Edina <small>Digitálisan aláírta: Kovacs, Edina Dátum: 2021.08.31 09:30:20 +02'00'</small> |
| 8. | Italy | Commerzbank AG Milan Branch Corso Europa 2 20122 Milan, Italy | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |



| | | | | | | |
|----|---------|---|-------------------------------------|-------------------------------------|---|---|
| 5. | France | Commerzbank AG Paris Branch 86 Boulevard Haussmann 75008 Paris France | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |
| 6. | Germany | Commerzbank AG Kaiserstraße 16 (Kaiserplatz) 60311 Frankfurt/Main Germany | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |
| 7. | Hungary | Commerzbank Zrt. Széchenyi rakpart 8 1054 Budapest, Hungary Postal address: P.O. Box 1070 1245 Budapest, Hungary | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |
| 8. | Italy | Commerzbank AG Milan Branch Corso Europa 2 20122 Milan, Italy | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: Braun, Kristian | Capacity: Place, date: Signature: Casartelli, Luciano |

Digitally signed by Braun, Kristian
Date: 2021.07.23
09:46:17 +02'00'

Digitally signed by Casartelli, Luciano
Date: 2021.07.23
09:49:39 +02'00'

| | | | | | | |
|-----|-------------|--|-------------------------------------|-------------------------------------|---|--|
| 9. | Luxembourg | Commerzbank AG Luxembourg Branch 25, rue Edward Steichen 2540 Luxembourg Luxembourg Postal address: Boîte Postale 303 2013 Luxembourg Luxembourg | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: <i>General Manager</i> Place, date: <i>Luxembourg, 27-08-21</i> Signature: <i>Klaus Diéderich</i> | Capacity: <i>Head of Treasury</i> Place, date: <i>Luxembourg, 27-08-21</i> Signature: <i>Markus Braes</i> <i>Director</i> |
| | | Commerzbank Finance & Covered Bond S.A. P.O.Box 321 L-2013 Luxembourg | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |
| 10. | Netherlands | Commerzbank AG Amsterdam Branch Claude Debussylaan 24 (10th Floor) 1082 MD Amsterdam The Netherlands | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |

| | | | | | | |
|-----|-------------|--|-------------------------------------|-------------------------------------|---|--|
| 9. | Luxembourg | Commerzbank AG Luxembourg Branch 25, rue Edward Steichen 2540 Luxembourg Luxembourg Postal address: Boite Postale 303 2013 Luxembourg Luxembourg | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |
| | | Commerzbank Finance & Covered Bond S.A. P.O.Box 321 L-2013 Luxembourg | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Gerard-Jan Bais Place, date: Managing Director Signature:  | Capacity: 27.08.21 Place, date: Markus Blaes Signature: Managing Director  |
| 10. | Netherlands | Commerzbank AG Amsterdam Branch Claude Debussylaan 24 (10th Floor) 1082 MD Amsterdam The Netherlands | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |

| | | | | | | |
|-----|-------------|--|-------------------------------------|-------------------------------------|--|---|
| 9. | Luxembourg | Commerzbank AG Luxembourg Branch 25, rue Edward Steichen 2540 Luxembourg Luxembourg Postal address: Boîte Postale 303 2013 Luxembourg Luxembourg | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |
| | | Commerzbank Finance & Covered Bond S.A. P.O.Box 321 L-2013 Luxembourg | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |
| 10. | Netherlands | Commerzbank AG Amsterdam Branch Claude Debussylaan 24 (10th Floor) 1082 MD Amsterdam The Netherlands | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: ICC-IC Country CEO Place, date: Amsterdam, 04 Aug. 2021 Signature:  | Capacity: CC-IC CAO Local COO Place, date: Amsterdam, 04 Aug. 2021 Signature:  |

| | | | | | | |
|-----|----------|---|-------------------------------------|-------------------------------------|---|---|
| 11. | Poland | Commerzbank AG Oddział w Łodzi ul. Wersalska 91 – 203 Łódź Poland | <input type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: 12.08.2021 Łódź Signature: <i>[Signature]</i> |
| | | mBank SA ul. Senatorska 18 00-950 Warszawa Poland Postal address: P.O. Box 728 00-950 Warszawa Poland | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |
| | | CERI International Sp. Z o.o. ul. Wersalska 6 91-203 Łódź Poland | <input type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |
| 12. | Slovakia | Commerzbank AG acting through COMMERZBANK Aktiengesellschaft, pobočka zahraničnej banky, Bratislava Bratislava Branch Rajská 15/A 81108 Bratislava Slovak Republic Postal address: P.O. Box 138 810 00 Bratislava Slovak Republic | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |



Unterscriben und alle Unterschriften sind gultig.

Unterschriftsfenster



Unterschriften



Alle prufen



> Revision 1: Unterscriben von Cezary Kocik



> Revision 2: Unterscriben von Adam Pers

Data Processing and Guarantee Agreement

This Data Processing and Guarantee Agreement ("DPGA") is entered into by and between the data exporters (each a "Data Exporter") and the data importers (each a "Data Importer") listed on the Signature Page (each a "Party" and collectively the "Parties").

Preamble

WHEREAS, Commerzbank AG, headquartered in Frankfurt/Main Germany, is an internationally active business bank, represented in numerous countries inside and outside of the European Union ("EU") and the European Economic Area ("EEA") through a network of branches and legal entities;

WHEREAS, in certain circumstances, it may become necessary that Commerzbank AG, its branches and/or affiliates transfer personal data relating to customers and individual representatives, directors, contact persons, authorized signatories and authorized traders of its corporate customers as well as ultimate beneficial owners that are natural persons (together "Data Subjects"), to other branches and/or legal entities outside the EU/the EEA. Some countries in which the Commerzbank Group does business and to which personal data are transferred, may not provide for the same standard of data protection which applies in Germany or in the EU/the EEA;

WHEREAS, the Parties wish to provide appropriate safeguards in connection with such transfers of personal data with respect to the protection of privacy and fundamental rights and freedoms of the data subjects;

WHEREAS, European data protection laws require data exporters in EU/EEA countries to provide appropriate safeguards for transfers of personal data to controllers in non-EU/EEA countries and such appropriate safeguards can be adduced by requiring the Data Importers to enter into the Standard Contractual Clauses for the Transfer of Personal Data to Third Countries ("Model Contract C2C") pursuant to Commission Decision 2004/915/EC of 27 December 2004;

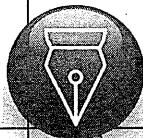
WHEREAS, European data protection laws require data exporters in EU/EEA countries to provide appropriate safeguards for transfers of personal data to processors in non-EU/EEA countries and such appropriate safeguards can be adduced by requiring the Data Importers to enter into the Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries ("Model Contract C2P") pursuant to Commission Decision 2010/87/EU of 5 February 2010;

WHEREAS, the Model Contract C2C as well as the Model Contract C2P are usually incorporated in an agreement between the legal entity transferring and the legal entity receiving the personal data. In the case of a transfer between a legal entity and its legally dependent branch, some data protection authorities have taken the view that a unilateral guarantee declaration, to be made available to the Data Subjects shall be used instead;

WHEREAS, for transfers of personal data by a Data Exporter being a legal entity to one of its branches, the Data Exporter and the Data Importer guarantee to the Data Subjects that they assume the data exporter's and the data importer's obligations, respectively, as if they had entered into the Model Contract C2C respectively the Model Contract C2P as set out in Exhibit 1 respectively Exhibit 2 ("Guarantee"). Under this Guarantee, the Data Subjects shall have the same rights against the relevant Data Exporter as if its branch office was located in the EU/the EEA;

WHEREAS, the Parties agree that the bundling of the Data Exporters and the Data Importers (as listed on the Signature Page) within this single DPGA is only undertaken for efficiency purposes (i.e., to avoid a multitude of different contract documents) and (i) shall result in legally separate agreements between each Data Exporter and each Data Importer and (ii) shall not create any legal or other relationship whatsoever between the "bundled" Parties other than between each Data Exporter and each Data Importer separately;



| | | | | | | |
|-----|----------|---|-------------------------------------|-------------------------------------|---|---|
| 11. | Poland | Commerzbank AG Oddział w Łodzi ul. Wersalska 91 – 203 Łódź Poland | <input type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |
| | | mBank SA ul. Senatorska 18 00-950 Warszawa Poland Postal address: P.O. Box 728 00-950 Warszawa Poland | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |
| | | CERI International Sp. Z o.o. ul. Wersalska 6 91-203 Łódź Poland | <input type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |
| 12. | Slovakia | Commerzbank AG acting through | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |
| | | COMMERZBANK Aktiengesellschaft, pobočka zahraničnej banky, Bratislava Branch Rajská 15/A 81108 Bratislava Slovak Republic Postal address: P.O. Box 138 810 00 Bratislava Slovak Republic | | | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |



Signed by /
Podpisano przez:
KIM
WULLENWEBER
Date / Data:
2021-09-10 15:06



Signed by /
Podpisano przez:
MIGUEL ANGEL
RODRIGUEZ
ALVAREZ
Date / Data: 2021-
09-10 08:21

| | | | | | | |
|-----|----------|---|-------------------------------------|-------------------------------------|---|---|
| 11. | Poland | Commerzbank AG Oddzial w Lodzi ul. Wersalska 91 – 203 Lodz Poland | <input type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |
| | | mBank SA ul. Senatorska 18 00-950 Warszawa Poland Postal address: P.O. Box 728 00-950 Warszawa Poland | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |
| | | CERI International Sp. Z o.o. ul. Wersalska 6 91-203 Lodz Poland | <input type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |
| 12. | Slovakia | Commerzbank AG acting through COMMERZBANK Aktiengesellschaft, pobočka zahraničnej banky, Bratislava Bratislava Branch Rajská 15/A 81108 Bratislava Slovak Republic Postal address: P.O. Box 138 810 00 Bratislava Slovak Republic | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Country CEO Place, date: Signature:  Ing. Ľudovít Bán Date: 2021.07.21 14:28:35 +02'00' | Capacity: Local COO Place, date: Signature:  Jens Hohmann Date: 2021.07.21 09:44:44 +02'00' |

| | | | | | | |
|-----|----------------|---|-------------------------------------|-------------------------------------|--|--|
| 13. | Spain | Commerzbank AG Madrid Branch Torre de Cristal, Paseo de la Castellana 259 C 28046 Madrid Spain | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: Masalles, Jorge <small>Digitally signed by Masalles, Jorge Date: 2021.08.05 14:29:36 +02'00'</small> | Capacity: Place, date: Signature: Daum, Jens (IC - Madrid) <small>Digital unterscriben von Daum, Jens (IC - Madrid) Datum: 2021.08.02 14:06:50 +02'00'</small> |
| 14. | United Kingdom | Commerzbank AG London Branch 30 Gresham Street London EC2V 7PG United Kingdom Postal address: PO Box 52715 London EC2P 2XY United Kingdom | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |



| | | | | | | |
|-----|----------------|---|-------------------------------------|-------------------------------------|---|--|
| 13. | Spain | Commerzbank AG Madrid Branch Torre de Cristal, Paseo de la Castellana 259 C 28046 Madrid Spain | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |
| 14. | United Kingdom | Commerzbank AG London Branch 30 Gresham Street London EC2V 7PG United Kingdom Postal address: PO Box 52715 London EC2P 2XY United Kingdom | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: Smith, Ian (FINANCE) Digitally signed by Smith, Ian (FINANCE) Date: 2021.08.02 14:47:10 +01'00' | Capacity: Place, date: Signature: Clapham , David Digitally signed by Clapham, David Date: 2021.08.03 16:51:27 +01'00' |

II. Commerzbank AG entities (including branch offices, located outside of the EU/EEA or the UK):


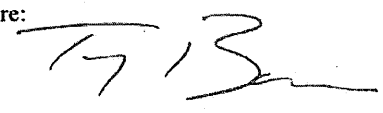
| # | Country | Name, legal form and address | Exporter | Importer | Signature 1 | Signature 2 |
|----|-----------|--|-------------------------------------|-------------------------------------|---|---|
| 1. | Brazil | Commerzbank Brasil S.A. Banco Múltiplo Avenida Dr. Chucris Zaidan, 1240 11° andar / 11th Floor CEP 04711-130 São Paulo - SP, Brazil | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: Correa, Ronaldo Digitally signed by Correa, Ronaldo Date: 2021.08.17 15:43:59 -03'00' | Capacity: Place, date: Signature: Pazin, Eduardo Moherdaui Assinado de forma digital por Pazin, Eduardo Moherdaui Dados: 2021.08.17 12:21:39 -03'00' |
| 2. | China | Commerzbank AG Beijing Branch Suite 2502 East Tower, Twin Towers B-12 Jianguomenwai Dajie Chaoyang District Beijing 100022, China | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |
| | | Commerzbank AG Shanghai Branch 37F, Shanghai World Financial Center 100 Century Avenue 200120 Shanghai, China | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |
| 3. | Hong Kong | Commerzbank AG Hong Kong Branch 15th Floor, Lee Garden One 33 Hysan Avenue Causeway Bay Hong Kong China Postal address: G.P.O. Box 11378 Hong Kong SAR, China | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |

ME

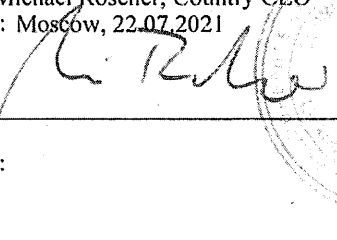
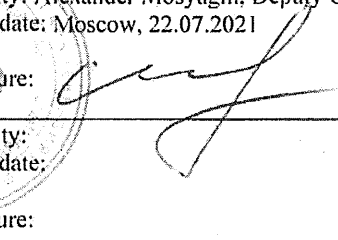
II. Commerzbank AG entities (including branch offices, located outside of the EU/EEA or the UK):


| # | Country | Name, legal form and address | Exporter | Importer | Signature 1 | Signature 2 |
|----|-----------|--|-------------------------------------|-------------------------------------|--|---|
| 1. | Brazil | Commerzbank Brasil S.A. Banco Múltiplo Avenida Dr. Chucri Zaidan, 1240 11° andar / 11th Floor CEP 04711-130 São Paulo - SP, Brazil | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |
| 2. | China | Commerzbank AG Beijing Branch Suite 2502 East Tower, Twin Towers B-12 Jianguomenwai Dajie Chaoyang District Beijing 100022, China | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: Zhang, Tony  | Capacity: Place, date: Signature: |
| | | Commerzbank AG Shanghai Branch 37F, Shanghai World Financial Center 100 Century Avenue 200120 Shanghai, China | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: Zhang, Tony  | Capacity: Place, date: Signature: |
| 3. | Hong Kong | Commerzbank AG Hong Kong Branch 15th Floor, Lee Garden One 33 Hysan Avenue Causeway Bay Hong Kong China Postal address: G.P.O. Box 11378 Hong Kong SAR, China | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |

II. Commerzbank AG entities (including branch offices, located outside of the EU/EEA or the UK):

| # | Country | Name, legal form and address | Exporter | Importer | Signature 1 | Signature 2 |
|----|-----------|--|-------------------------------------|-------------------------------------|---|---|
| 1. | Brazil | Commerzbank Brasil S.A. Banco Múltiplo Avenida Dr. Chucris Zaidan, 1240 11° andar / 11th Floor CEP 04711-130 São Paulo - SP, Brazil | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |
| 2. | China | Commerzbank AG Beijing Branch Suite 2502 East Tower, Twin Towers B-12 Jianguomenwai Dajie Chaoyang District Beijing 100022, China | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |
| | | Commerzbank AG Shanghai Branch 37F, Shanghai World Financial Center 100 Century Avenue 200120 Shanghai, China | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |
| 3. | Hong Kong | Commerzbank AG Hong Kong Branch 15th Floor, Lee Garden One 33 Hysan Avenue Causeway Bay Hong Kong China Postal address: G.P.O. Box 11378 Hong Kong SAR, China | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Chief Operating Officer Place, date: Hong Kong, 4th August 2021 Signature:  Jens Ritter Chief Operating Officer Commerzbank AG Hong Kong Branch Jens Ritter | Capacity: Country CEO Place, date: Hong Kong, 4th August 2021 Signature:  CEO, HONG KONG BRANCH Tony Barrons |


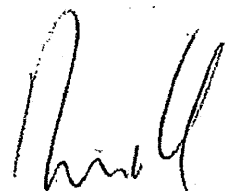
| | | | | | | |
|----|-----------|---|-------------------------------------|-------------------------------------|--|---|
| 4. | Japan | Commerzbank AG Tokyo Branch Glass Cube Shinagawa 10F 4-13-14 Higashi-Shinagawa, Shinagawa-ku Tokyo 140-0002, Japan | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: Zurmuehlen, Sandrina <small>Digitally signed by Zurmuehlen, Sandrina Date: 2021.07.21 17:07:48 +09'00'</small> | Capacity: Place, date: Signature: Sajima, Yasutaka <small>電子署名者: Sajima, Yasutaka DN: ou=INur zur Interneten Verwendung!, cn=Sajima, Yasutaka, email=Yasutaka.Sajima@commer zbank.com 日付: 2021.07.21 16:35:29 +09'00'</small> |
| 5. | Russia | Commerzbank (Eurasija) AO 14/2 Kadashevskaya Nab. 119017 Moscow Russia | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |
| 6. | Singapore | Commerzbank AG Singapur Branch 71 Robinson Road #12-01 Singapore 068895 Postal address: P.O. Box 3314 Robinson Road Singapore 905314 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |

| | | | | | | |
|----|-----------|---|-------------------------------------|-------------------------------------|---|--|
| 4. | Japan | Commerzbank AG Tokyo Branch Glass Cube Shinagawa 10F 4-13-14 Higashi-Shinagawa, Shinagawa-ku Tokyo 140-0002, Japan | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |
| 5. | Russia | Commerzbank (Eurasija) AO 14/2 Kadashevskaya Nab. 119017 Moscow Russia | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Michael Roscher, Country CEO Place, date: Moscow, 22.07.2021 Signature:  | Capacity: Alexander Mosyagin, Deputy CCEO Place, date: Moscow, 22.07.2021 Signature:  |
| 6. | Singapore | Commerzbank AG Singapur Branch 71 Robinson Road #12-01 Singapore 068895 Postal address: P.O. Box 3314 Robinson Road Singapore 905314 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |

| | | | | | | |
|----|-----------|---|-------------------------------------|-------------------------------------|---|---|
| 4. | Japan | Commerzbank AG Tokyo Branch Glass Cube Shinagawa 10F 4-13-14 Higashi-Shinagawa, Shinagawa-ku Tokyo 140-0002, Japan | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |
| 5. | Russia | Commerzbank (Eurasija) AO 14/2 Kadashevskaya Nab. 119017 Moscow Russia | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |
| 6. | Singapore | Commerzbank AG Singapur Branch 71 Robinson Road #12-01 Singapore 068895 Postal address: P.O. Box 3314 Robinson Road Singapore 905314 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: <div>  <p>COMMERZBANK</p> <p>Andreas Papaspyrou Chief Operating Officer Deputy General Manager</p> </div> | Capacity: Place, date: Signature: <div> <p>Johnston, Nick</p> <p>Digitally signed by Johnston, Nick Date: 2021.08.16 14:14:59 +08'00'</p> </div> |

| | | | | | | |
|----|-------------|--|-------------------------------------|-------------------------------------|---|--|
| 7. | Switzerland | Commerzbank AG Filiale Zürich Pelikanplatz 15 8001 Zürich Switzerland | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Zürich, 10.08.2021 Signature: Marc Steinkat | Capacity: Place, date: Zürich, 10.08.2021 Signature: Olaf Oelschläger |
| | | Commerzbank AG Agentur Basel Hirschgässlein 19 4051 Basel Switzerland | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Zürich, 10.08.2021 Signature: Marc Steinkat | Capacity: Place, date: Zürich, 10.08.2021 Signature: Olaf Oelschläger |
| | | Commerzbank AG Agentur Bern Bahnhofplatz 5 3011 Bern Switzerland | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Zürich, 10.08.2021 Signature: Marc Steinkat | Capacity: Place, date: Zürich, 10.08.2021 Signature: Olaf Oelschläger |
| | | Commerzbank AG Agentur Lausanne Avenue Mon-Repos 14 1005 Lausanne Switzerland | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Zürich, 10.08.2021 Signature: Marc Steinkat | Capacity: Place, date: Zürich, 10.08.2021 Signature: Olaf Oelschläger |
| | | Commerzbank AG Agentur Luzern Alpenquai 28 a 6005 Luzern Switzerland | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Zürich, 10.08.2021 Signature: Marc Steinkat | Capacity: Place, date: Zürich, 10.08.2021 Signature: Olaf Oelschläger |
| | | Commerzbank AG Agentur St. Gallen Vadianstrasse 59 9000 St. Gallen Switzerland | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Zürich, 10.08.2021 Signature: Marc Steinkat | Capacity: Place, date: Zürich, 10.08.2021 Signature: Olaf Oelschläger |

| | | | | | | |
|----|-----|---|-------------------------------------|-------------------------------------|---|--|
| 8. | USA | Commerzbank AG New York Branch 225 Liberty Street New York, NY 10281-1050 USA | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Fruchter, Michael Signature: r, Michael Date: 2021.09.16 12:51:01 -04'00' | Capacity: Place, date: Holsten, Andreas Signature: Holsten, Andreas Date: 2021.09.16 12:37:15 -04'00' |
| | | Commerz Markets LLC 225 Liberty Street New York, NY 10281-1050 USA | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Royan, Lee-Ann Signature: Lee-Ann Date: 2021.09.16 15:20:03 -04'00' | Capacity: Place, date: Williams, Christopher Signature: Christopher Date: 2021.09.16 14:02:53 -04'00' |
| 9. | UAE | Commerzbank AG Dubai Branch Suite 11 - 15, Building GV 05, 4th floor Gate Village, DIFC, Dubai Dubai United Arab Emirates Postal address: P.O. Box 506596 Dubai United Arab Emirates (based in Dubai International Financial Centre ("DIFC")) | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |

| | | | | | | |
|----|-----|---|-------------------------------------|-------------------------------------|--|--|
| 8. | USA | Commerzbank AG New York Branch 225 Liberty Street New York, NY 10281-1050 USA | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |
| | | Commerz Markets LLC 225 Liberty Street New York, NY 10281-1050 USA | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Place, date: Signature: | Capacity: Place, date: Signature: |
| 9. | UAE | Commerzbank AG Dubai Branch Suite 11 - 15, Building GV 05, 4th floor Gate Village, DIFC, Dubai Dubai United Arab Emirates Postal address: P.O. Box 506596 Dubai United Arab Emirates (based in Dubai International Financial Centre ("DIFC")) | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Capacity: Country CEO GCC Place, date: Signature:  | Capacity: Local COO DIFC Branch Place, date: Signature:  |