Amendment of Commerzbank Data Processing and Guarantee Agreement

Commerzbank AG has amended the attached Data Processing and Guarantee Agreement ("**DPGA**") in the name and on behalf of all the Parties to the DPGA listed below, in particular, to reflect changes regarding branches and processing activities, with the effective date of 22 May 2026 by signing this amended version of the DPGA for itself in its own name and on behalf of the other Parties in their name (Section 4.3 of the Main Body of the DPGA).

The amended DPGA applies for:

1. Commerzbank AG
2. Commerzbank AG, Vienna Branch
3. Commerzbank AG acting through COMMERZBANK Aktiengesellschaft, Pobočka Praha, Prague Branch
4. Commerzbank AG, Paris Branch
5. Commerzbank AG, Milan Branch
6. Commerzbank Finance & Covered Bond S.A.
7. Commerzbank AG, Benelux Branch
8. Commerzbank AG acting through Commerzbank Aktiengesellschaft Spółka Akcyjna Oddział w Polsce
9. mBank SA
10. Commerzbank AG, Madrid Branch
11. Commerzbank AG, Filiale Zürich
12. Commerzbank AG, London Branch
13. Commerzbank AG, Beijing Branch
14. Commerzbank AG, Shanghai Branch
15. Commerzbank AG, Tokyo Branch
16. Commerzbank (Eurasija) AO
17. Commerzbank AG, Singapore Branch
18. Commerzbank AG, New York Branch
19. Commerz Markets LLC
20. Digital Technology Center Commerzbank AG, Sofia Branch
21. CERI International Sp. z o.o.

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, 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 respectively applicable Modules of the Standard Contractual Clauses for the Transfer of Personal Data to Third Countries pursuant to Commission Implementing Decision (EU) 2021/914 of 4 June 2021 – each a "**Model Contract**" and collectively the **"Model Contracts**";

WHEREAS, in their wish to comply with data protection laws applicable in particular in the EU/EEA the Parties by September 2021 had entered into a Data Processing and Guarantee Agreement ("**DPGA 2021**") and now wish to adapt their contractual relationship to the Commission Implementing Decision (EU) 2021/914 of 4 June 2021;

WHEREAS, the Model Contracts 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 respective Model Contract as set out in the Exhibits hereto ("**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 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 Contracts 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 I.B to the Exhibits hereto;

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 for controller to controller transfers as per Commission Implementing Decision (EU) 2021/914 of 4 June 2021 ("**Model Contract C2C"**);
APPENDIX TO EXHIBIT 1	
ANNEX I.A TO EXHIBIT 1 – LIST OF PARTIES:	Provides a list of all Parties to the Model Contract C2C and their role as Data Exporters and/or Data Importers respectively according to Annex I.A of the Model Contract C2C
ANNEX I.B TO EXHIBIT 1 – DESCRIPTION OF TRANSFER:	Contains descriptions of transfers of personal data according to Annex I.B of the Model Contract C2C;
ANNEX I.C. TO EXHIBIT 1 – COMPETENT SUPERVISORY AUTHORITY:	Lists the competent Supervisory Authorities according to Annex I.C. of the Model Contract C2C
ANNEX II TO EXHIBIT 1 – TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA:	Provides information on the technical and organisational measures applicable to the data exchange under the Model Contract C2C according to its Annex II
ANNEX III TO EXHIBIT 1 – LIST OF SUB-PROCESSORS:	*Intentionally left blank as not applicable to the Model Contract C2C*
ANNEX IV TO EXHIBIT 1 – LOCAL LAW AMENDMENTS:	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;
Exhibit 2: Model Contract C2P:	contains the unmodified body document of the Model Contract C2P for controller to processor transfers as per Commission Implementing Decision (EU) 2021/914 of 4 June 2021 (**"Model Contract C2P"**);
APPENDIX TO EXHIBIT 2	
ANNEX I.A TO EXHIBIT 2 – LIST OF PARTIES:	Provides a list of all Parties to the Model Contract C2P and their role as Data Exporters and/or Data Importers respectively according to Annex I.A of the Model Contract C2P

ANNEX I.B TO EXHIBIT 2 – DESCRIPTION OF TRANSFER:	Contain descriptions of transfers of personal data according to Annex I.B of the Model Contract C2P;
ANNEX I.C. TO EXHIBIT 2 – COMPETENT SUPERVISORY AUTHORITY:	Lists the competent Supervisory Authorities according to Annex I.C. of the Model Contract C2P
ANNEX II TO EXHIBIT 2 – TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA:	Provides information on the technical and organisational measures applicable to the data exchange under the Model Contract C2P according to its Annex II
ANNEX III TO EXHIBIT 2 – LIST OF SUB-PROCESSORS:	*Intentionally left blank as not applicable to the Model Contract C2P*
ANNEX IV TO EXHIBIT 2 – LOCAL LAW AMENDMENTS:	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;
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 respectively applicable Model Contract with each other Party (as applicable).

1.3 For transfers of personal data from an EU/EEA country to a non-EU/EEA country the clauses of the respectively applicable Exhibit hereto (e.g., the Model Contract C2C for data transfers controller to controller) and its Annexes shall prevail over any conflicting clauses in the remainder of the DPGA, unless expressly called out otherwise in Annex IV to the respective Exhibit (Local Law Amendments). For the avoidance of doubt, any provisions in this DPGA that do not contradict the respective Model Contract shall remain valid.

1.4 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 respectively applicable Model Contract as set out in the Exhibits hereto. 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.

1.5 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.

1.6 In relation to any transfers of personal data from an EU/EEA country to Japan, Switzerland and / or the United Kingdom, clauses 1.2 to 1.5 shall apply and the Model Contract(s) (as applicable) shall apply if the importing country in question:

(a) is not a White-List Country; and
(b) there are no other arrangements (including without limitation transitional arrangements) or legislation in place permitting the transfer of personal data from the EU/EEA to this country 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(s) where defined terms are not capitalized):

2.1 The term "**Clauses**", as used herein, shall be interpreted as meaning all provisions of this DPGA, unless provided otherwise in the relevant context;

2.2 The term "**Data Exporter**", as used herein, shall be interpreted as meaning each entity specified as a Data Exporter in the relevant Annex I.A to the respective Exhibit, 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);

2.3 The term "**Data Importer**", as used herein, shall be interpreted as meaning each entity specified as a Data Importer in the relevant Annex I.A to the respective Exhibit, 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);

2.4 The term "**Service**" or "**Services**", as used herein, shall mean the (processing) services rendered by the Data Importer, as described in Annex I.B to Exhibit 1 and Annex I.B to Exhibit 2 (also if used with additions or in variations, for instance "processing Services");

2.5 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);

2.6 The terms "**Subprocessor**", "**Sub-processor**" 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;,

2.7 "**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 IV to each of the Exhibits hereto. These amendments shall apply to any data transfer or set of transfers described in Annexes I.B. to the respective Exhibit (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

4.1 Commerzbank AG shall be entitled to amend this DPGA in the name and on behalf of all the entities party to this agreement from time to time unless such amendments are prohibited by applicable law or the terms of this DPGA. Further data processing activities may be added or amended by Commerzbank AG unilaterally subject to its reasonable discretion.

4.2 Subject to its reasonable discretion Commerzbank AG in the name and on behalf of all the entities party to this agreement may agree with any (i) entity that is party to this DPGA to exclude it from this DPGA and / or (ii) other entity to include this entity as an additional party to this DPGA.

4.3 Commerzbank AG shall inform the Parties to this DPGA of any amendment (Clause 4.1) and/or any exclusion / addition of parties (Clause 4.2) – e.g., by providing new Annexes or by providing an amended Signature Page respectively – thirty (30) days prior to their entry into force. Clause 7 of Exhibit 1 and Exhibit 2 shall remain unaffected.

5. Term and termination

5.1 This DPGA shall come into force as from December 25, 12.00 p.m. CET / December 26, 2022, 00.00 a.m. CET ("**Effective Date**").

5.2 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 5.3.

5.3 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 the Exhibits hereto, 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 17 of the respective Exhibit. For the avoidance of doubt and by way of example for Exhibit 1 and its Annexes the choice of law according to Clause 17 of Exhibit 1 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.

6.6 As from the Effective Date the DPGA 2021 shall be repealed.

Signatures: See Signature Page

Exhibit 1: Model Contract C2C

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

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

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

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

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

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.5 (e) and Clause 8.9(b);

(iii) *intentionally left blank as n/a*;

(iv) Clause 12(a) and (d);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b);

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

8.1 **Purpose limitation**

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

(i) where it has obtained the data subject's prior consent;

(ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 **Transparency**

(a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:

(i) of its identity and contact details;

(ii) of the categories of personal data processed;

(iii) of the right to obtain a copy of these Clauses;

(vi) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

(b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

(c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

(d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 **Accuracy and data minimisation**

(a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

(b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

(c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 **Storage limitation**

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

8.5 **Security of processing**

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

(b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(d) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.

(e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

(f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

(g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 **Sensitive data**

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

8.7 **Onward transfers**

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

(i) it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;

(iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

(iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;

(v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or

(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the

lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

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

8.8 **Processing under the authority of the data importer**

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

8.9 **Documentation and compliance**

(a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

(b) The data importer shall make such documentation available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

Intentionally left blank as not applicable

Clause 10

Data subject rights

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request. The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

(b) In particular, upon request by the data subject the data importer shall, free of charge:

(i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

(ii) rectify inaccurate or incomplete data concerning the data subject;

(iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

(c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

(d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter 'automated decision'), which would produce legal effects concerning the data subject or similarly significantly affect him/her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

(i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

(ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

(e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

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

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject

b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

Clause 13

Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

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

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

Clause 14

Local laws and practices affecting compliance with the Clauses

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

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

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

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

15.1 **Notification**

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 **Review of legality and data minimisation**

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

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

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

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

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

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

Clause 17

Governing law

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

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Germany.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX
TO EXHIBIT 1

ANNEX I A TO EXHIBIT 1
- LIST OF PARTIES –

Name	**Commerzbank AG, Vienna Branch**
Address	Hietzinger Kai 101 – 105, 1130 Vienna, Austria
Contact person's name, position and contact details:	Data Protection Contact Commerzbank AG, Vienna Branch Hietzinger Kai 101-105, 1130 Vienna, Austria E-mail: info.vienna@commerzbank.com
Activities relevant to the data transferred under these Clauses	A broad range of banking activities for corporate customers such as but not limited to the opening and maintaining of accounts, credit relations etc.
Data Exporter	yes
Data Importer	yes
Controller	yes
Processor	yes
Signature and date	

Name	**Commerzbank AG acting through** **COMMERZBANK Aktiengesellschaft, Pobočka Praha, Prague Branch**
Address	Jugoslávská 1, 120 21 Praha 2, Czech Republic
Contact person's name, position and contact details:	Data Protection Contact Commerzbank AG, Prague Branch Jugoslavska 934/1, 12000 Praha 2, Czech Republic E-mail: GS-OSISPrag@commerzbank.com
Activities relevant to the data transferred under these Clauses	A broad range of banking activities for corporate customers such as but not limited to the opening and maintaining of accounts, credit relations etc.
Data Exporter	yes
Data Importer	yes
Controller	yes
Processor	yes
Signature and date	

Name	**Commerzbank AG, Paris Branch**
Address	86 Boulevard Haussmann, 75008 Paris, France
Contact person's name, position and contact details:	Data Protection Officer Commerzbank AG, Paris Branch 86 Boulevard Haussmann – F-75008 Paris E-mail: rdt@commerzbank.com
Activities relevant to the data transferred under these Clauses	A broad range of banking activities for corporate customers such as but not limited to the opening and maintaining of accounts, credit relations etc.
Data Exporter	yes
Data Importer	yes
Controller	yes
Processor	yes
Signature and date	

Name	**Commerzbank AG**
Address	Kaiserstraße 16 (Kaiserplatz), 60311 Frankfurt/Main, Germany
Contact person's name, position and contact details:	Data Protection Officer Commerzbank AG Kaiserstrasse 16 (Kaiserplatz), 60261 Frankfurt am Main E-mail: datenschutzbeauftragter@commerzbank.com
Activities relevant to the data transferred under these Clauses	A broad range of banking activities such as but not limited to the opening and maintaining of accounts, credit relations etc.
Data Exporter	yes
Data Importer	yes
Controller	yes
Processor	yes
Signature and date	

Name	**Commerzbank AG, Milan Branch**
Address	Corso Europa 2, 20122 Milan, Italy
Contact person's name, position and contact details:	Data Protection Contact Commerzbank AG, Milan Branch Corso Europa 2, 20122 Milano, Italia E-mail: compliance.milano@commerzbank.com
Activities relevant to the data transferred under these Clauses	A broad range of banking activities for corporate customers such as but not limited to the opening and maintaining of accounts, credit relations etc.
Data Exporter	yes
Data Importer	yes
Controller	yes
Processor	yes
Signature and date	

Name	**Commerzbank Finance & Covered Bond S.A.**
Address	5 rue Jean Monnet , L-2180 Luxembourg Grand Duchy of Luxembourg
Contact person's name, position and contact details:	Data Protection Contact Commerzbank Finance & Covered Bond S.A. 25, rue Edward Steichen, L-2540 Luxembourg Grand Duchy of Luxembourg E-mail: dataprotection-luxembourg@commerzbank.com
Activities relevant to the data transferred under these Clauses	A broad range of banking activities for corporate customers such as but not limited to the opening and maintaining of accounts, credit relations etc.
Data Exporter	yes
Data Importer	yes
Controller	yes
Processor	yes
Signature and date	

Name	**Commerzbank AG, Benelux Branch**
Address	Claude Debussylaan 24 (10th Floor), 1082 MD Amsterdam, The Netherlands
Contact person's name, position and contact details:	Data Protection Contact Commerzbank AG, Benelux Branch Claude Debussylaan 24, 1082 MD Amsterdam, The Netherlands E-mail: DataprotectionAMS@commerzbank.com
Activities relevant to the data transferred under these Clauses	A broad range of banking activities for corporate customers such as but not limited to the opening and maintaining of accounts, credit relations etc.
Data Exporter	yes
Data Importer	yes
Controller	yes
Processor	yes
Signature and date	

Name	**mBank SA**
Address	ul. Prosta 18, 00-850 Warszawa Poland
Contact person's name, position and contact details:	Data Protection Contact (Inspektor Danych Osobowych) mBank SA ul. Prosta 18, 00-850 Warszawa, Poland E-mail: inspektordanychosobowych@mbank.pl
Activities relevant to the data transferred under these Clauses	A broad range of banking activities for corporate customers such as but not limited to the opening and maintaining of accounts, credit relations etc.
Data Exporter	yes
Data Importer	yes
Controller	yes
Processor	yes
Signature and date	

Name	**Commerzbank AG, Madrid Branch**
Address	Torre de Cristal, Paseo de la Castellana 259 C, 28046 Madrid, Spain
Contact person's name, position and contact details:	Data Protection Contact Commerzbank AG, Madrid Branch Paseo de la Castellana 259 C, 28046 Madrid, Spain E-mail: Madrid.Protecciondatos@commerzbank.com
Activities relevant to the data transferred under these Clauses	A broad range of banking activities for corporate customers such as but not limited to the opening and maintaining of accounts, credit relations etc.
Data Exporter	yes
Data Importer	yes
Controller	yes
Processor	yes
Signature and date	

Name	**Commerzbank AG, Filiale Zürich**
Address	Pelikanplatz 15, 8001 Zürich, Switzerland
Contact person's name, position and contact details:	Data Protection Contact Commerzbank AG, Zurich Branch Pelikanplatz 15, 8001 Zürich Telefon: +41 44563 6931 datenschutz.zuerich@commerzbank.com
Activities relevant to the data transferred under these Clauses	A broad range of banking activities for corporate customers such as but not limited to the opening and maintaining of accounts, credit relations etc.
Data Exporter	yes
Data Importer	yes
Controller	yes
Processor	yes
Signature and date	

Name	**Commerzbank AG, London Branch**
Address	30 Gresham Street, London EC2V7PG, United Kingdom
Contact person's name, position and contact details:	Data Protection Officer Commerzbank AG, London Branch 30 Gresham Street, London EC2V 7PG, UK E-mail: Dataprotection.london@commerzbank.com
Activities relevant to the data transferred under these Clauses	A broad range of banking activities for corporate customers such as but not limited to the opening and maintaining of accounts, credit relations etc.
Data Exporter	yes
Data Importer	yes
Controller	yes
Processor	yes
Signature and date	

Name	**Commerzbank AG, Beijing Branch**
Address	Suite 2502 East Tower, Twin Towers, B-12 Jianguomenwai Dajie, Chaoyang District, Beijing 100022, People's Republic of China
Contact person's name, position and contact details:	Data Protection Officer Commerzbank AG, Beijing Branch 2602, C Tower, Beijing Yintai Centre, No.2 Jianguomenwai Street, Chaoyang District, Beijing 100022 E-mail: DPOChina@commerzbank.com
Activities relevant to the data transferred under these Clauses	A broad range of banking activities for corporate customers such as but not limited to the opening and maintaining of accounts, credit relations etc.
Data Exporter	yes
Data Importer	yes
Controller	yes
Processor	yes
Signature and date	

Name	**Commerzbank AG, Shanghai Branch**
Address	37F, Shanghai World Financial Center, 100 Century Avenue, Pudong, 200120 Shanghai, People's Republic of China
Contact person's name, position and contact details:	Data Protection Officer Commerzbank AG, Shanghai Branch 37F Shanghai World Financial Center, 100 Century Avenue, Pudong, Shanghai 200120 E-mail: DPOChina@commerzbank.com
Activities relevant to the data transferred under these Clauses	A broad range of banking activities for primarily corporate customers such as but not limited to the opening and maintaining of accounts, credit relations etc.
Data Exporter	yes
Data Importer	yes
Controller	yes
bene	yes
Signature and date	

Name	**Commerzbank AG, Tokyo Branch**
Address	Toranomon Hills Station Tower 9F , 2-6-1 Toranomon, Minato-ku, Tokyo 105-5509, Japan
Contact person's name, position and contact details:	Data Protection Officer Commerzbank AG, Tokyo Branch Toranomon Hills Station Tower 9F2-6-1 Toranomon, Minato-ku, TokyoE-mail: tokyo-corporatesinternational@commerzbank.com
Activities relevant to the data transferred under these Clauses	A broad range of banking activities for corporate customers such as but not limited to the opening and maintaining of accounts, credit relations etc.
Data Exporter	yes
Data Importer	yes
Controller	yes
Processor	yes
Signature and date	

Name	**Commerzbank (Eurasija) AO**
Address	14/2 Kadashevskaya Nab., 119017 Moscow, Russia
Contact person's name, position and contact details:	Data Protection Contact (ISO) Commerzbank (Eurasija) AO (subsidiary) 119017 Moscow, Russia, Kadashevskaya nab., 14/2 E-mail: Roman.Kirdeev@commerzbank.com Data Protection Contact (COO) Commerzbank (Eurasija) AO (subsidiary) 119017 Moscow, Russia, Kadashevskaya nab., 14/2 E-mail: Sergey.Prusakov@commerzbank.com
Activities relevant to the data transferred under these Clauses	A broad range of banking activities for primarily corporate customers such as but not limited to the opening and maintaining of accounts, credit relations etc.
Data Exporter	yes
Data Importer	yes
Controller	yes
Processor	yes
Signature and date	

Name	**Commerzbank AG, Singapore Branch**
Address	128 Beach Road, #17-01, Guoco Midtown, Singapore 189773
Contact person's name, position and contact details:	Data Protection Officer Commerzbank AG, Singapore Branch 128 Beach Road, #17-01, Guoco Midtown, Singapore 189773 E-mail: DPOSingapore@commerzbank.com
Activities relevant to the data transferred under these Clauses	A broad range of banking activities for corporate customers such as but not limited to the opening and maintaining of accounts, credit relations etc.
Data Exporter	yes
Data Importer	yes
Controller	yes
Processor	yes
Signature and date	

Name	**Commerzbank AG, New York Branch**
Address	225 Liberty Street, New York, NY 10281-1050, USA
Contact person's name, position and contact details:	Data Protection Contact Commerzbank AG, New York Branch 225 Liberty Street, New York, NY 10281-1050, USA E-mail: infosecny@commerzbank.com
Activities relevant to the data transferred under these Clauses	A broad range of banking activities for corporate customers such as but not limited to the opening and maintaining of accounts, credit relations etc.
Data Exporter	yes
Data Importer	yes
Controller	yes
Processor	yes
Signature and date	

Name	**Commerz Markets LLC**
Address	225 Liberty Street, New York, NY 10281-1050, USA
Contact person's name, position and contact details:	Data Protection Contact Commerz Markets LLC 225 Liberty Street, New York, NY 10281-1050, USA E-mail: infosecny@commerzbank.com
Activities relevant to the data transferred under these Clauses	A broad range of banking activities for corporate customers such as but not limited to the opening and maintaining of accounts, credit relations etc.
Data Exporter	yes
Data Importer	yes
Controller	yes
Processor	yes
Signature and date	

APPENDIX
TO EXHIBIT 1

ANNEX I.B.1 TO EXHIBIT 1
- DESCRIPTION OF TRANSFER -

KNOW YOUR CUSTOMER DATA SHARING

Categories of data subjects whose personal data is transferred

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

Categories of personal data transferred

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

1. Customers, e.g. • Full name / first names • Title • Function • E-mail 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 • E-mail 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/funds, if required • Results of screening and negative news search

Sensitive data transferred (if appliable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

n/a

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis)

Data are transferred on a continuous basis.

Nature of the processing

Data are processed by way of collecting, recording, structuring, storing, disclosure by transfer, erasure.

The data will be exported by the Commerzbank entities and branches marked as Exporter as per Annex I.A and imported by the Commerzbank entities and branches marked as Importer as per Annex I.A.

Purpose(s) of the data transfer and further processing

Customer Due Diligence in accordance with group-wide standards and local requirements

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Group-wide standard for the maximum retention is 10 years, but a minimum retention for a period of 5 years must be ensured; local requirements may vary.

For transfers to (sub-)processors, also specify subject matter, nature and duration of the processing

Subject matter, nature and duration of processing by a (sub-)processor, if any, depend upon the respective "Use Case" and may vary but never go beyond the previous transfer from the Exporter as per Annex I.A to the Importer as per Annex I.A as described herein. If retained (sub-)processors, if any, are obliged by contract to erase data when the contractual relationship is terminated or when retention periods have expired.

APPENDIX
TO EXHIBIT 1

ANNEX I.B.2 TO EXHIBIT 1
- DESCRIPTION OF TRANSFER -

AUDIT / REPORTING

Categories of data subjects whose personal data is transferred

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

Categories of personal data transferred

Customers	**Contact persons of (corporate) customers and of potential (corporate) customers**	**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 • E-mail address • Phone, fax • Concerned data of business relationship	e.g. • Name • Function • Phone, fax • E-mail address	e.g. • Full name/first names • Title • Function • E-mail address • Phone, fax

Sensitive data transferred (if appliable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

n/a

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis)

Data may be transferred on a continuous basis and / or on a one-off basis, e.g. in the case of specific audit procedures.

Nature of the processing

Data are processed by way of collecting, recording, structuring, storing, disclosure by transfer, erasure.

The Data will be exported by the Commerzbank entities and branches marked as Exporter as per Annex I.A and imported by the Commerzbank entities and branches marked as Importer as per Annex I.A.

Purpose(s) of the data transfer and further processing

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

- 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.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Data will be retained in line with applicable statutory retention periods. In particular audit reports for standard audits will be retained for a period of 10 years, audit reports related to special investigations for 30 years, working documents for 6 years. Due to local legislation longer retention periods may apply.

For transfers to (sub-)processors, also specify subject matter, nature and duration of the processing

Subject matter, nature and duration of processing by a (sub-)processor, if any, depend upon the respective "Use Case" and may vary but never go beyond the previous transfer from the Exporter as per Annex I.A to the Importer as per Annex I.A as described herein. If retained (sub-)processors, if any, are obliged by contract to erase data when the contractual relationship is terminated or when retention periods have expired.

APPENDIX
TO EXHIBIT 1

ANNEX I.B.3 TO EXHIBIT 1
- DESCRIPTION OF TRANSFER -

GLOBAL SURVEILLANCE & MONITORING

Categories of data subjects whose personal data is transferred

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

Trade surveillance & monitoring	Communication surveillance
• Customers • Employees	• Customers • Potential customers • Employees • Third parties

Categories of personal data transferred

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

Trade surveillance & monitoring:	Communication surveillance:
e.g.: • Order data • Trade data • Customer data (e.g. client or counterparty data such as client number or deposit number, decision maker (asset management mandates, algo trade responsibles, legal representative) • Employee data (e.g. deposit number) • Market data • Research data • Static data (e.g. portfolio hierarchy, instrument data) • Additional compliance data (e.g. Watch List, Restricted List)	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/potential customer data (e.g. E-Mail address, phone number, name, content of communication)

Sensitive data transferred (if appliable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

n/a

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis)

Data are transferred on a continuous basis.

Nature of the processing

Data are processed by way of recording, structuring, storing, using, disclosure by transfer, erasure.

The Data will be exported by the Commerzbank entities and branches marked as Exporter as per Annex I.A*)* and imported by the Commerzbank entities and branches marked as Importer as per Annex I.A.

Purpose(s) of the data transfer and further processing

For both, Trade Surveillance & Monitoring 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.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Data will be retained in line with applicable statutory retention periods.

For transfers to (sub-)processors, also specify subject matter, nature and duration of the processing

Subject matter, nature and duration of processing by a (sub-)processor, if any, depend upon the respective "Use Case" and may vary but never go beyond the previous transfer from the Exporter as per Annex I.A to the Importer as per Annex I.A as described herein. If retained (sub-)processors, if any, are obliged by contract to erase data when the contractual relationship is terminated or when retention periods have expired.

APPENDIX
TO EXHIBIT 1

ANNEX I.B.4 TO EXHIBIT 1
- DESCRIPTION OF TRANSFER -

ANTI-MONEY-LAUNDERING AND COUNTER-TERRORIST FINANCING

Categories of data subjects whose personal data is transferred

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

Global PNG List:	Information sharing via the Financial Crime Unit at Head Office	Internal Reporting and Escalation:
• Customers • Contact persons • Representatives/authorized persons • Keycontrollers (if identified due to local law) and ultimate beneficial owners of corporate customers • Persons included on local external lists	• Customers • Contact persons • Representatives/authorized persons • Keycontrollers (if identified due to local law) and ultimate beneficial owners of corporate customers.	• Customers • Contact persons • Representatives/authorized persons • Keycontrollers (if identified due to local law) and ultimate beneficial owners of corporate customers

Categories of personal data transferred

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

PNG List	Information sharing via the Financial Crime Unit	Internal Reporting and Escalation
• Customers and contact persons, representatives/authorized persons, keycontrollers and ultimate beneficial owners of (corporate) customers o Name o Address o Nationality o Birthplace o Birthdate o Position o Reason for inclusion on Global PNG List (if possible)	• 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	• 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

○ 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)	• 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	• 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)

Sensitive data transferred (if appliable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

n/a

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis)

Data are transferred on a continuous basis.

Nature of the processing

Data are processed by way of collecting, recording, structuring, storing, disclosure by transfer, erasure.

The Data will be exported by the Commerzbank entities and branches marked as Exporter as per Annex I.A and imported by the Commerzbank entities and branches marked as Importer as per Annex I.A.

Purpose(s) of the data transfer and further processing

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.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Retention period differs from category to category

Category A: 30 years	**Category B: 6 years**
In cases of external Suspicious Activity Report ("SAR") and/or account termination, e.g. for reasons of sufficient evidence for terrorist activities	In cases of external SAR and/or account termination, e.g. for reasons of sufficient evidence for violation of German Securities Trading Act ("WpHG")
Category C: 12 months	**Category D: 10 years**
In cases of external SAR related to certain obligations under German Anti-Money-Laundering ("AML") Legislation ("GWG") and/or account termination, e.g. for reasons of AML-related activities without clear evidence	Only in relation to external Service Providers, e.g. in cases of proven criminal offences / serious suspicions of criminal offences

Category E: 5 Years
Only in relation to external Service Providers, e.g. in cases other than covered by category D

For transfers to (sub-)processors, also specify subject matter, nature and duration of the processing

Subject matter, nature and duration of processing by a (sub-)processor, if any, depend upon the respective "Use Case" and may vary but never go beyond the previous transfer from the Exporter as per Annex I.A to the Importer as per Annex I.A as described herein. If retained (sub)-processors, if any, are obliged by contract to erase data when the contractual relationship is terminated or when retention periods have expired.

APPENDIX
TO EXHIBIT 1

ANNEX I.B.5 TO EXHIBIT 1
- DESCRIPTION OF TRANSFER -

CREDIT RISK ASSESSMENT

Categories of data subjects whose personal data is transferred

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

For credit risk assessment/management i.e. credit analysis, credit decision and credit monitoring, (financial) information regarding customers with existing and/or potential new credit exposure (*Bestands- und potentielle Neukunden*) may be affected.

In conjunction with the credit risk assessment/management, employees (credit risk related staff) may also be affected.

Categories of personal data transferred

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

- With regard to credit risk (assessment/management)
    - 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)

- With regard to Employee data

    - Employee data (e.g. e-mail, address, phone number, Comsi-ID, department, name, functional manager, country, employee number)
    - E-mail data (e.g. sender, receiver, subject, text body)
    - Chat communication data (e.g. participants, messages)

Sensitive data transferred (if appliable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

n/a

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis)

Data are generally transferred on a one-off basis, additional data only if deemed necessary.

Nature of the processing
Data are processed by way of collecting, recording, structuring, storing, disclosure by transfer, erasure.

The Data will be exported by the Commerzbank entities and branches marked as Exporter as per Annex I.A and imported by the Commerzbank entities and branches marked as Importer as per Annex I.A.

Purpose(s) of the data transfer and further processing

The transfer is made for the purpose of credit risk assessment/credit risk management, i.e. credit analysis, credit decisions and credit monitoring, (financial) information regarding customers/customer groups with existing and/or potential new credit exposure.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Data are retained for periods in accordance with applicable legal/regulatory requirements such as MaRisk.

For transfers to (sub-)processors, also specify subject matter, nature and duration of the processing

Subject matter, nature and duration of processing by a (sub-)processor, if any, depend upon the respective "Use Case" and may vary but never go beyond the previous transfer from the Exporter as per Annex I.A to the Importer as per Annex I.A as described herein. If retained (sub-)processors, if any, are obliged by contract to erase data when the contractual relationship is terminated or when retention periods have expired.

APPENDIX
TO EXHIBIT 1

ANNEX I.B.6 TO EXHIBIT 1
- DESCRIPTION OF TRANSFER -

PORTFOLIO-, SALES-, CUSTOMER- AND RISK-STEERING

Categories of data subjects whose personal data is transferred

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

Categories of personal data transferred

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

1. Customers, e.g. • Full name/first names • Title • Function • E-mail 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 • E-mail 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/funds, if required • Results of screening and negative news search

Sensitive data transferred (if appliable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

n/a

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis)

Data are transferred on a continuous basis.

Nature of the processing

Data are processed by way of collecting, recording, structuring, storing, disclosure by transfer, erasure.

The data will be exported by the Commerzbank entities and branches marked as Exporter as per Annex I.A and imported by the Commerzbank entities and branches marked as Importer as per Annex I.A.

Purpose(s) of the data transfer and further processing

Data is processed to analyze key performance indicators and to assess the sales performance of different divisions within Corporate Clients. Data is also processed to prepare portfolio steering and client review committees. The purpose of these committees is to discuss (potential) transactions and client exposures including the analysis of a risk and return profile of the transaction and the client

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

10 years

For transfers to sub-processors, also specify subject matter, nature and duration of the processing

n/a

APPENDIX
TO EXHIBIT 1

ANNEX I.B.7 TO EXHIBIT 1
- DESCRIPTION OF TRANSFER -

HR PROCESSES

Categories of data subjects whose personal data is transferred

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

1. Employees, applicants, temporary workers
2. Individual representatives/authorized signatories and/or authorized traders/directors (senior executives, members of the board or governing body) and other executive personnel
3. External service providers, auditors and their personnel

Categories of personal data transferred

Applicants	**Employees / temporary workers and individual representatives/authorized signatories and/or authorized traders/directors (senior executives, members of the board or governing body) and other executive personnel**
• Master, address and communication data (name, gender, date of birth, disability, e-mail, address, etc.) • Date types (application, entry dates, etc.) • CV (e.g., education and training (educational and vocational training (including qualifications, grades, attendance at educational establishments and training received), student status, Work history, spoken/written/reading language proficiency)	• Master, address and communication data (name, gender, date of birth, disability, e-mail, address, etc.) • Date types (application, entry, transfer, leaving dates, etc.) • Time data (vacation, absences, MTA, etc.) • Salary, benefits and pension data (basic salary, one-off payments, health insurance, pension insurance, etc.) • Tax and social security data (tax class, tax number, social security number, etc.) • Training and further education (training, seminar, development, target agreement, assessment, skills data, etc.) • Organizational assignment data (company, organization, position, cost centre, etc.) • Digital personnel file (documents relating to the employment relationship, organized by document type)

External service providers, auditors and their personnel
• Master, address and communication data (name, gender, date of birth, disability, e-mail, address, etc.) • Date types (application, entry, transfer, leaving dates, etc.) • Training and further education (training, seminar, development, target agreement, assessment, skills data, etc.) • Organizational assignment data (company, organization, position, cost centre, etc.)

Sensitive data transferred (if appliable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Applicants	Employees / temporary workers
• Health (e.g. severe disability, maternity protection) • Biometric data (e.g., [ID card and passport photos if provided voluntarily)	• Health (e.g. severe disability, maternity protection, long-term illness) • Religious/ideological beliefs • Racial/ethnic origin (if provided voluntarily) • Biometric data • **France only:** The French employing entity remains the sole controller for employee **NIR** and **health data**; other Group entities shall have no access to these categories. Group IT may host the data solely as processor, with access technically restricted to the French entity (and, for occupational health content, to SPST personnel). See **Annex IV to Exhibit 1 – France (FR-1)**.
Individual representatives/authorized signatories and/or authorized traders/directors (senior executives, members of the board or governing body) and other executive personnel	**External service providers, auditors and their personnel**
• Health (e.g. severe disability, maternity protection, long-term illness) • Religious/ideological beliefs • Racial/ethnic origin • Biometric data	• N/A

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis)

Data are transferred on a continuous basis.

Nature of the processing

Data are processed by way of collecting, recording, disclosure by transmission, deletion/destruction, alteration, blocking, use, review, maintenance or transfer to local databases/directories (e.g., to control local IT applications (business context) or data processing systems by other bodies whose access to personal data cannot be ruled out).

The Data will be exported by the Commerzbank entities and branches marked as Exporter as per Annex I.A and imported by the Commerzbank entities and branches marked as Importer as per Annex I.A.

Purpose(s) of the data transfer and further processing

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

- personnel management processes in the context of the employment relationship, an application or an external service, temporary employment or external audits in accordance with regulatory requirements (e.g., pursuant to the General Data Protection Regulation (GDPR)) and internal requirements.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Data will be retained in line with applicable statutory retention periods.

When determining relevant retention periods, factors, including, but not limited to, the following are considered:

- contractual relationship with the data subject (e.g., employee)
- legal obligations under applicable law to retain personal data for a certain period of time. In Germany such retention obligations may arise, in particular, under the German Commercial Code (*Handelsgesetzbuch*, "**HGB**") or the German Fiscal Code (*Abgabenordnung*, "**AO**"), and may generally be 6 to 10 years (e.g., for contracts and business letters);
- the amount, nature and sensitivity of personal data;
- the potential risk of harm from unauthorised use or disclosure of personal data;
- statutes of limitation under applicable law;
- (potential) disputes;
- guidelines issued by relevant supervisory authorities; and
- archival and backup policies and procedures.

Due to local legislation longer retention periods may apply.

For transfers to (sub-)processors, also specify subject matter, nature and duration of the processing

Subject matter, nature and duration of processing by a (sub-)processor, if any, depend upon the respective "Use Case" and may vary but never go beyond the previous transfer from the Exporter as per Annex I.A to the Importer as per Annex I.A as described herein. If retained (sub-)processors, if any, are obliged by contract to erase data when the contractual relationship is terminated or when retention periods have expired.

APPENDIX
TO EXHIBIT 1

ANNEX I.B.8 TO EXHIBIT 1
- DESCRIPTION OF TRANSFER –

ACTIVE DIRECTORY

Categories of data subjects whose personal data is transferred

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

The on-premises global operations of the Microsoft Active Directory (AD) infrastructure and the worldwide cloud-based services of Microsoft Entra ID (previously known as Azure Active Directory) are used as repositories for user objects (user accounts) which are being managed by a central Identity & Access Management System (IAMS). AD is the central authentication and authorization mechanism for all user accounts of the Commerzbank AG.

Categories of personal data transferred

Limited data which user objects contain, e.g.:
- Name of account
- First name, last name
- Organizational information (e. g., title, manager, assistant)
- Address information (e. g., street, city, state)
- Contact information (e. g., mail, phone)
- Exchange specific information (e.g., nickname)
- User profile (e.g., drive mapping containing user account name)
- Further attributes of an account (e.g., canonical name)
- Active Directory system attributes (e.g., date of account creation)

Sensitive data transferred (if appliable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

No special categories of personal data pursuant to Article 9 GDPR is processed.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis)

Continuous synchronization process in place.

Nature of the processing

- Retainment of data which is provided by the central Identity & Access Management System
- Synchronization of data within the Microsoft Active Directory Infrastructure and Entra ID
- Provision of data for parties privileged to access data
- Deletion of data which isn’t possible via automated processing

Purpose(s) of the data transfer and further processing

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

- Localized authentication and authorization processing including operational stabilization and the mitigation of performance degradation.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Depending on the situation, user objects containing personal data are retained for a 6-month period when a leaver process is initiated (end of employment). As long as an employment exists, this data remains retained.

In exceptional cases, immediate deletion is possible.

For transfers to (sub-)processors, also specify subject matter, nature and duration of the processing

Microsoft Entra ID is a cloud-based identity and access management service that employees can use to access external resources. The retaining of data is dependent on the existence of those residing within the infrastructure of the Active Directory, e.g., if a user account is deleted within the Active Directory, this initiates a deletion of the user account residing in the Tenant.

APPENDIX
TO EXHIBIT 1

ANNEX I.C. TO EXHIBIT 1
- COMPETENT SUPERVISORY AUTHORITY -

Competent supervisory authority in accordance with Clause 13 with regard to data exports where the data exporter is established in

Austria	**Österreichische Datenschutzbehörde** Barichgasse 40 - 42 1030 Wien Austria Phone: + 43 1 52 152-0 E-mail: dsb@dsb.gv.at Homepage: www.dsb.gv.at
Bulgaria	**Commission for Personal Data Protection** 2 Prof. Tsvetan Lazarov Blvd. Sofia 1592 Bulgaria Phone: +359 2/91-53-519 E-mail: kzld@cpdp.bg Homepage: https://www.cpdp.bg
Czech Republic	**The Office for Personal Data Protection** Pplk. Sochora 27 170 00 Praha 7 Czech Republic Phone: +420 234 665 111 E-mail: posta@uoou.cz Homepage: https://www.uoou.cz

France	**Commission nationale de l'informatique et des libertés** 3 Place de Fontenoy TSA 80715 75334 Paris Cedex 07 France Phone: +33 (0)1 53 73 22 22 Homepage: www.cnil.fr/en/home
Germany	**Der Hessische Beauftragte für Datenschutz und Informationsfreiheit** Postfach 3163, 65021 Wiesbaden Gustav-Stresemann-Ring 1, 65189 Wiesbaden Phone: +49 6 11/140 80 E-mail: poststelle@datenschutz.hessen.de Homepage: https://www.datenschutz.hessen.de
Italy	**Garante per la Protezione dei Dati Personali** Piazza Venezia n. 11 00187 Roma Italy Phone: + 39 06 69 677.1 E-mail: protocollo@gpdp.it PEC-Mail: protocollo@pec.gdp.it Homepage: https://www.garanteprivacy.it
Japan	**Personal Information Protection Commission** Kasumigaseki Common Gate West Tower 32nd Floor 3-2-1, Kasumigaseki Chiyoda-ku Tokyo, 100-0013 Japan Phone: +81-(0)3-6457-9680 Contact: https://www.ppc.go.jp/en/contactus/ Homepage: https://www.ppc.go.jp/en/
Luxembourg	**Commission nationale pour la protection des données** 15, Boulevard du Jazz 4370 Belvaux Luxembourg Phone: + 352 26 10 601 E-mail: info@cnpd.lu Homepage: https://www.cnpd.lu

The Netherlands	**Autoriteit Persoonsgegevens** PO Box 93374 2509 AJ DEN HAAG The Netherlands Phone: + 31-70-88 88 500 Homepage: https://autoriteitpersoonsgegevens.nl/nl
People's Republic of China	**Office of the Central Cyberspace Affairs Commission/Cyberspace Administration of China (中共中央网络安全和信息化委员会办公室/国家互联网信息办公室)** **No.15 Fucheng Road, Haidian District, Beijing** **Phone: 010-55636504** **Homepage: https://www.cac.gov.cn** **National Financial Regulatory Administration, Shanghai Bureau** (国家金融监督管理总局上海监管局) Address: 35#, Hehuan Road, Pudong New District, Shanghai 200135, PRC. Phone: 86 21 38650100 Homepage: 国家金融监督管理总局 (https://www.nfra.gov.cn/cn/view/pages/index/index.html) **National Financial Regulatory Administration, Beijing Bureau** (国家金融监督管理总局北京监管局) Address: B Area, Bank of Communications Tower, 20# Financial Street, Xicheng District, Beijing 100032 Phone: 86 10 66021378 Homepage: 国家金融监督管理总局 (https://www.nfra.gov.cn/cn/view/pages/index/index.html) **People's Bank of China Shanghai Headquarters /Shanghai Branch** (人民银行上海总部/上海分行) Address: 181# Lujiazui East Road, Pudong New District, Shanghai 200120, Phone: 86 21 58845000 Homepage: 上海总部/上海分行(pbc.gov.cn) **People's Bank of China, Beijing Operation Management Department/Beijing Branch** (人民银行北京营业管理部/北京分行) Address: 79 Yuetan South St, Beijing 100045, Phone: 86 10 68559550 Homepage: 营业管理部/北京分行（北京） (pbc.gov.cn)
Poland	**Prezes Urzędu Ochrony Danych Osobowych (The President of the Office for Personal Data Protection)** ul. Stawki 2 00-193 Warszawa Poland Phone:+48 22 531 03 00 E-mail: kancelaria@uodo.gov.pl

Russia	**Управление Роскомнадзора по Центральному федеральному округу (Roskomnadzor Office for the Central Federal District)** 17997, ГСП-7, Москва г., ш. Старокаширское, д. 2, к. 10 (17997, GSP-7, Moscow, Starokashirskoe shosse, h. 2, b. 10) Phone: 8 (495)587-44-85 E-mail: rsockanc77@rkn.gov.ru Homepage: https://rkn.gov.ru/personal-data/
Singapore	**The Personal Data Protection Commission** 10 Pasir Panjang Road #03-01 Mapletree Business City Singapore 117438 Phone: +65 6377 3131 Contact: online feedback form Homepage: www.pdpc.gov.sg
Spain	**Agencia Espanola de Protección de Datos (AEPD)** C/Jorge Juan, 6 28001 Madrid Spain Phone: + 34 900 293 183 Homepage: https://www.agpd.es/
Switzerland	**Federal Data Protection and Information Commissioner** Feldeggweg 1 CH - 3003 Bern Phone: +41 (0)58 462 43 95 Homepage: https://www.edoeb.admin.ch
United Kingdom	**The Information Commissioner's Office** Wycliffe House, Water Lane Wilmslow Cheshire SK9 5AF Great Britain United Kingdom Phone: +44 303 123 1113 E-mail: dpo@ico.org.uk Homepage: https://www.ico.org.uk
United States	**n/a**

APPENDIX
TO EXHIBIT 1

ANNEX II TO EXHIBIT 1
- TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA -

Description of the technical and organizational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

A. General

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

(1a) Measures to **pseudonymize and anonymize** personal data:
• 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 anonymized sufficiently before transfer. The methods of anonymization are decided case-by-case. Any deviations must undergo a standardized exception process.

Explanation:

Pseudonymization 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 organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. An anonymization 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:
• Development of security concepts via a centralized security analysis application of Commerzbank for IT applications that process personal data and for IT infrastructures. • Encryption measures as set forth in the policy of the bank (Information Security Control Framework). Depending on the data classification determined by the centralized security 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 encrypted in accordance with the defined encoding matrix by the cryptographic processes allowed in the bank in accordance with the technical standard. • In case of cloud services, personal data will be encrypted with Commerzbank keys which are under control and the management of Commerzbank.

Explanation:

Encryption of personal data is a common practice to protect such data from disclosure to unauthorized 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 security concepts via a centralized security 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. • In addition, these applications will undergo a standardized process for the Privacy Impact Assessment. • Encryption measures; see Sec. 1 (1b). • The assignment of authorizations to IT application will be done via a standardized 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 unauthorized 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:**
• 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 security concepts via a centralized security 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 centralized/standardized 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 unauthorized or unlawful processing as well as unintentional loss, unintentional destruction or unintentional damages as well as unauthorized 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:**
• Use of fire protection devices (smoke and fire detectors, fire extinguishers, fire doors, fire extinguishing systems) in the computing center 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 center 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 (centralized and decentralized). • Use or 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 centralized 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:**

- Centralized 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 center and server) so as to realize 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 organizational measures:**
• Continuous improvement process in the information security management system (ISMS). • Regular compliance checks for IT systems processing personal data within the scope of the centralized security analysis process of Commerzbank. The results of these checks will be included in existing risk analyses for modification of the security concepts. • Verification of compliance with the conditions on information security by risk-oriented tests (on the basis of the relevant security compliance checks) by a second line of defense. • 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 organizational measures unless stated under Sec. 1

(2a) Measures to **deny unauthorized 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 safeguard the buildings by the general electronic admission control, the entrances to the rooms of the computing centers are partly secured biometrically and by badge readers. • Access to the computing center by individual admission systems. • External individuals will be accompanied by authorized employees in the special protection zones (such as, among others, the computing center, the technology rooms). • Special authorization processes for access to certain special protection zones. • Transparency and the possibility of analyzing admissions.

Explanation:

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

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

(2b) Measures to **prevent unauthorized individuals from using data processing systems** (controlling access to data processing systems):
• Access to Commerzbank systems through a personalized user ID and password. • Administration of authorization systems for use of the Commerzbank systems. • Application and change management for granting or withdrawing access authorizations, 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 encryption 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 unauthorized individuals from using data processing facilities and processes. In this connection, measures are taken to ensure that only individuals with proper authorization 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 unauthorized individuals** (access control by authorization management):
• Use of personal user IDs and passwords. • Authorization management (rights and roles concept). • Granting authorizations to IT applications will be done in accordance with the standardized process according to the principle of minimum rights ("need-to-know"). • Annual check of authorizations or the scope of authorization (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 authorizations. • Logging of user activities in the Commerzbank systems. • Separation between development, test and production environments.

Explanation:

This means measures to ensure that individuals authorized to use the data processing processes have access only to personal data for which they have access authorization. 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 authorization 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 unauthorized 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 encryption 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 authorization 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 ANNEX II to EXHIBIT 1 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.

APPENDIX
TO EXHIBIT 1

ANNEX III TO EXHIBIT 1
- LIST OF SUB-PROCESSORS -

Intentionally left blank as not applicable to the Model Contract C2C

APPENDIX
TO EXHIBIT 1

ANNEX IV TO EXHIBIT 1
- LOCAL LAW AMENDMENTS -

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

France	**With regard to exports of data from France by a data exporter located in France, Clause 4.3 of the Main Body of the DPGA is replaced by the following:** "Commerzbank AG will communicate the above amendments (Clauses 4.1 and 4.2) 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." **FR-1. Employee Social Security Number (NIR) and Health Data – France** **1.** **Scope.** This clause applies to the HR Processes described in Annex I.B.7 to Exhibit 1, to the extent they concern employees located in France or HR data for which the French employing entity acts as exporter. **2.** **Roles.** For the processing of the French Social Security Number (numéro d'inscription au répertoire des personnes physiques, **NIR**) and any **health data** relating to employees in France, the **French employing entity remains the sole controller**. No other Commerzbank Group entity shall act as controller for such categories. **3.** **Access to health data.** Access to medical content forming part of occupational health surveillance is restricted to the **Service de Prévention et de Santé au Travail (SPST)** and persons acting under the **occupational physician's** authority. The employer may receive only the outcomes and administrative information permitted by French law, such as dates of medical visits, fitness-for-work opinions, and any job-adaptation proposals issued by the occupational physician. **4.** **Access to NIR.** Access to NIR fields is strictly limited to duly authorized personnel of the **French employing entity** for legally permitted HR purposes. No other Commerzbank Group entity or centralized function may access NIR fields. **5.** **Hosting model.** Commerzbank Group IT may host systems containing the above data exclusively as processor on behalf of the French employing entity, provided that: a) Access is logically and organizationally restricted so that only the French employing entity's authorized users (and, for occupational health content, only SPST personnel) can view or retrieve the data. b) Data is segregated at tenant, dataset, or field level; encryption at rest and in transit is implemented; and key management is under the control of the French employing entity.

	c) Administrative, support, and remote access by other Commerzbank Group entities or vendors is prevented by default and, where strictly necessary for maintenance, is exceptional, logged, justified, time-bound, and supervised by the French employing entity or the SPST, as applicable. d) If hosting covers health data within the meaning of the French Public Health Code, the external host (if any) must meet the Hébergeur de Données de Santé (HDS) certification requirements. **6. International transfers.** Cross-border access to the **medical record** content of occupational health surveillance is not permitted. Cross-border access to **NIR** is permitted only where strictly necessary for a purpose authorized by French law and subject to applicable transfer safeguards under the Exhibits. **7. No re-role.** Nothing in this DPGA creates an independent controller role for any non-French Group entity over NIR or health data relating to employees in France.
Italy	**With regard to exports of data from Italy by a data exporter located in Italy, Clause 4.3 of the Main Body of the DPGA is replaced by the following:** "Commerzbank AG will communicate the above amendments (Clauses 4.1 and 4.2) 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."
Japan	**With regard to exports of data from Japan by a data exporter located in Japan,** I. **clauses 1.2 to 1.6 of the Main Body of the DPGA** shall apply and the Model Contract C2C shall apply (as amended in accordance with section II below) to the extent permissible under data protection laws in Japan if personal data is transferred to a jurisdiction which is (a) not subject to an arrangement with Japan (or transitional arrangements) under the laws of Japan permitting the transfer of personal data from Japan to the jurisdiction in which the Data Importer is located; or (b) not subject to an adequacy decision or similar decision (or transitional arrangement) under the laws of Japan permitting the transfer of personal data to jurisdictions outside of Japan **whereby** **II. the Model Contract C2C (if applicable, including its Appendix) shall be amended as follows:** 1. The term "European Union", "Union", "EU", "EU Member State" or "Member State" shall be replaced with the term "Japan". 2. The terms

	• "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" • "Regulation (EU) 2016/679" • "Articles 13 and 14 of Regulation (EU) 2016/679" • "Article 23(1) of Regulation (EU) 2016/679" • "Article 45 of Regulation (EU) 2016/679" • "Articles 46 or 47 of Regulation (EU) 2016/679" shall be replaced with the term "the **Applicable Data Protection Laws and Regulations of Japan**". 3. Clause 2 (a) shall be restated as follows: (a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to the Applicable Data Protection Laws and Regulations of Japan. 4. Clause 4 (a) shall be restated as follows: (a) Where these Clauses use terms that are used in the Applicable Data Protection Laws and Regulations of Japan, in particular but not limited to the terms • "sensitive data" (*you hairyo kojin joho*), • "controller" (*kojin joho toriatsukai jigyo sha*), • "data subject" (*honnin*), • "supervisory authority/authority" (*kojin joho hogo iinkai*), unless the context requires otherwise, each term shall have the same meaning as ascribed to the equivalent term (as indicated in parenthesis above) in these laws and regulations. 5. Clause 8.2 (a) shall be restated as follows: (a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10 or otherwise to comply with Applicable Data Protection Laws and Regulations of Japan, the data importer shall inform them, either directly or through the data exporter: (i) of its identity and contact details; (ii) of the categories of personal data processed; (iii) of the right to obtain a copy of these Clauses; (iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7; and (v) of its purpose of use of personal data 6. Clause 8.8 (*Processing under the authority of the data importer*) shall be restated as follows:

	The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions and supervise the processor as necessary and appropriate to ensure that personal data is securely managed. 7. Clause 8.7 (*Onward transfers*) shall be restated as follows: 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 Applicable Data Protection Laws and Regulations of Japan, but where uncertain, shall default to obtaining consent for the data transfers from data subjects. 8. Clause 10(b)(i) shall be restated as follows: (i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 11 (c)(i); 9. Clause 11 (c)(i), Clause 11 (d) and Clause 11 (e) shall be restated as follows: (c)(i) lodge a complaint with the supervisory authority or any other competent authority in Japan pursuant to Clause 13; d) The parties accept that the data subject may be represented by a not-for-profit body, organization or association under the conditions set out under the Applicable Data Protection Laws and Regulations of Japan, if any. (e) The data importer shall abide by a decision that is binding under Data Protection Laws and Regulations of Japan. 10. Clause 13 (a) shall be restated as follows: (a) The Personal Information Protection Commission shall act as competent supervisory authority. 11. Clause 16 (e) shall be deleted in its entirety. 12. The following Clause 19 shall be added *Clause 19* The Data Importer shall take all reasonable measures to ensure its employees comply with all necessary and appropriate security measures under the Applicable Data Protection Laws and Regulations of Japan, 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 **and** **III. Clause 1.5 of this DPGA notwithstanding,** 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.
People's Republic of China (“**PRC**” - which, when referring to jurisdiction, does not include Hong Kong, Macau and Taiwan)	**With regard to exports of data from PRC by a data exporter located in PRC, (i) the data protection agreements based on the Standard Contract for Outbound Transfer of Personal Information of the Cyberspace Administration of China entered into by Commerzbank AG with Commerzbank AG, Beijing Branch, and Commerzbank AG, Shanghai Branch, apply, and (ii) the following amendments shall be made to the DPGA including** **I. Clause 1.5 of the Main Body of the DPGA shall be replaced with the following:** In the event of inconsistencies between the provisions of this DPGA and any other standard agreement in a form formulated by the competent authority in the PRC (i.e. the Cyberspace Administration of China) between the Parties in relation to the subject-matters addressed herein (the “China Standard Contract”), the provisions of the China Standard Contract shall prevail as it relates to the Parties' data protection obligations in connection with data transfers. **II. Exhibit 1 (if applicable, including its Appendix) shall be amended as follows:** 1. The terms • “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)” • “Regulation (EU) 2016/679” • “Articles 13 and 14 of Regulation (EU) 2016/679” • “Article 23(1) of Regulation (EU) 2016/679” • “Article 28(7) of Regulation (EU) 2016/679” • “Article 45 of Regulation (EU) 2016/679” • “Article 45(3) of Regulation (EU) 2016/679” • “Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679” • “Articles 46 or 47 of Regulation (EU) 2016/679” • “Article 80 (1) of Regulation (EU) 2016/679 shall be replaced with the term "the **Applicable Data Protection Laws and Regulations of the PRC**".

	"**Applicable Data Protection Laws and Regulations of the PRC**" means all laws, administrative regulations, judicial interpretations, regulatory rules and other binding normative documents of the People's Republic of China (for these purposes, excluding the Hong Kong Special Administrative Region, the Macao Special Administrative Region and Taiwan) that relate to the protection of personal information, data security, cybersecurity or cross-border data transfer, in each case, as amended, replaced or supplemented from time to time, including without limitation: (a) the Personal Information Protection Law of the PRC; (b) the Cybersecurity Law of the PRC; (c) the Data Security Law of the PRC; (d) any such implementing regulations, measures, rules and guidelines issued by any competent PRC authority (including the Cyberspace Administration of China and other relevant regulators) in connection with the laws mentioned in (a) to (c); and (e) any other applicable PRC laws and regulations governing the collection, storage, use, processing, transmission, disclosure, security or cross-border transfer of personal information or other data. 2. The term "sensitive data" shall be replaced with the term "sensitive personal data". 3. Clause 2 (a) shall be restated as follows: (a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to the Applicable Data Protection Laws and Regulations of the PRC. 4. Clause 4 (a) shall be restated as follows: (a) Where these Clauses use terms that are used in the Applicable Data Protection Laws and Regulations of the PRC, unless the context requires otherwise, each term shall have the meaning as ascribed to it in these laws and regulations. The foregoing notwithstanding the term "supervisory authority" shall mean the competent data protection authority in the People's Republic of China. 5. Clause 8.7 (*Onward transfers*) shall be restated as follows: The data importer shall not disclose the personal data to a third party located outside the PRC (in the same country as the data importer or in another third country, hereinafter 'onward transfer') unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if: (i) it is to a country benefitting from a decision of the competent body under the Applicable Data Protection Laws and Regulations of the PRC finding that the third country provides adequate protection; (ii) the third party otherwise ensures appropriate safeguards with respect to the processing in question satisfactory under the Applicable Data Protection Laws and Regulations of the PRC;

	(iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter; (iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; (v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or (vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject. Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses and the Applicable Data Protection Laws and Regulations of the PRC, in particular purpose limitation. 6. Clause 10(b)(i) shall be restated as follows: (i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 11 (c)(i); 7. Clause 11 (c)(i), Clause 11 (d) and Clause 11 (e) shall be restated as follows: (c)(i) lodge a complaint with the supervisory authority or the competent authority pursuant to Clause 13; (d) The parties accept that the data subject may be represented by a not-for-profit body, organization or association under the conditions set out under the Applicable Data Protection Laws and Regulations of the PRC, if any. (e) The data importer shall abide by a decision that is binding under the Applicable Data Protection Laws and Regulations of the PRC. 8. Clause 15.2 (a) shall be restated as follows: The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under or in

	violation of the laws and regulations of the country of destination or the PRC, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e). 9. Clause 16 (e) shall be deleted in its entirety. 10. Clause 17 shall be restated as follows: These Clauses shall be governed by the laws of the PRC. 11. Clause 18 shall be restated as follows: (a) Any dispute arising from these Clauses shall be resolved by the courts of the PRC. (b) The Parties agree to submit themselves to the jurisdiction of such courts.
Singapore	**With regard to exports of data from Singapore by a data exporter located in Singapore,** **I. Exhibit 1 (if applicable, including its Appendix) shall be amended as follows:** 1. The terms • "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" • "Regulation (EU) 2016/679" • "Articles 13 and 14 of Regulation (EU) 2016/679" • "Article 23(1) of Regulation (EU) 2016/679" • "Article 28(7) of Regulation (EU) 2016/679" • "Article 45 of Regulation (EU) 2016/679" • "Article 45(3) of Regulation (EU) 2016/679" • "Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679" • "Articles 46 or 47 of Regulation (EU) 2016/679" • "Article 80 (1) of Regulation (EU) 2016/679 shall be replaced with the term "**the Applicable Data Protection Laws and Regulations of Singapore"** which, as used herein, shall be interpreted as meaning any law and regulation of Singapore that is applicable to the parties in their access and use of personal data, including (but not necessarily limited to) the Personal Data Protection Act 2012 and all related regulations, codes of practice and guidelines published by a Regulator relating to personal information**.**

	2. Clause 2 (a) shall be restated as follows: (a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to the Applicable Data Protection Laws and Regulations of Singapore. 3. Clause 4 (a) shall be restated as follows: (a) Where these Clauses use terms that are used in the Applicable Data Protection Laws and Regulations of Singapore, in particular but not limited to • Personal data • Process/processing unless the context requires otherwise, each term shall have the same meaning as ascribed to it in these laws and regulations. The foregoing notwithstanding the term “supervisory authority/authority" shall have the meaning given to the term "Commission" in Singapore’s Personal Data Protection Act including all subsidiary regulation enacted thereunder, whether now or in the future 4. Clause 8.1 (ii) shall be restated as follows: (ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings, provided that: a. prior to such processing, the data importer conducts an assessment to determine that the data importer's interests in such proceedings outweigh any likely residual adverse affect to the data subject; and b. promptly following such processing, the data importer takes reasonable steps to notify the data subject that the data importer has used the data subject's personal data for such purpose, in each case in accordance with the requirements of the Applicable Data Protection Laws and Regulations of Singapore; or 5. Clause 8.2(b) shall be restated as follows: (b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter. In the latter case, the data importer shall, to the extent possible, make the information publicly available. 6. Clause 8.5 (a), Clause 8.5(e), and Clause 8.5 (f) shall be restated as follows: (a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against (i) a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised

	disclosure or access to that data and (ii) the loss of any storage medium or decide on which personal data is stored (hereinafter 'personal data breach').). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. (e) In case of a personal data breach that is likely to: a. result in significant harm to the affected data subject(s) (as defined under Applicable Data Protection Laws and Regulations of Singapore); or b. affect 500 or more individual data subjects (or such other amount of data subjects as indicated by the Applicable Data Protection Laws and Regulations of Singapore), the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain (i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), (ii) its likely consequences, (iii) the measures taken or proposed to address the breach, and (iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay. (f) In case of a personal data breach that is likely to: a. result in significant harm to the affected data subject(s) (as defined under Applicable Data Protection Laws and Regulations of Singapore); or b. affect 500 or more individual data subjects (or such other amount of data subjects as indicated by the Applicable Data Protection Laws and Regulations of Singapore), the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points (ii) to (iv), unless the data importer has promptly implemented measures to render the personal data breach unlikely to result in significant harm to the affected data subject(s) (as defined under Applicable Data Protection Laws and Regulations of Singapore), or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach. 7. Clause 8.7 (*Onward transfers*) shall be restated as follows:

	The data importer shall not disclose the personal data to a third party located outside Singapore (in the same country as the data importer or in another third country, hereinafter 'onward transfer') unless the data exporter has consented to the onward transfer and: (a) such third party is or agrees to be bound by these Clauses, under the appropriate Module; or (b) such third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses and, in any event, as is required by the Applicable Data Protection Laws and Regulations of Singapore, and the data importer provides a copy of these safeguards to the data exporter. Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation. 8. Clause 10 (b) (i) shall be restated as follows: (i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 11 (c)(i); 9. Clause 11 (c)(i), Clause 11 (d) and Clause 11 (e) shall be restated as follows: (c)(i) lodge a complaint with the Commission or any other competent authority in Singapore pursuant to Clause 13; (d) The parties accept that the data subject may be represented by a not-for-profit body, organization or association under the conditions set out under the Applicable Data Protection Laws and Regulations of Singapore, if any. (e) The data importer shall abide by a decision that is binding under the any applicable law of Singapore. 10. Clause 13 (a) shall be restated as follows: (a) The Commission shall act as competent supervisory authority. 11. Clause 16 (e) shall be deleted in its entirety. 12. Clause 17 shall be restated as follows: These Clauses shall be governed by the laws of Singapore.

	13. Clause 18 shall be restated as follows: (a) Any dispute arising from these Clauses shall be resolved by the courts of Singapore. (b) The Parties agree to submit themselves to the jurisdiction of such courts. **and** **II. Clause 1.5 of this DPGA notwithstanding,** 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.
Spain	**With regard to exports of data from Spain by a data exporter located in Spain, Clause 4.3 of the Main Body of the DPGA is replaced by the following:** "Commerzbank AG will communicate the above amendments (Clauses 4.1 and 4.2) 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."
Switzerland	**With regard to exports of data from Switzerland by a data exporter located in Switzerland,** I. **Clauses 1.2 to 1.6 of the Main Body of the DPGA** shall apply and the Model Contract C2C shall apply (as amended in accordance with section II below) to the extent permissible under data protection laws in Switzerland if personal data is transferred to a jurisdiction which is a) not subject to an arrangement with Switzerland (or transitional arrangements under the laws of Switzerland) permitting the transfer of personal data from Switzerland to the jurisdiction in which the Data Importer is located; or b) not subject to an adequacy decision or similar decision (or transitional arrangement) under the laws of Switzerland permitting the transfer of personal data to jurisdictions outside of Switzerland **whereby** **II. the Model Contract C2C (if applicable, including its Appendix) shall be amended as follows:** 1. The term "European Union", "Union", "EU", "EU Member State" or "Member State" shall be replaced with the term "Switzerland". 2. The terms

	• "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" • "Regulation (EU) 2016/679" • "Articles 13 and 14 of Regulation (EU) 2016/679" • "Article 23(1) of Regulation (EU) 2016/679" • "Article 28(7) of Regulation (EU) 2016/679" • "Article 45 of Regulation (EU) 2016/679" • "Article 45(3) of Regulation (EU) 2016/679" • "Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679" • "Articles 46 or 47 of Regulation (EU) 2016/679" • "Article 80 (1) of Regulation (EU) 2016/679 shall be replaced with the term "**the Applicable Data Protection Laws and Regulations of Switzerland**". 3. Clause 2 (a) shall be restated as follows: (a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to the Applicable Data Protection Laws and Regulations of Switzerland. 4. Clause 4 (a) shall be restated as follows: (a) Where these Clauses use terms that are used in the Applicable Data Protection Laws and Regulations of Switzerland, unless the context requires otherwise, each term shall have the same meaning as ascribed to it in these laws and regulations. The foregoing notwithstanding the Term "supervisory authority" shall mean the competent data protection authority of Switzerland. 5. Clause 8.7 (*Onward transfers*) shall be restated as follows: The data importer shall not disclose the personal data to a third party located outside Switzerland (in the same country as the data importer or in another third country, hereinafter 'onward transfer') unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if: (i) it is to a country benefitting from a decision of the competent body under the applicable Laws and regulations of Switzerland finding that the third country provides adequate protection; (ii) the third party otherwise ensures appropriate safeguards with respect to the processing in question satisfactory under the Applicable Data Protection Laws and Regulations of Switzerland; (iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

(iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;

(v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or

(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

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

6. Clause 10(b)(i) shall be restated as follows:

(i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 11 (c)(i);

7. Clause 11 (c)(i), Clause 11 (d) and Clause 11 (e) shall be restated as follows:

(c)(i) lodge a complaint with the supervisory authority or the competent authority pursuant to Clause 13;

d) The parties accept that the data subject may be represented by a not-for-profit body, organization or association under the conditions set out under the Applicable Data Protection Laws and Regulations of Switzerland, if any.

(e) The data importer shall abide by a decision that is binding under the Applicable Data Protection Laws and Regulations of Switzerland.

8. The "supervisory authority" pursuant to Clause 13 shall be the Swiss Federal Data Protection and Information Commissioner.

9. Clause 16 (e) shall be deleted in its entirety.

10. Clause 17 shall be restated as follows:

These Clauses shall be governed by the laws of Switzerland.

11. Clause 18 shall be restated as follows:

	(a) Any dispute arising from these Clauses shall be resolved by the courts of the city of Zurich, Switzerland. The Parties agree to submit themselves to the jurisdiction of such courts.
United Kingdom	If the Data Exporter of a particular transfer/category of transfers of personal data is located in the UK, the "International Data Transfer Addendum to the EU Commission Standard Contractual Clauses" (ANNEX V TO EXHIBIT 1) applies**.**
United States	**With regard to exports of data from the United States by a data exporter located in the United States,** **I. Exhibit 1 (if applicable, including its Appendix) shall be amended as follows:** 1. The terms • "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" • "Regulation (EU) 2016/679" • "Articles 13 and 14 of Regulation (EU) 2016/679" • "Article 23(1) of Regulation (EU) 2016/679" • "Article 28(7) of Regulation (EU) 2016/679" • "Article 45 of Regulation (EU) 2016/679" • "Article 45(3) of Regulation (EU) 2016/679" • "Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679" • "Articles 46 or 47 of Regulation (EU) 2016/679" • "Article 80 (1) of Regulation (EU) 2016/679 shall be replaced with the term "**the Applicable Data Protection Laws and Regulations of the United States**". 2. The terms "competent supervisory authority" and "supervisory authority" shall both be replaced with the term "appropriate regulatory authorities"; 3. Clauses 8.5(e) and 8.5(f) shall be replaced with: (e) In the case of a personal data breach, the data importer shall notify the data subjects concerned, the data exporter, and appropriate regulatory authorities in accordance the Applicable Data Protection Laws and Regulations of the United States. 4. Clause 10(g) shall be restated as follows: (g) If the data importer intends to refuse a data subject's request, it shall, in accordance with the Applicable Data Protection Laws and Regulations of the United States, inform the data subject of the reasons for the refusal and the possibility of appeal, lodging a complaint with an appropriate regulatory authority, and/or seeking judicial redress. 5. Clause 16(c) shall be restated as follows: (c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

	(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension; (ii) the data importer is in substantial or persistent breach of these Clauses; or (iii) the data importer fails to comply with a binding decision of a competent court or appropriate regulatory authority regarding its obligations under these Clauses. In these cases, in accordance with the Applicable Data Protection Laws and Regulations of the United States, it shall inform the appropriate regulatory authorities of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

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.

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.

APPENDIX
TO EXHIBIT 1

ANNEX V TO EXHIBIT 1

- INTERNATIONAL DATA TRANSFER ADDENDUM TO THE EU COMMISSION STANDARD CONTRACTUAL CLAUSES -

VERSION B1.0, in force 21 March 2022

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties [**Drafting Note:** This table does not need to be completed as the information is already provided in other Exhibits]

Start date		
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: Trading name (if different): Main address (if a company registered address): Official registration number (if any) (company number or similar identifier):	Full legal name: Trading name (if different): Main address (if a company registered address): Official registration number (if any) (company number or similar identifier):
Key Contact	Full Name (optional): Job Title: Contact details including email:	Full Name (optional): Job Title: Contact details including email:
Signature (if required for the purposes of Section 2)		

Table 2: Selected SCCs, Modules and Selected Clauses [**Drafting Note:** This table does not need to be completed as the information is already provided in other Exhibits]

Addendum EU SCCs	☒ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: Reference (if any): Other identifier (if any): Or ☐ the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1						
2						
3						
4						

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: **Fehler! Verweisquelle konnte nicht gefunden werden.**
Annex 1B: Description of Transfer: **Fehler! Verweisquelle konnte nicht gefunden werden.** et seqq.
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: **Fehler! Verweisquelle konnte nicht gefunden werden.** et seqq.
Annex III: List of Sub processors (Modules 2 and 3 only): **Fehler! Verweisquelle konnte nicht gefunden werden.** et seqq.

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☐ Importer ☐ Exporter ☒ neither Party

Part 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.

ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

    c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

    a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

    b. In Clause 2, delete the words:

        "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

    c. Clause 6 (Description of the transfer(s)) is replaced with:

        "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

    d. Clause 8.7(i) of Module 1 is replaced with:

        "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

    e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

        "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

    f. References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

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

    h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with:

> "the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:

> "These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

> "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

    a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or

    b. reflects changes to UK Data Protection Laws;

    The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

    a. its direct costs of performing its obligations under the Addendum; and/or

    b. its risk under the Addendum,

    and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by

providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

Alternative Part 2 Mandatory Clauses:

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

Exhibit 2: Model Contract C2P

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

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

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

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

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

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

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

Clause 6
Description of the transfer(s)

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 7

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

Clause 8

Data protection safeguards

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

8.1 **Instructions**

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 **Purpose limitation**

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

8.3 **Transparency**

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

8.4 **Accuracy**

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

8.5 **Duration of processing and erasure or return of data**

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

8.6 **Security of processing**

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 **Sensitive data**

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

8.8 **Onward transfers**

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

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

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

8.9 **Documentation and compliance**

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non- compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least four weeks in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

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

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

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

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

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub- processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

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

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

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

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

15.1 **Notification**

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). [For Module Three: The data exporter shall forward the information to the controller.]

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 **Review of legality and data minimisation**

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

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

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

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

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

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

Clause 17

Governing law

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

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Germany.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX
TO EXHIBIT 2

ANNEX I A TO EXHIBIT 2
- LIST OF PARTIES -

Name	**Commerzbank AG, Vienna Branch**
Address	Hietzinger Kai 101 – 105, 1130 Vienna, Austria
Contact person's name, position and contact details:	Data Protection Contact Commerzbank AG, Vienna Branch Hietzinger Kai 101-105, 1130 Vienna, Austria E-mail: info.vienna@commerzbank.com
Activities relevant to the data transferred under these Clauses	A broad range of banking activities for corporate customers such as but not limited to the opening and maintaining of accounts, credit relations etc.
Data Exporter	yes
Data Importer	yes
Controller	yes
Processor	yes
Signature and date	

Name	**Digital Technology Center Commerzbank AG, Sofia Branch**
Address	Bulgaria, Sofia, district Mladost, zh.k. Mladost 4, 1715, str. Samara 2, Advance Business Center II, 3rd floor
Contact person's name, position and contact details:	Data Protection Contact Digital Technology Center Commerzbank AG, Sofia Branch 2 Samara str., zh.k. Mladost 4, Advance Business Center II, 1715 Sofia, Bulgaria E-mail: DTC_Sofia_GDPR@commerzbank.com
Activities relevant to the data transferred under these Clauses	Various IT-related services in connection with banking activities
Data Exporter	no
Data Importer	yes
Controller	no
Processor	yes
Signature and date	

Name	**Commerzbank AG acting through** **COMMERZBANK Aktiengesellschaft, Pobočka Praha, Prague Branch**
Address	Jugoslávská 1, 120 21 Praha 2, Czech Republic
Contact person's name, position and contact details:	Data Protection Contact Commerzbank AG, Prague Branch Jugoslavska 934/1, 12000 Praha 2, Czech Republic E-mail: GS-OSISPrag@commerzbank.com
Activities relevant to the data transferred under these Clauses	A broad range of banking activities for corporate customers such as but not limited to the opening and maintaining of accounts, credit relations etc.
Data Exporter	yes
Data Importer	yes
Controller	yes
Processor	yes
Signature and date	

Name	**Commerzbank AG, Paris Branch**
Address	86 Boulevard Haussmann, 75008 Paris, France
Contact person's name, position and contact details:	Data Protection Officer Commerzbank AG, Paris Branch 86 Boulevard Haussmann – F-75008 Paris E-mail: rdt@commerzbank.com
Activities relevant to the data transferred under these Clauses	A broad range of banking activities for corporate customers such as but not limited to the opening and maintaining of accounts, credit relations etc.
Data Exporter	yes
Data Importer	yes
Controller	yes
Processor	yes
Signature and date	

Name	**Commerzbank AG**
Address	Kaiserstraße 16 (Kaiserplatz), 60311 Frankfurt/Main, Germany
Contact person's name, position and contact details:	Data Protection Officer Commerzbank AG Kaiserstrasse 16 (Kaiserplatz), 60261 Frankfurt am Main E-mail: datenschutzbeauftragter@commerzbank.com
Activities relevant to the data transferred under these Clauses	A broad range of banking activities such as but not limited to the opening and maintaining of accounts, credit relations etc.
Data Exporter	yes
Data Importer	yes
Controller	yes
Processor	yes
Signature and date	

Name	**Commerzbank AG, Milan Branch**
Address	Corso Europa 2, 20122 Milan, Italy
Contact person's name, position and contact details:	Data Protection Contact Commerzbank AG, Milan Branch Corso Europa 2, 20122 Milano, Italia E-mail: compliance.milano@commerzbank.com
Activities relevant to the data transferred under these Clauses	A broad range of banking activities for corporate customers such as but not limited to the opening and maintaining of accounts, credit relations etc.
Data Exporter	yes
Data Importer	yes
Controller	yes
Processor	yes
Signature and date	

Name	**Commerzbank Finance & Covered Bond S.A.**
Address	5 rue Jean Monnet , L-2180 Luxembourg Grand Duchy of Luxembourg
Contact person's name, position and contact details:	Data Protection Contact Commerzbank Finance & Covered Bond S.A. 25, rue Edward Steichen, L-2540 Luxembourg Grand Duchy of Luxembourg E-mail: dataprotection-luxembourg@commerzbank.com
Activities relevant to the data transferred under these Clauses	A broad range of banking activities for corporate customers such as but not limited to the opening and maintaining of accounts, credit relations etc.
Data Exporter	yes
Data Importer	yes
Controller	yes
Processor	yes
Signature and date	

Name	**Commerzbank AG, Benelux Branch**
Address	Claude Debussylaan 24 (10th Floor), 1082 MD Amsterdam, The Netherlands
Contact person's name, position and contact details:	Data Protection Contact Commerzbank AG, Benelux Branch Claude Debussylaan 24, 1082 MD Amsterdam, The Netherlands E-mail: DataprotectionAMS@commerzbank.com
Activities relevant to the data transferred under these Clauses	A broad range of banking activities for corporate customers such as but not limited to the opening and maintaining of accounts, credit relations etc.
Data Exporter	yes
Data Importer	yes
Controller	yes
Processor	yes
Signature and date	

Name	**mBank SA**
Address	ul. Prosta 18, 00-850 Warszawa Poland
Contact person's name, position and contact details:	Data Protection Contact (Inspektor Danych Osobowych) mBank SA ul. Prosta 18, 00-850 Warszawa, Poland E-mail: inspektordanychosobowych@mbank.pl
Activities relevant to the data transferred under these Clauses	A broad range of banking activities for corporate customers such as but not limited to the opening and maintaining of accounts, credit relations etc.
Data Exporter	yes
Data Importer	yes
Controller	yes
Processor	yes
Signature and date	

Name	**CERI International Sp. z o.o.**
Address	ul. Wersalska 6, 91-203 Łódź, Poland
Contact person's name, position and contact details:	Data Protection Officer CERI International Sp. z o.o. ul. Wersalska 6, 91-203 Łódź, Poland E-mail: iod@ceri.pl
Activities relevant to the data transferred under these Clauses	Various services related to the onboarding and offboarding of (new) customers.
Data Exporter	no
Data Importer	yes
Controller	no
Processor	yes
Signature and date	

Name	**Commerzbank AG, Madrid Branch**
Address	Torre de Cristal, Paseo de la Castellana 259 C, 28046 Madrid, Spain
Contact person's name, position and contact details:	Data Protection Contact Commerzbank AG, Madrid Branch Paseo de la Castellana 259 C, 28046 Madrid, Spain E-mail: Madrid.Protecciondatos@commerzbank.com
Activities relevant to the data transferred under these Clauses	A broad range of banking activities for corporate customers such as but not limited to the opening and maintaining of accounts, credit relations etc.
Data Exporter	yes
Data Importer	yes
Controller	yes
Processor	yes
Signature and date	

Name	**Commerzbank AG, Filiale Zürich**
Address	Pelikanplatz 15, 8001 Zürich, Switzerland
Contact person's name, position and contact details:	Data Protection Contact Commerzbank AG, Zurich Branch Pelikanplatz 15, 8001 Zürich Telefon: +41 44563 6931 datenschutz.zuerich@commerzbank.com
Activities relevant to the data transferred under these Clauses	A broad range of banking activities for corporate customers such as but not limited to the opening and maintaining of accounts, credit relations etc.
Data Exporter	yes
Data Importer	yes
Controller	yes
Processor	yes
Signature and date	

Name	**Commerzbank AG, London Branch**
Address	30 Gresham Street, London EC2V7PG, United Kingdom
Contact person's name, position and contact details:	Data Protection Officer Commerzbank AG, London Branch 30 Gresham Street, London EC2V 7PG, UK E-mail: Dataprotection.london@commerzbank.com
Activities relevant to the data transferred under these Clauses	A broad range of banking activities for corporate customers such as but not limited to the opening and maintaining of accounts, credit relations etc.
Data Exporter	yes
Data Importer	yes
Controller	yes
Processor	yes
Signature and date	

Name	**Commerzbank AG, Beijing Branch**
Address	Suite 2502 East Tower, Twin Towers, B-12 Jianguomenwai Dajie, Chaoyang District, Beijing 100022, People's Republic of China
Contact person's name, position and contact details:	Data Protection Officer Commerzbank AG, Beijing Branch 2602, C Tower, Beijing Yintai Centre, No.2 Jianguomenwai Street, Chaoyang District, Beijing 100022 E-mail: DPOChina@commerzbank.com
Activities relevant to the data transferred under these Clauses	A broad range of banking activities for corporate customers such as but not limited to the opening and maintaining of accounts, credit relations etc.
Data Exporter	yes
Data Importer	yes
Controller	yes
Processor	yes
Signature and date	

Name	**Commerzbank AG, Shanghai Branch**
Address	37F, Shanghai World Financial Center, 100 Century Avenue, Pudong, 200120 Shanghai, People's Republic of China
Contact person's name, position and contact details:	Data Protection Officer Commerzbank AG, Shanghai Branch 37F Shanghai World Financial Center, 100 Century Avenue, Pudong, Shanghai 200120 E-mail: DPOChina@commerzbank.com
Activities relevant to the data transferred under these Clauses	A broad range of banking activities for primarily corporate customers such as but not limited to the opening and maintaining of accounts, credit relations etc.
Data Exporter	yes
Data Importer	yes
Controller	yes
Processor	yes
Signature and date	

Name	**Commerzbank AG, Tokyo Branch**
Address	Toranomon Hills Station Tower 9F, 2-6-1 Toranomon, Minato-ku, Tokyo 105-5509, Japan
Contact person's name, position and contact details:	Data Protection Officer Commerzbank AG, Tokyo Branch Toranomon Hills Station Tower 9F 2-6-1 Toranomon, Minato-ku, TokyoE-mail: tokyo-corporatesinternational@commerzbank.com
Activities relevant to the data transferred under these Clauses	A broad range of banking activities for corporate customers such as but not limited to the opening and maintaining of accounts, credit relations etc.
Data Exporter	yes
Data Importer	yes
Controller	yes
Processor	yes
Signature and date	

Name	**Commerzbank (Eurasija) AO**
Address	14/2 Kadashevskaya Nab., 119017 Moscow, Russia
Contact person's name, position and contact details:	Data Protection Contact (ISO) Commerzbank (Eurasija) AO (subsidiary) 119017 Moscow, Russia, Kadashevskaya nab., 14/2 E-mail: Roman.Kirdeev@commerzbank.com Data Protection Contact (COO) Commerzbank (Eurasija) AO (subsidiary) 119017 Moscow, Russia, Kadashevskaya nab., 14/2 E-mail: Sergey.Prusakov@commerzbank.com
Activities relevant to the data transferred under these Clauses	A broad range of banking activities for primarily corporate customers such as but not limited to the opening and maintaining of accounts, credit relations etc.
Data Exporter	yes
Data Importer	yes
Controller	yes
Processor	yes
Signature and date	

Name	**Commerzbank AG, Singapore Branch**
Address	128 Beach Road #17-01, Guoco Midtown, Singapore 189773
Contact person's name, position and contact details:	Data Protection Officer Commerzbank AG, Singapore Branch 128 Beach Road, #17-01, Guoco Midtown, Singapore 189773 E-mail: DPOSingapore@commerzbank.com
Activities relevant to the data transferred under these Clauses	A broad range of banking activities for corporate customers such as but not limited to the opening and maintaining of accounts, credit relations etc.
Data Exporter	yes
Data Importer	yes
Controller	yes
Processor	yes
Signature and date	

Name	**Commerzbank AG, New York Branch**
Address	225 Liberty Street, New York, NY 10281-1050, USA
Contact person's name, position and contact details:	Data Protection Contact Commerzbank AG, New York Branch 225 Liberty Street, New York, NY 10281-1050, USA E-mail: infosecny@commerzbank.com
Activities relevant to the data transferred under these Clauses	A broad range of banking activities for corporate customers such as but not limited to the opening and maintaining of accounts, credit relations etc.
Data Exporter	yes
Data Importer	yes
Controller	yes
Processor	yes
Signature and date	

Name	**Commerz Markets LLC**
Address	225 Liberty Street, New York, NY 10281-1050, USA
Contact person's name, position and contact details:	Data Protection Contact Commerz Markets LLC 225 Liberty Street, New York, NY 10281-1050, USA E-mail: infosecny@commerzbank.com
Activities relevant to the data transferred under these Clauses	A broad range of banking activities for corporate customers such as but not limited to the opening and maintaining of accounts, credit relations etc.
Data Exporter	yes
Data Importer	yes
Controller	yes
Processor	yes
Signature and date	

APPENDIX
TO EXHIBIT 2

ANNEX I.B.1 TO EXHIBIT 2
- DESCRIPTION OF TRANSFER -

CREDIT RISK ASSESSMENT

Categories of data subjects whose personal data is transferred

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

For credit risk risk assessment/risk management i.e. credit analysis, credit decision and credit monitoring, (financial) information regarding customers with existing and/or potential new credit exposure (Bestands-und potentielle Neukunden) may be affected.

In conjunction with the credit risk assessment/management, employees (credit risk related staff) may also be affected.

Categories of personal data transferred

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

- With regard to credit risk (assessment/management)
  - 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)

- With regard to Employee data
  - Employee data (e.g. e-mail, address, phone-number, Comsi-ID, department, name, functional manager, country, employee number)
  - E-mail data (e.g. sender, receiver, subject, text body)
  - Chat communication data (e.g. participants, messages)

Sensitive data transferred (if appliable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

n/a

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis)

Data are generally transferred on a one-off basis, additional data only if deemed necessary.

Nature of the processing
Data are processed by way of collecting, recording, structuring, storing, disclosure by transfer, erasure

The Data will be exported by the Commerzbank entities and branches marked as Exporter as per Annex I.A and imported by the Commerzbank entities and branches marked as Importer as per Annex I.A.

Purpose(s) of the data transfer and further processing

The transfer is made for the purpose of credit risk assessment/credit risk management, i.e. credit analysis, credit decisions and credit monitoring, (financial) information regarding customers/customer groups with existing and/or potential new credit exposure.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Data are retained for periods in accordance with applicable legal/regulatory requirements such as MaRisk.

For transfers to sub-processors, also specify subject matter, nature and duration of the processing

Subject matter, nature and duration of processing by a sub-processor, if any, depend upon the respective "Use Case" and may vary but never go beyond the previous transfer from Controller to the Processor as described herein. If retained sub-processors, if any, are obliged by contract to erase data when the contractual relationship is terminated or when retention periods have expired.

APPENDIX
TO EXHIBIT 2

ANNEX I.B.2 TO EXHIBIT 2
- DESCRIPTION OF TRANSFER -

CENTRALIZATION OF ONBOARDING/OFFBOARDING

Categories of data subjects whose personal data is transferred

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 personal data transferred

Customers	**Contact persons 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/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/funds, if required • Results of screening and negative news search	e.g. • Name • Function, • Phone, fax • E-mail address

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	Ulitimate Beneficial Owners/Shareholders of (corporate) customers or potential (corporate) customers,
e.g. • Full name / first names • Title • Function • E-mail 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	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/funds, if required • Results of screening and negative news search

Sensitive data transferred (if appliable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

n/a

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis)

Data are transferred on a continuous basis.

Nature of the processing

Data are processed by way of collecting, recording, structuring, storing, disclosure by transfer, erasure.

The Data will be exported by the Commerzbank entities and branches marked as Exporter as per Annex I.A.

The Data will be imported by

- **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
  - **CERI International Sp. z o.o., Poland** (receives personal data from the entities/branches in Austria, Czech Republic, France, Germany, Italy, Luxembourg, the Netherlands, Spain, UK, Switzerland)
  - **Singapore Branch** (receives personal data from various locations)

Purpose(s) of the data transfer and further processing

Customer Due Diligence in accordance with group-wide standards and local requirements

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

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.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Group-wide standard for the maximum retention is 10 years, but a minimum retention for a period of 5 years must be ensured; local requirements may vary.

For transfers to sub-processors, also specify subject matter, nature and duration of the processing

Subject matter, nature and duration of processing by a sub-processor, if any, depend upon the respective "Use Case" and may vary but never go beyond the previous transfer from Controller to the Processor as described herein. If retained sub-processors, if any, are obliged by contract to erase data when the contractual relationship is terminated or when retention periods have expired.

APPENDIX
TO EXHIBIT 2

ANNEX I.B.3 TO EXHIBIT 2
- DESCRIPTION OF TRANSFER -

GLOBAL SURVEILLANCE & MONITORING

Categories of data subjects whose personal data is transferred

The personal data transferred concern, in particular, the following categories of data subj*e*cts:

Trade surveillance & monitoring:	**Communication surveillance:**
• Customers • Employees	• Customers • Potential customers • Employees • Third parties

Categories of personal data transferred

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

Trade surveillance & monitoring	**Communication Surveillance (for trade staff, employees, customers, potential customers, and other third parties)**
e.g. • Order data • Trade data • Customer data (e.g. client or counterparty data such as client number or deposit number, decision maker (asset management mandates, algo trade responsibles, legal representative) • Employee data (e.g. deposit number) • Market data • Research data • Static data (e.g. portfolio hierarchy, instrument data) • Additional compliance data (e.g. Watch List, Restricted List	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/potential customer data (e.g. E-mail address, phone number, name, content of communication)

Sensitive data transferred (if appliable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

n/a

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis)

Data are transferred on a continuous basis.

Nature of the processing

Data are processed by way of recording, structuring, storing, using, disclosure by transfer, erasure.

The Data will be exported by the Commerzbank entities and branches marked as Exporter as per Annex I.A.

The Data will be imported by **Commerzbank AG, Germany** (Head Office) as the host provider for the system for Trade Surveillance & Monitoring and for Communication Surveillance and where the Global Control Room is located.

Purpose(s) of the data transfer and further 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.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Data will be retained in line with applicable statutory retention periods.

For transfers to sub-processors, also specify subject matter, nature and duration of the processing

Subject matter, nature and duration of processing by a sub-processor, if any, depend upon the respective "Use Case" and may vary but never go beyond the previous transfer from Controller to the Processor as described herein. If retained sub-processors, if any, are obliged by contract to erase data when the contractual relationship is terminated or when retention periods have expired.

APPENDIX
TO EXHIBIT 2

ANNEX I.B.4 TO EXHIBIT 2
- DESCRIPTION OF TRANSFER -

ANTI-MONEY-LAUNDERING AND COUNTER-TERRORIST FINANCING

Categories of data subjects whose personal data is transferred

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

Name Screening	Customer Risk Rating	Transaction Monitoring and Sanction Screening
• Customer ultimate beneficial owner • Authorized person • Keycontroller of (corporate) customer (if identified due to local law)	• Customer • Ultimate beneficial owner • Authorized person • Keycontroller of (corporate) customer (if identified due to local law)	• Customer • Ultimate beneficial owner, authorized person • Keycontroller of corporate customer (if identified due to local law)

Categories of personal data transferred

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

Name Screening	Customer Risk Rating	Transaction Monitoring and Sanction Screening
e.g. • Name, • Address, • Birthdate, • Birthplace • Nationality • Position	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	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)

	• 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)	• 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.)

Sensitive data transferred (if appliable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

n/a

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis)

Data are transferred on a continuous basis.

Nature of the processing

Data are processed by way of collecting, recording, structuring, storing, disclosure by transfer, erasure.

The Data will be exported by the Commerzbank entities and branches marked as Exporter as per Annex I.A.
The Data will be imported by Commerzbank AG, Germany (Head Office)

Purpose(s) of the data transfer and further 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.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Data will be retained in line with applicable statutory retention periods.

For transfers to sub-processors, also specify subject matter, nature and duration of the processing

Subject matter, nature and duration of processing by a sub-processor, if any, depend upon the respective "Use Case" and may vary but never go beyond the previous transfer from Controller to the Processor as described herein. If retained sub-processors, if any, are obliged by contract to erase data when the contractual relationship is terminated or when retention periods have expired.

APPENDIX
TO EXHIBIT 2

ANNEX I.B.5 TO EXHIBIT 2
- DESCRIPTION OF TRANSFER -

AUDIT / REPORTING

Categories of data subjects whose personal data is transferred

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.

Categories of personal data transferred

Customers	**Contact persons of (corporate) customers and of potential (corporate) customers**	**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 • E-mail address • Phone, fax • Concerned data of business relationship	e.g. • Name • Function, • Phone, fax • E-mail address	e.g. • Full name/first names • Title • Function • E-mail address • Phone, fax

Sensitive data transferred (if appliable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

n/a

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis)

Data may be transferred on a continuous basis and / or on a one-off basis, e.g. in the case of specific audit procedures.

Nature of the processing

Data are processed by way of collecting, recording, structuring, storing, disclosure by transfer, erasure.

The Data will be exported by the Commerzbank entities and branches marked as Exporter as per Annex I.A and imported by the Commerzbank entities and branches marked as Importer as per Annex I.A.

Purpose(s) of the data transfer and further processing

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

- 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.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Data will be retained in line with applicable statutory retention periods. In particular audit reports for standard audits will be retained for a period of 10 years, audit reports related to special investigations for 30 years, working documents for 6 years. Due to local legislation longer retention periods may apply.

For transfers to sub-processors, also specify subject matter, nature and duration of the processing

Subject matter, nature and duration of processing by a sub-processor, if any, depend upon the respective "Use Case" and may vary but never go beyond the previous transfer from Controller to the Processor as described herein. If retained sub-processors, if any, are obliged by contract to erase data when the contractual relationship is terminated or when retention periods have expired.

APPENDIX
TO EXHIBIT 2

ANNEX I.B.6 TO EXHIBIT 2
- DESCRIPTION OF TRANSFER -

HR PROCESSES

Categories of data subjects whose personal data is transferred

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

1. Employees, applicants, temporary workers
2. Individual representatives/authorized signatories and/or authorized traders/directors (senior executives, members of the board or governing body) and other executive personnel
3. External service providers, auditors and their personnel

Categories of personal data transferred

Applicants	**Employees / temporary workers and individual representatives/authorized signatories and/or authorized traders/directors (senior executives, members of the board or governing body) and other executive personnel**
• Master, address and communication data (name, gender, date of birth, disability, e-mail, address, etc.) • Date types (application, entry dates, etc.) • CV (e.g., education and training (educational and vocational training (including qualifications, grades, attendance at educational establishments and training received), student status, Work history, spoken/written/reading language proficiency)	• Master, address and communication data (name, gender, date of birth, disability, e-mail, address, etc.) • Date types (application, entry, transfer, leaving dates, etc.) • Time data (vacation, absences, MTA, etc.) • Salary, benefits and pension data (basic salary, one-off payments, health insurance, pension insurance, etc.) • Tax and social security data (tax class, tax number, social security number, etc.) • Training and further education (training, seminar, development, target agreement, assessment, skills data, etc.) • Organizational assignment data (company, organization, position, cost centre, etc.) • Digital personnel file (documents relating to the employment relationship, organized by document type)

External service providers, auditors and their personnel
• Master, address and communication data (name, gender, date of birth, disability, e-mail, address, etc.) • Date types (application, entry, transfer, leaving dates, etc.) • Tax and social security data (tax class, tax number, social security number, etc.) • Training and further education (training, seminar, development, target agreement, assessment, skills data, etc.) • Organizational assignment data (company, organization, position, cost centre, etc.

Sensitive data transferred (if appliable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Applicants	Employees / temporary workers and individual representatives/authorized signatories and/or authorized traders/directors (senior executives, members of the board or governing body) and other executive personnel
• Health (e.g. severe disability, maternity protection) • Biometric data (e.g., ID card and passport photos if provided voluntarily)	• Health (e.g. severe disability, maternity protection, long-term illness) • Religious/ideological beliefs • Racial/ethnic origin (if provided voluntarily) • Biometric data • **France only:** The French employing entity remains the sole controller for employee **NIR** and **health data**; other Group entities shall have no access to these categories. Group IT may host the data solely as processor, with access technically restricted to the French entity (and, for occupational health content, to SPST personnel). See **Annex IV to Exhibit 2 – France (FR-1)**. •
External service providers, auditors and their personnel	
• N/A	

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis)

Data are transferred on a continuous basis.

Nature of the processing

Data are processed by way of collecting, recording, disclosure by transmission, deletion/destruction, alteration, blocking, use, review, maintenance or transfer to local databases/directories (e.g., to control local IT applications (business context) or data processing systems by other bodies whose access to personal data cannot be ruled out).

The Data will be exported by the Commerzbank entities and branches marked as Exporter as per Annex I.A and imported by the Commerzbank entities and branches marked as Importer as per Annex I.A.

Purpose(s) of the data transfer and further processing

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

- personnel management processes in the context of the employment relationship, an application or an external service, temporary employment or external audits in accordance with regulatory requirements (e.g., pursuant to the General Data Protection Regulation (GDPR)) and internal requirements.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Data will be retained in line with applicable statutory retention periods.

When determining relevant retention periods, factors, including, but not limited to, the following are considered:

- contractual relationship with the data subject (e.g., employee)
- legal obligations under applicable law to retain personal data for a certain period of time. In Germany such retention obligations may arise, in particular, under the German Commercial Code (*Handelsgesetzbuch*, "**HGB**") or the German Fiscal Code (*Abgabenordnung*, "**AO**"), and may generally be 6 to 10 years (e.g., for contracts and business letters);
- the amount, nature and sensitivity of personal data;
- the potential risk of harm from unauthorised use or disclosure of personal data;
- statutes of limitation under applicable law;
- (potential) disputes;
- guidelines issued by relevant supervisory authorities; and
- archival and backup policies and procedures.

Due to local legislation longer retention periods may apply.

For transfers to sub-processors, also specify subject matter, nature and duration of the processing

Subject matter, nature and duration of processing by a sub-processor, if any, depend upon the respective “Use Case” and may vary but never go beyond the previous transfer from the Exporter as per Annex I.A to the Importer as per Annex I.A as described herein. If retained sub-processors, if any, are obliged by contract to erase data when the contractual relationship is terminated or when retention periods have expired.

APPENDIX
TO EXHIBIT 2

ANNEX I.B.7 TO EXHIBIT 2
- DESCRIPTION OF TRANSFER –

ACTIVE DIRECTORY

Categories of data subjects whose personal data is transferred

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

The on-premises global operations of the Microsoft Active Directory (AD) infrastructure and the worldwide cloud-based services of Microsoft Entra ID (previously known as Azure Active Directory) are used as repositories for user objects (user accounts) which are being managed by a central Identity & Access Management System (IAMS). AD is the central authentication and authorization mechanism for all user accounts of the Commerzbank AG.

Categories of personal data transferred

Limited data which user objects contain, e.g.:
- Name of account
- First name, last name
- Organizational information (e. g., title, manager, assistant)
- Address information (e. g., street, city, state)
- Contact information (e. g., mail, phone)
- Exchange specific information (e.g., nickname)
- User profile (e.g., drive mapping containing user account name)
- Further attributes of an account (e.g., canonical name)
- Active Directory system attributes (e.g., date of account creation)

Sensitive data transferred (if appliable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

No special categories of personal data pursuant to Article 9 GDPR is processed.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis)

Continuous synchronization process in place.

Nature of the processing

- Retainment of data which is provided by the central Identity & Access Management System
- Synchronization of data within the Microsoft Active Directory Infrastructure and Entra ID
- Provision of data for parties privileged to access data
- Deletion of data which isn’t possible via automated processing

Purpose(s) of the data transfer and further processing

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

- Localized authentication and authorization processing including operational stabilization and the mitigation of performance degradation.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Depending on the situation, user objects containing personal data are retained for a 6-month period when a leaver process is initiated (end of employment). As long as an employment exists, this data remains retained.

In exceptional cases, immediate deletion is possible.

For transfers to (sub-)processors, also specify subject matter, nature and duration of the processing

Microsoft Entra ID is a cloud-based identity and access management service that employees can use to access external resources. The retaining of data is dependent on the existence of those residing within the infrastructure of the Active Directory, e.g., if a user account is deleted within the Active Directory, this initiates a deletion of the user account residing in the Tenant.

APPENDIX
TO EXHIBIT 2

ANNEX I.C TO EXHIBIT 2
- COMPETENT SUPERVISORY AUTHORITY -

Competent supervisory authority in accordance with Clause 13 with regard to data exports where the data exporter is established in

Austria	**Österreichische Datenschutzbehörde** Barichgasse 40 - 42 1030 Wien Austria Phone: + 43 1 52 152-0 E-mail: dsb@dsb.gv.at Homepage: www.dsb.gv.at
Bulgaria	**Commission for Personal Data Protection** 2 Prof. Tsvetan Lazarov Blvd. Sofia 1592 Bulgaria Phone: +359 2/91-53-519 E-mail: kzld@cpdp.bg Homepage: https://www.cpdp.bg
Czech Republic	**The Office for Personal Data Protection** Pplk. Sochora 27 170 00 Praha 7 Czech Republic Phone: +420 234 665 111 E-mail: posta@uoou.cz Homepage: https://www.uoou.cz
France	**Commission nationale de l'informatique et des libertés** 3 Place de Fontenoy TSA 80715 75334 Paris Cedex 07 France Phone: +33 (0)1 53 73 22 22 Homepage: www.cnil.fr/en/home
Germany	**Der Hessische Beauftragte für Datenschutz und Informationsfreiheit** Postfach 3163, 65021 Wiesbaden Gustav-Stresemann-Ring 1, 65189 Wiesbaden Phone: +49 6 11/140 80

	E-mail: poststelle@datenschutz.hessen.de Homepage: https://www.datenschutz.hessen.de
Italy	**Garante per la Protezione dei Dati Personali** Piazza Venezia n. 11 00187 Roma Italy Phone: + 39 06 69 677.1 E-mail: protocollo@gpdp.it PEC-Mail: protocollo@pec.gdp.it Homepage: https://www.garanteprivacy.it
Japan	Personal **Information Protection Commission** Kasumigaseki Common Gate West Tower 32nd Floor 3-2-1, Kasumigaseki Chiyoda-ku Tokyo, 100-0013 Japan Phone: +81-(0)3-6457-9680 Contact: https://www.ppc.go.jp/en/contactus/ Homepage: https://www.ppc.go.jp/en/
Luxembourg	**Commission nationale pour la protection des données** 15, Boulevard du Jazz 4370 Belvaux Luxembourg Phone: + 352 26 10 601 E-mail: info@cnpd.lu Homepage: https://www.cnpd.lu
The Netherlands	**Autoriteit Persoonsgegevens** PO Box 93374 2509 AJ DEN HAAG The Netherlands Phone: + 31-70-88 88 500 Homepage: https://autoriteitpersoonsgegevens.nl/nl
People's Republic of China	**Office of the Central Cyberspace Affairs Commission/Cyberspace Administration of China (中共中央网络安全和信息化委员会办公室/国家互联网信息办公室)** **No.15 Fucheng Road, Haidian District, Beijing** **Phone: 010-55636504** **Homepage: https://www.cac.gov.cn** **National Financial Regulatory Administration, Shanghai Bureau** (国家金融监督管理总局上海监管局) Address: 35#, Hehuan Road, Pudong New District, Shanghai 200135, PRC. Phone: 86 21 38650100 Homepage: 国家金融监督管理总局 (https://www.nfra.gov.cn/cn/view/pages/index/index.html)

	National Financial Regulatory Administration, Beijing Bureau (国家金融监督管理总局北京监管局) Address: B Area, Bank of Communications Tower, 20# Financial Street, Xicheng District, Beijing 100032 Phone: 86 10 66021378 Homepage: 国家金融监督管理总局 (https://www.nfra.gov.cn/cn/view/pages/index/index.html) **People's Bank of China Shanghai Headquarters /Shanghai Branch** (人民银行上海总部/上海分行) Address: 181# Lujiazui East Road, Pudong New District, Shanghai 200120, Phone: 86 21 58845000 Homepage: 上海总部/上海分行(pbc.gov.cn) **People's Bank of China, Beijing Operation Management Department/Beijing Branch** (人民银行北京营业管理部/北京分行) Address: 79 Yuetan South St, Beijing 100045, Phone: 86 10 68559550 Homepage: 营业管理部（北京）/北京分行(pbc.gov.cn)
Poland	**Urząd Ochrony Danych Osobowych (The President of the Office for Personal Data Protection)** ul. Stawki 2 00-193 Warszawa Poland Phone:+48 22 531 03 00 E-mail: kancelaria@uodo.gov.pl
Russia	**Управление Роскомнадзора по Центральному федеральному округу (Roskomnadzor Office for the Central Federal District)** 17997, ГСП-7 , Москва г., ш. Старокаширское, д. 2, к. 10 (17997, GSP-7, Moscow, Starokashirskoe shosse, h. 2, b. 10) Phone: 8 (495)587-44-85 E-mail: rsockanc77@rkn.gov.ru Homepage: https://rkn.gov.ru/personal-data/
Singapore	**The Personal Data Protection Commission** 10 Pasir Panjang Road #03-01 Mapletree Business City Singapore 117438 Phone: +65 6377 3131 Contact: online feedback form Homepage: www.pdpc.gov.sg
Spain	**Agencia Espanola de Protección de Datos (AEPD)** C/Jorge Juan, 6 28001 Madrid Spain Phone: + 34 900 293 183

	Homepage: https://www.agpd.es/
Switzerland	**Federal Data Protection and Information Commissioner** Feldeggweg 1 CH - 3003 Bern Phone: +41 (0)58 462 43 95 Homepage: https://www.edoeb.admin.ch
United Kingdom	**The Information Commissioner's Office** Wycliffe House, Water Lane Wilmslow Cheshire SK9 5AF Great Britain United Kingdom Phone: +44 303 123 1113 E-mail: dpo@ico.org.uk Homepage: https://www.ico.org.uk
United States	**n/a**

APPENDIX
TO EXHIBIT 2

ANNEX II TO EXHIBIT 2
- TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA -

Description of the technical and organizational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

A. General

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

(1a) Measures to **pseudonymize and anonymize** personal data:
• 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 anonymized sufficiently before transfer. The methods of anonymization are decided case-by-case. Any deviations must undergo a standardized exception process.

Explanation:

Pseudonymization 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 organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. An anonymization 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:
• Development of security concepts via a centralized security analysis application of Commerzbank for IT applications that process personal data and for IT infrastructures. • Encryption measures as set forth in the policy of the bank (Information Security Control Framework). Depending on the data classification determined by the centralized security 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 encrypted in accordance with the defined encoding matrix by the cryptographic processes allowed in the bank in accordance with the technical standard. • In case of cloud services, personal data will be encrypted with Commerzbank keys which are under control and the management of Commerzbank.

Explanation:

Encryption of personal data is a common practice to protect such data from disclosure to unauthorized 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 security concepts via a centralized security 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. • In addition, these applications will undergo a standardized process for the Privacy Impact Assessment. • Encryption measures; see Sec. 1 (1b). • The assignment of authorizations to IT application will be done via a standardized 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 unauthorized 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:**
• 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 security concepts via a centralized security 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 centralized/standardized 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 unauthorized or unlawful processing as well as unintentional loss, unintentional destruction or unintentional damages as well as unauthorized 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:**
• Use of fire protection devices (smoke and fire detectors, fire extinguishers, fire doors, fire extinguishing systems) in the computing center 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 center 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 (centralized and decentralized). • Use or 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 centralized 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:**

- Centralized 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 center and server) so as to realize 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 organizational measures:**
• Continuous improvement process in the information security management system (ISMS). • Regular compliance checks for IT systems processing personal data within the scope of the centralized security analysis process of Commerzbank. The results of these checks will be included in existing risk analyses for modification of the security concepts. • Verification of compliance with the conditions on information security by risk-oriented tests (on the basis of the relevant security compliance checks) by a second line of defense. • 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 organizational measures unless stated under Sec. 1

(2a) Measures to **deny unauthorized 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 safeguard the buildings by the general electronic admission control, the entrances to the rooms of the computing centers are partly secured biometrically and by badge readers. • Access to the computing center by individual admission systems. • External individuals will be accompanied by authorized employees in the special protection zones (such as, among others, the computing center, the technology rooms). • Special authorization processes for access to certain special protection zones. • Transparency and the possibility of analyzing admissions.

Explanation:

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

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

(2b) Measures to **prevent unauthorized individuals from using data processing systems** (controlling access to data processing systems):
• Access to Commerzbank systems through a personalized user ID and password. • Administration of authorization systems for use of the Commerzbank systems. • Application and change management for granting or withdrawing access authorizations, 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 encryption 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 unauthorized individuals from using data processing facilities and processes. In this connection, measures are taken to ensure that only individuals with proper authorization 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 unauthorized individuals** (access control by authorization management):
• Use of personal user IDs and passwords. • Authorization management (rights and roles concept). • Granting authorizations to IT applications will be done in accordance with the standardized process according to the principle of minimum rights ("need-to-know"). • Annual check of authorizations or the scope of authorization (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 authorizations. • Logging of user activities in the Commerzbank systems. • Separation between development, test and production environments.

Explanation:

This means measures to ensure that individuals authorized to use the data processing processes have access only to personal data for which they have access authorization. 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 authorization 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 unauthorized 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 encryption 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 authorization 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 ANNEX II to 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.

APPENDIX
TO EXHIBIT 2

ANNEX III TO EXHIBIT 2
- LIST OF SUB-PROCESSORS -

Intentionally left blank as not applicable to the Model Contract C2P

APPENDIX
TO EXHIBIT 2

ANNEX IV 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

France	**With regard to exports of data from France by a data exporter located in France, Clause 4.3 of the Main Body of the DPGA is replaced by the following:** "Commerzbank AG will communicate the above amendments (Clauses 4.1 and 4.2) 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." **FR-1. Employee Social Security Number (NIR) and Health Data – France** 1. **Scope.** This clause applies to the HR Processes described in Annex I.B.6 to Exhibit 2, to the extent they concern employees located in France or HR data for which the French employing entity acts as exporter. 2. **Roles.** For the processing of the French Social Security Number (numéro d'inscription au répertoire des personnes physiques, "NIR") and any **health data** relating to employees in France, the **French employing entity remains the sole controller**. No other Commerzbank Group entity shall act as controller for such categories. 3. **Access to health data.** Access to medical content forming part of occupational health surveillance is restricted to the **Service de Prévention et de Santé au Travail (SPST)** and persons acting under the **occupational physician's** authority. The employer may receive only the outcomes and administrative information permitted by French law, such as dates of medical visits, fitness-for-work opinions, and any job-adaptation proposals issued by the occupational physician. 4. **Access to NIR.** Access to NIR fields is strictly limited to duly authorized personnel of the **French employing entity** for legally permitted HR purposes. No other Commerzbank Group entity or centralized function may access NIR fields. 5. **Hosting model.** Commerzbank Group IT may host systems containing the above data exclusively as processor on behalf of the French employing entity, provided that: a) Access is logically and organizationally restricted so that only the French employing entity's authorized users (and, for occupational health content, only SPST personnel) can view or retrieve the data. b) Data is segregated at tenant, dataset, or field level; encryption at rest and in transit is implemented; and key management is under the control of the French employing entity.

	c) Administrative, support, and remote access by other Commerzbank Group entities or vendors is prevented by default and, where strictly necessary for maintenance, is exceptional, logged, justified, time-bound, and supervised by the French employing entity or the SPST, as applicable. d) If hosting covers health data within the meaning of the French Public Health Code, the external host (if any) must meet the Hébergeur de Données de Santé (HDS) certification requirements. 6. **International transfers.** Cross-border access to the **medical record** content of occupational health surveillance is not permitted. Cross-border access to **NIR** is permitted only where strictly necessary for a purpose authorized by French law and subject to applicable transfer safeguards under the Exhibits. 7. **No re-role.** Nothing in this DPGA creates an independent controller role for any non-French Group entity over NIR or health data relating to employees in France.
Italy	**With regard to exports of data from Italy by a data exporter located in Italy, Clause 4.3 of the Main Body of the DPGA is replaced by the following:** "Commerzbank AG will communicate the above amendments (Clauses 4.1 and 4.2) 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."
Japan	**With regard to exports of data from Japan by a data exporter located in Japan,** **I. clauses 1.2 to 1.6 of the Main Body of the DPGA** shall apply and the Model Contract C2P shall apply (as amended in accordance with section II below) to the extent permissible under data protection laws in Japan if personal data is transferred to a jurisdiction which is a) not subject to an arrangement with Japan (or transitional arrangements under the laws of Japan permitting the transfer of personal data from Japan to the jurisdiction in which the Data Importer is located; or b) not subject to an adequacy decision or similar decision (or transitional arrangement) under the laws of Japan permitting the transfer of personal data to jurisdictions outside of Japan **whereby** **II. the Model Contract C2P (if applicable, including its Appendix) shall be amended as follows:** 1. The term "European Union", "Union", "EU", "EU Member State" or "Member State" " shall be replaced with the term "Japan". 2. The terms

	• "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" • "Regulation (EU) 2016/679" • "Articles 13 and 14 of Regulation (EU) 2016/679" • "Article 23(1) of Regulation (EU) 2016/679" • "Article 45 of Regulation (EU) 2016/679" • "Articles 46 or 47 of Regulation (EU) 2016/679" shall be replaced with the term "**the Applicable Data Protection Laws and Regulations of Japan**". 3. Clause 2 (a) shall be restated as follows: (a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to the Applicable Data Protection Laws and Regulations of Japan. 4. Clause 4 (a) shall be restated as follows: (a) Where these Clauses use terms that are used in the Applicable Data Protection Laws and Regulations of Japan, in particular but not limited to the terms • "sensitive data" (*you hairyo kojin joho*), • "controller" (*kojin joho toriatsukai jigyo sha*), • "data subject" (*honnin*), • "supervisory authority/authority" (*kojin joho hogo iinkai*), unless the context requires otherwise, each term shall have the same meaning as ascribed to the equivalent term (as indicated in parenthesis above)in these laws and regulations. 5. A new paragraph as follows to be added to Clause 8.3 as paragraph (b) (with the existing provision being paragraph (a)): (b) In order to comply with Applicable Data Protection Laws and Regulations of Japan, the data importer shall inform them, either directly or through the data exporter of its identity and contact details and its purpose of use of personal data 6. Clause 8.6 *(Security of Processing)* shall be amended with the following lit. (e): e) The foregoing notwithstanding the Data Importer shall take all reasonable measures to ensure its employees comply with all necessary and appropriate security measures under Applicable Data Protection Laws and Regulations of Japan, 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. 7. Clause 8.8 *(Onward transfers)* shall be restated as follows: 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 Applicable Data Protection Laws and Regulations of Japan, but where uncertain, shall default to obtaining consent for the data transfers from data subjects. 8. A new paragraph as follows to be added to Clause 8.9 as paragraph (f): (f) the data importer shall make the procedures for exercising the data subjects' right under the Applicable Data Protection Laws and Regulations of Japan available to the data subjects. 9. Clause 11 (c)(i), Clause 11 (d) and Clause 11 (e) shall be restated as follows: (c)(i) lodge a complaint with the supervisory authority or any other competent authority in Japan pursuant to Clause 13; (d) The parties accept that the data subject may be represented by a not-for-profit body, organization or association under the conditions set out under the Applicable Data Protection Laws and Regulations of Japan, if any. (e) The data importer shall abide by a decision that is binding under the Applicable Data Protection Laws and Regulations of Japan. 10. Clause 13 (a) shall be restated as follows: (a) The Personal Information Protection Commission shall act as competent supervisory authority. 11. Clause 16 (e) shall be deleted in its entirety.
People's Republic of China ("**PRC**" - which, when referring to jurisdiction, does not include Hong Kong, Macau and Taiwan)	**With regard to exports of data from the PRC by a data exporter located in the PRC, (i) the data protection agreements based on the Standard Contract for Outbound Transfer of Personal Information of the Cyberspace Administration of China entered into by Commerzbank AG with Commerzbank AG, Beijing Branch, and Commerzbank AG, Shanghai Branch, apply, and (ii) the following amendments shall be made to the DPGA, including:** **I. Clause 1.5 of the Main Body of the DPGA** shall be replaced with the following: In the event of inconsistencies between the provisions of this DPGA and any other standard agreement in a form formulated by the competent authority in the PRC (i.e. the Cyberspace Administration of China) between the Parties in relation to the subject-matters addressed herein (the "China Standard Contract"), the provisions of the China

	Standard Contract shall prevail as it relates to the Parties' data protection obligations in connection with data transfers. **II. Exhibit 2 (if applicable, including its Appendix) shall be amended as follows:** 1. The terms • "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" • "Regulation (EU) 2016/679" • "Articles 13 and 14 of Regulation (EU) 2016/679" • "Article 23(1) of Regulation (EU) 2016/679" • "Article 28(7) of Regulation (EU) 2016/679" • "Article 45 of Regulation (EU) 2016/679" • "Article 45(3) of Regulation (EU) 2016/679" • "Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679" • "Articles 46 or 47 of Regulation (EU) 2016/679" • "Article 80 (1) of Regulation (EU) 2016/679 shall be replaced with the term "the **Applicable Data Protection Laws and Regulations of the PRC**". **"Applicable Data Protection Laws and Regulations of the PRC"** means all laws, administrative regulations, judicial interpretations, regulatory rules and other binding normative documents of the People's Republic of China (for these purposes, excluding the Hong Kong Special Administrative Region, the Macao Special Administrative Region and Taiwan) that relate to the protection of personal information, data security, cybersecurity or cross-border data transfer, in each case, as amended, replaced or supplemented from time to time, including without limitation: (a) the Personal Information Protection Law of the PRC; (b) the Cybersecurity Law of the PRC; (c) the Data Security Law of the PRC; (d) any such implementing regulations, measures, rules and guidelines issued by any competent PRC authority (including the Cyberspace Administration of China and other relevant regulators) in connection with the laws mentioned in (a) to (c); and (e) any other applicable PRC laws and regulations governing the collection, storage, use, processing, transmission, disclosure, security or cross-border transfer of personal information or other data. 2. The term "sensitive data" shall be replaced with the term "sensitive personal data". 3. Clause 2 (a) shall be restated as follows: (a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to the Applicable Data Protection Laws and Regulations of the PRC.

	4. Clause 4 (a) shall be restated as follows: (a) Where these Clauses use terms that are used in the Applicable Data Protection Laws and Regulations of the PRC, unless the context requires otherwise, each term shall have the same meaning as ascribed to it in these laws and regulations. The foregoing notwithstanding the term "supervisory authority" shall mean the competent data protection authority in the PRC. 5. Clause 8.7 *(Sensitive data)* shall be amended with the following sentence 2: The data exporter warrants that 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 6. Clause 8.8 *(Onward transfers)* shall be restated as follows: The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the PRC (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if: (i) the onward transfer is to a country benefitting from a decision of the competent body under the Applicable Data Protection Laws and Regulations of the PRC finding that the third country provides adequate protection; (ii) the third party otherwise ensures appropriate safeguards with respect to the processing in question satisfactory under the Applicable Data Protection Laws and Regulations of the PRC; (iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings, or (iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person. Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses and the Applicable Data Protection Laws and Regulations of the PRC, in particular purpose limitation. 7. Clause 11 (c)(i), Clause 11 (d) and Clause 11 (e) shall be restated as follows: (c)(i) lodge a complaint with the competent supervisory authority; (d) The parties accept that the data subject may be represented by a not-for-profit body, organization or association under the conditions set out under the Applicable Data Protection Laws and Regulations of the PRC, if any.

	(e) The data importer shall abide by a decision that is binding under the Applicable Data Protection Laws and Regulations of the PRC. 8. Clause 15.2 (a) shall be restated as follows: The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under or in violation of the laws and regulations of the country of destination or the PRC, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e). 9. Clause 16 (e) shall be deleted in its entirety. 10. Clause 17 shall be restated as follows: These Clauses shall be governed by the laws of the PRC. 11. Clause 18 shall be restated as follows: (a) Any dispute arising from these Clauses shall be resolved by the Courts of the PRC. (b) The Parties agree to submit themselves to the jurisdiction of such courts.
Russia	**With regard to exports of data from Russia by a data exporter located in Russia,** **I. Exhibit 2 (if applicable, including its Appendix) shall be amended as follows:** 1. The term "Community" shall be replaced with the term "Russia". 2. The terms • "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" • "Regulation (EU) 2016/679" • "Articles 13 and 14 of Regulation (EU) 2016/679" • "Article 23(1) of Regulation (EU) 2016/679" • "Article 28(7) of Regulation (EU) 2016/679" • "Article 45 of Regulation (EU) 2016/679" • "Article 45(3) of Regulation (EU) 2016/679" • "Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679"

	• "Articles 46 or 47 of Regulation (EU) 2016/679" • "Article 80 (1) of Regulation (EU) 2016/679" shall be replaced with the term "the **Applicable Data Protection Laws and Regulations of Russia**" (including but not limited to Federal law "On personal data" # 152-FZ dated 27.07.2006 (hereinafter referred to as "PD Law"). 3. Clause 2 (a) shall be restated as follows: (a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to the Applicable Data Protection Laws and Regulations of Russia. 4. Clause 4 (a) shall be restated as follows: (a) Where these Clauses use terms that are used in the Applicable Data Protection Laws and Regulations of Russia, unless the context requires otherwise, each term shall have the same meaning as ascribed to it in these laws and regulations. In the absence of the term in the Applicable Data Protection Laws and Regulations of Russia the closest meaning is applied. 5. Clause 8.6 (a) shall be amended with the following sentence 7: The foregoing notwithstanding the Data Importer (i) 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 Applicable Data Protection Laws and Regulations of Russia, in particular under Articles 18.1, 19 of the PD 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; (ii) 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. 6. Clause 8.6 (b) shall be amended with the following sentence 3: Notwithstanding anything to the contrary in these Clauses 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 PD Law. 7. Clause 8.8 *(Onward transfers)* shall be restated as follows: The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside Russia (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if: (i) the onward transfer is to a country benefitting from a decision of the competent body under the applicable Laws and regulations of Russia finding that the third country provides adequate protection; (ii) the third party otherwise ensures appropriate safeguards with respect to the processing in question satisfactory under the Applicable Data Protection Laws and Regulations of Russia; (iii) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person. Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation. 8. Clause 11 (c) (i), Clause 11 (d) and Clause 11 (e) shall be restated as follows: (c)(i) lodge a complaint with the supervisory authority, or the competent authority pursuant to Clause 13; d) The parties accept that the data subject may be represented by a not-for-profit body, organization or association under the conditions set out under the Applicable Data Protection Laws and Regulations of Russia, if any. (e) The data importer shall abide by a decision that is binding under the Applicable Data Protection Laws and Regulations of Russia. 9. Clause 16 (e) shall be deleted in its entirety. 10. Clause 17 shall be restated as follows: These Clauses shall be governed by the laws of Russia. 11. Clause 18 shall be restated as follows: (a) Any dispute arising from these Clauses shall be resolved by the Courts of Russia. (b) The Parties agree to submit themselves to the jurisdiction of such courts.

	II. Annex I.B.1 to Annex I.B.5 to Exhibit 2 shall be amended with the following sentence 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, whether with or without means of automation.
Singapore	**With regard to exports of data from Singapore by a data exporter located in Singapore,** **I. Exhibit 2 (if applicable, including its Appendix) shall be amended as follows:** 1. The terms • "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" • "Regulation (EU) 2016/679" • "Articles 13 and 14 of Regulation (EU) 2016/679" • "Article 23(1) of Regulation (EU) 2016/679" • "Article 28(7) of Regulation (EU) 2016/679" • "Article 45 of Regulation (EU) 2016/679" • "Article 45(3) of Regulation (EU) 2016/679" • "Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679" • "Articles 46 or 47 of Regulation (EU) 2016/679" • "Article 80 (1) of Regulation (EU) 2016/679 shall be replaced with the term "**the Applicable Data Protection Laws and Regulations of Singapore**" which, as used herein, shall be interpreted as meaning any law and regulation of Singapore that is applicable to the parties in their access and use of personal data, including (but not necessarily limited to) the Personal Data Protection Act 2012 and all related regulations, codes of practice and guidelines published by a Regulator relating to personal information.. 2. Clause 2 (a) shall be restated as follows: (a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to the Applicable Data Protection Laws and Regulations of Singapore. 3. Clause 4 (a) shall be restated as follows: (a) Where these Clauses use terms that are used in the Applicable Data Protection Laws and Regulations Singapore in particular but not limited to , • Personal data

	• Process/processing unless the context requires otherwise, each term shall have the same meaning as ascribed to it in these laws and regulations. The foregoing notwithstanding the term “supervisory authority/authority" shall have the meaning given to the term "Commission" in Singapore’s Personal Data Protection Act including all subsidiary regulation enacted thereunder, whether now or in the future. 4. Clause 8.5 (*Duration of processing and erasure or return of data*) shall be restated as follows: The data importer shall only conduct processing of personal data for the duration specified in Annex I.B and, in any event, shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a). 5. Clause 8.6 (a) shall be restated as follows: The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against (i) a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data and (ii) the loss of any storage medium or decide on which personal data is stored (hereinafter ‘personal data breach’). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security. 6. Clause 8.8 *(Onward transfers)* shall be restated as follows:

	The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside Singapore (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the data exporter has consented to the onward transfer and such third party is or agrees to be bound by these Clauses, under the appropriate Module, or if such third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses and, in any event, as is required by the Applicable Data Protection Laws and Regulations of Singapore, and the data importer provides a copy of these safeguards to the data exporter. Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation. 7. Clause 11 (c) (i), Clause 11 (d) and Clause 11 (e) shall be restated as follows: (c)(i) lodge a complaint with the Commission, or any other competent authority in Singapore pursuant to Clause 13; d) The parties accept that the data subject may be represented by a not-for-profit body, organization or association under the conditions set out under the Applicable Data Protection Laws and Regulations of Singapore, if any. (e) The data importer shall abide by a decision that is binding under any applicable law of Singapore . 8. Clause 13 (a) shall be restated as follows: (a) The Commission shall act as competent supervisory authority. 9. Clause 16 (e) shall be deleted in its entirety. 10. Clause 17 shall be restated as follows: These Clauses shall be governed by the laws of Singapore. 11. Clause 18 shall be restated as follows: (a) Any dispute arising from these Clauses shall be resolved by the Courts of Singapore. (b) The Parties agree to submit themselves to the jurisdiction of such courts. **and** **II. Clause 1.5 of this DPGA notwithstanding,** 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.
Spain	**With regard to exports of data from Spain by a data exporter located in Spain, Clause 4.3 of the Main Body of the DPGA is replaced by the following:** "Commerzbank AG will communicate the above amendments (Clauses 4.1 and 4.2) 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."
Switzerland	**With regard to exports of data from Switzerland by a data exporter located in Switzerland,** I. **clauses 1.2 to 1.6 of the Main Body of the DPGA** shall apply and the Model Contract C2P shall apply (as amended in accordance with section II below) to the extent permissible under data protection laws in Switzerland if personal data is transferred to a jurisdiction which is a) not subject to an arrangement with Switzerland (or transitional arrangements under the laws of Switzerland) permitting the transfer of personal data from Switzerland to the jurisdiction in which the Data Importer is located; or **b)** not subject to an adequacy decision or similar decision (or transitional arrangement) under the laws of Switzerland permitting the transfer of personal data to jurisdictions outside of Switzerland **whereby** **II. the Model Contract C2P (if applicable, including its Appendix) shall be amended as follows:** 1. The term "European Union", "Union", "EU", "EU Member State" or "Member State" shall be replaced with the term "Switzerland". 2. The terms • "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" • "Regulation (EU) 2016/679" • "Articles 13 and 14 of Regulation (EU) 2016/679" • "Article 23(1) of Regulation (EU) 2016/679" • "Article 28(7) of Regulation (EU) 2016/679" • "Article 45 of Regulation (EU) 2016/679" • "Article 45(3) of Regulation (EU) 2016/679" • "Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679"

	• "Articles 46 or 47 of Regulation (EU) 2016/679" • "Article 80 (1) of Regulation (EU) 2016/679 shall be replaced with the term "the **Applicable Data Protection Laws and Regulations of Switzerland**". 3. Clause 2 (a) shall be restated as follows: (a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to the applicable Data Protection Laws and Regulations of Switzerland. 4. Clause 4 (a) shall be restated as follows: (a) Where these Clauses use terms that are used in the Applicable Data Protection Laws and Regulations of Switzerland, unless the context requires otherwise, each term shall have the same meaning as ascribed to it in these laws and regulations. The foregoing notwithstanding the Term "supervisory authority" shall mean the competent data protection authority of Switzerland. 5. Clause 8.8 *(Onward transfers)* shall be restated as follows: The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside Switzerland (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if: (i) the onward transfer is to a country benefitting from a decision of the competent body under the applicable Laws and regulations of Switzerland finding that the third country provides adequate protection; (ii) the third party otherwise ensures appropriate safeguards with respect to the processing in question satisfactory under the Applicable Data Protection Laws and Regulations of Switzerland; (iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings, or (iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person. Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation. 6. Clause 11 (c)(i), Clause 11 (d) and Clause 11 (e) shall be restated as follows: (c)(i) lodge a complaint with the supervisory authority, or the competent authority pursuant to Clause 13;

	(d) The parties accept that the data subject may be represented by a not-for-profit body, organization or association under the conditions set out under the Applicable Data Protection Laws and Regulations of Switzerland, if any. (e) The data importer shall abide by a decision that is binding under the applicable Data Protection Laws and Regulations of Switzerland. 7. The "supervisory authority" pursuant to Clause 13 shall be the Swiss Federal Data Protection and Information Commissioner. 8. Clause 16 (e) shall be deleted in its entirety. 9. Clause 17 shall be restated as follows: These Clauses shall be governed by the laws of Switzerland. 10. Clause 18 shall be restated as follows: (a) Any dispute arising from these Clauses shall be resolved by the Courts of the city of Zurich, Switzerland. (b) The Parties agree to submit themselves to the jurisdiction of such courts.
United Kingdom	If the Data Exporter of a particular transfer/category of transfers of personal data is located in the UK, the "International Data Transfer Addendum to the EU Commission Standard Contractual Clauses" (ANNEX V TO EXHIBIT 1) applies**.**
United States	**With regard to exports of data from the United States by a data exporter located in the United States,** **I. Exhibit 2 (if applicable, including its Appendix) shall be amended as follows:** 1. The terms • "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" • "Regulation (EU) 2016/679" • "Articles 13 and 14 of Regulation (EU) 2016/679" • "Article 23(1) of Regulation (EU) 2016/679" • "Article 28(7) of Regulation (EU) 2016/679" • "Article 45 of Regulation (EU) 2016/679" • "Article 45(3) of Regulation (EU) 2016/679" • "Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679" • "Articles 46 or 47 of Regulation (EU) 2016/679" • "Article 80 (1) of Regulation (EU) 2016/679

	shall be replaced with the term "**the Applicable Data Protection Laws and Regulations of the United States**". 2. The terms "competent supervisory authority" and "supervisory authority" shall both be replaced with the term "appropriate regulatory authorities"; 3. Clause 16(c) shall be restated as follows: (c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where: (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension; (ii) the data importer is in substantial or persistent breach of these Clauses; or (iii) the data importer fails to comply with a binding decision of a competent court or appropriate regulatory authority regarding its obligations under these Clauses. In these cases, in accordance with the Applicable Data Protection Laws and Regulations of the United States, it shall inform the appropriate regulatory authorities of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

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.

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.

I. COMMERZBANK AG ENTITIES (INCLUDING BRANCH OFFICES) IN THE EU/EEA, SWITZERLAND OR UK

#	*Name, legal form and address Data Exporter / Data Importer*	*Signature 1*	*Signature 2*
1.	Commerzbank AG Vienna Branch Hietzinger Kai 101 – 105 1130 Wien, Austria Data Exporter ☒ Data Importer ☒	Date and Signature	Date and Signature

#	*Name, legal form and address* *Data Exporter / Data Importer*	*Signature 1*	*Signature 2*
3.	Digital Technology Center Commerzbank AG Sofia Branch, Bulgaria, Sofia, district Mladost, zh.k. Mladost 4, 1715, str. Samara 2, Advance Business Center II, 3rd floor Data Exporter ☐ Data Importer ☒	Date and Signature	Date and Signature

#	*Name, legal form and address* *Data Exporter / Data Importer*	*Signature 1*	*Signature 2*
4.	Commerzbank AG acting through COMMERZBANK Aktiengesellschaft, Pobočka Praha Prague Branch Jugoslávská 1 120 21 Praha 2, Czech Republic Data Exporter ☒ / Data Importer ☒	Date and Signature	Date and Signature

#	*Name, legal form and address* *Data Exporter / Data Importer*	*Signature 1*	*Signature 2*
5.	Commerzbank AG Paris Branch 86 Boulevard Haussmann 75008 Paris France Data Exporter: ☒ Data Importer: ☒	Date and Signature	Date and Signature

#	*Name, legal form and address* *Data Exporter / Data Importer*	*Signature 1*	*Signature 2*
6.	Commerzbank AG Kaiserstraße 16 (Kaiserplatz) 60311 Frankfurt/Main Germany Data Exporter ☒ / Data Importer ☒	Date and Signature	Date and Signature

#	*Name, legal form and address* *Data Exporter / Data Importer*	*Signature 1*	*Signature 2*
7.	Commerzbank AG Milan Branch Corso Europa 2 20122 Milan, Italy Data Exporter ☒ / Data Importer ☒	Date and Signature	Date and Signature

#	*Name, legal form and address* *Data Exporter / Data Importer*	*Signature 1*	*Signature 2*
9.	Commerzbank Finance & Covered Bond S.A. 5 rue Jean MonnetL-2180 Luxembourg Grand Duchy of Luxembourg Data Exporter: ☒ Data Importer: ☒	Date and Signature	Date and Signature

#	*Name, legal form and address* *Data Exporter / Data Importer*	*Signature 1*	*Signature 2*
10.	Commerzbank AG Benelux Branch Claude Debussylaan 24 (10th Floor) 1082 MD Amsterdam The Netherlands Data Exporter ☒ Data Importer ☒	Date and Signature	Date and Signature

#	*Name, legal form and address* *Data Exporter / Data Importer*	*Signature 1*	*Signature 2*
12.	mBank SA ul. Prosta 18 00-850 Warszawa Poland Data Exporter ☒ / Data Importer ☒	Date and Signature	Date and Signature

#	*Name, legal form and address* *Data Exporter / Data Importer*	*Signature 1*	*Signature 2*
13.	CERI International Sp. Z o.o. ul. Wersalska 6 91-203 Łódź Poland Data Exporter: ☐ Data Importer: ☒	Date and Signature	Date and Signature

#	*Name, legal form and address* *Data Exporter / Data Importer*	*Signature 1*	*Signature 2*
14.	Commerzbank AG Madrid Branch Torre de Cristal, Paseo de la Castellana 259 C 28046 Madrid Spain Data Exporter ☒ / Data Importer ☒	Date and Signature	Date and Signature

#	*Name, legal form and address Data Exporter / Data Importer*	*Signature 1*	*Signature 2*
15.	Commerzbank AG Filiale Zürich Pelikanplatz 15 8001 Zürich Switzerland Data Exporter ☒ / Data Importer ☒	Date and Signature	Date and Signature

#	*Name, legal form and address* *Data Exporter / Data Importer*	*Signature 1*	*Signature 2*
16.	Commerzbank AG London Branch 30 Gresham Street London EC2V 7PG United Kingdom Data Exporter ☒ Data Importer ☒	Date and Signature	Date and Signature

II. COMMERZBANK AG ENTITIES (INCLUDING BRANCH OFFICES) OUTSIDE THE EU/EEA, SWITZERLAND OR UK

#	*Name, legal form and address Data Exporter / Data Importer*	*Signature 1*	*Signature 2*
1.	Commerzbank AG Beijing Branch Suite 2502 East Tower, Twin Towers B-12 Jianguomenwai Dajie Chaoyang District Beijing 100022 People's Republic of China Data Exporter ☒ Data Importer ☒	Date and Signature	Date and Signature
2.	Commerzbank AG Shanghai Branch 37F, Shanghai World Financial Center 100 Century Avenue 200120 Shanghai People's Republic of China Data Exporter ☒ Data Importer ☒	Date and Signature	Date and Signature

#	*Name, legal form and address Data Exporter / Data Importer*	*Signature 1*	*Signature 2*

#	*Name, legal form and address* *Data Exporter / Data Importer*	*Signature 1*	*Signature 2*
4.	Commerzbank AG Tokyo Branch Toranomon Hills Station Tower 9F2-6-1 Toranomon, Minato-ku, Tokyo 105-5509, Japan Data Exporter ☒ Data Importer ☒	Date and Signature	Date and Signature

#	*Name, legal form and address* *Data Exporter / Data Importer*	*Signature 1*	*Signature 2*
5.	Commerzbank (Eurasija) AO 14/2 Kadashevskaya Nab. 119017 Moscow Russia Data Exporter ☒ Data Importer ☒	Date and Signature	Date and Signature

#	*Name, legal form and address* *Data Exporter / Data Importer*	*Signature 1*	*Signature 2*
6.	Commerzbank AG Singapore Branch 128 Beach Road #17-01 Guoco Midtown, Singapore 189773 Data Exporter ☒ / Data Importer ☒	Date and Signature	Date and Signature

#	*Name, legal form and address* *Data Exporter / Data Importer*	*Signature 1*	*Signature 2*
7.	Commerzbank AG New York Branch 225 Liberty Street New York, NY 10281-1050 USA Data Exporter ☒ Data Importer ☒	Date and Signature	Date and Signature

#	*Name, legal form and address* *Data Exporter / Data Importer*	*Signature 1*	*Signature 2*
8.	Commerz Markets LLC 225 Liberty Street New York, NY 10281-1050 USA Data Exporter: ☒ Data Importer: ☒	Date and Signature	Date and Signature