

Guarantee Agreement regarding certain transfers of personal data to Commerzbank AG (London)

of Commerzbank AG (including its branches in EU and Switzerland other than London branch) and
Commerzbank AG London Branch

Preamble

Commerzbank AG, headquartered in Frankfurt am Main, is an internationally active business bank, represented in various European countries with branch offices, including also in London, United Kingdom (Commerzbank AG (London), "Commerzbank AG London Branch").

On 29 March 2017, the Government of the United Kingdom (UK) invoked Article 50 of the Treaty on European Union (EU). As a result, the UK is due to leave the EU on 29 March 2019 when the period for negotiating an agreement for the withdrawal from the European Union ends (unless an extension is agreed).

In case the UK leaves the EU and there is no adequacy decision by the European Commission for the UK under Art. 45 of the General Data Protection Regulation (EU) 2016/679 ("GDPR") or other legal basis recognized by the authorities (see for example (COM(2018) 880final), under Art. 46 GDPR a controller may transfer personal data to a third country or an international organisation if the controller or processor has provided appropriate safeguards in accordance with Art. 46 GDPR.

According Art. 46(5) sentence 2 GDPR, decisions adopted by the European Commission on the basis of Article 26(4) of Directive 95/46/EC shall remain in force until amended, replaced or repealed, if necessary, by a Commission Decision adopted in accordance with paragraph 2 of Article 46.

Accordingly, the Standard Contractual Clauses (Processors) according to commission decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (notified under document C(2010) 593) remain applicable until amended, replace or repealed.

The Standard Contractual Clauses are usually agreed by the conclusion of an agreement between the party transferring and the party receiving the data. In the case of a transfer between a company and its legally dependent branch, data protection authorities have taken the view that a unilateral declaration, to be made available to the affected persons (data subjects), through which an agreement with the data subjects can be established, shall be used (see e.g. no. 11.2 of the 19th report of the state government regarding the activities of the supervisory authorities responsible for data protection in the non-public sector in Hesse (Germany), LT-Drs. 16/5892). This is the purpose of this document.

In light of the above, the following is declared and agreed by Commerzbank AG London Branch and Commerzbank AG regarding transfers of personal data as described in Annex A to this document to Commerzbank AG London Branch, provided that the UK leaves the EU and there is no adequacy decision by the European Commission for the UK under Art. 45 of the General Data Protection Regulation (EU) 2016/679 ("GDPR") (respectively for Switzerland no adequacy decision by the EDÜB) or another other legal basis for the transfer of personal data to the UK recognized by the authorities:

1. Commerzbank AG London Branch and Commerzbank AG make reference to the Standard Contractual Clauses (Processors), as attached to this document as Annex A (including its Appendices) regarding transfers of personal data from Commerzbank AG (including Commerzbank AG's branch offices in the EU and Switzerland as referred to in Appendix 3, as may be updated from time to time to include newly established branch offices or remove closed branch offices) to Commerzbank AG London Branch as described in Annex A.

COMMERZBANK

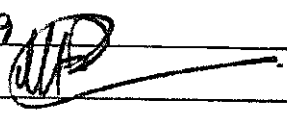

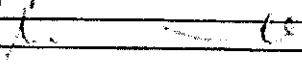
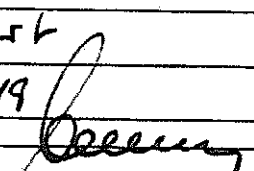
2. Commerzbank AG London Branch and Commerzbank AG declare and agree (subject to termination by them, that may in particular occur in case that the described processing activities end or that another legal basis for the transfer to a third country applies) that the data transfers carried out by Commerzbank AG (including Commerzbank AG's EU and Switzerland branch offices as described in Appendix 3), as data exporter, to Commerzbank AG London Branch, as data importer, as described in Appendix 1 of Annex A, and the subsequent data processing by the data importer, as described in Appendix 1 of Annex A, shall be carried out in compliance with the provisions of the Standard Contractual Clauses (Processors), as attached hereto in Annex A. This shall have third party effect, i.e. declared for the benefit of the data subjects listed in Appendix 1.

3. This agreement shall be governed and construed by the law of the country in which the data exporter is established.

4. Existing agreements with the data subjects (if any) will remain unaffected.

5. Should any of the provisions be ineffective, this shall not affect the effectiveness of the rest of the agreement. Commerzbank AG London Branch and Commerzbank AG will conduct best efforts in good faith towards a replacement of the ineffective provision by an effective provision that comes as close as possible to the intended purpose of this document.

Signatures:

Commerzbank AG London Branch	Commerzbank AG
Name: Michael Brunke	Name: Jan-Philipp Gillschew
Place: London	Place: Frankfurt
Date: 28.2.19	Date: 05.3.19
Signature: 	Signature: 
Name: Simon J. ...	Name: Roland Wolf
Place: London	Place: Frankfurt
Date: 1/2/19	Date: 12/3/19
Signature: 	Signature: 

ANNEX A

STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

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

Name of the data exporting organisation: **Commerzbank AG** (including Commerzbank AG's EU and Switzerland branch offices)

Address:

Tel.: Fax E-Mail:

Other information needed to identify the organisation:

Commerzbank AG's branch offices in EU and Switzerland include those as referred to in Appendix 3 (the data **exporter**)

And

Name of the data importing organisation: **Commerzbank AG London Branch**

Address: **30 Gresham Street, London EC2P 2XY, Great Britain**

Tel.: **+44 20 762 38000** Fax E-Mail:

Other information needed to identify the organisation:

.....

(the data **importer**)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data¹;

b) 'the data exporter' means the controller who transfers the personal data;

¹ Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

- c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
- d) 'the subprocessor' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
- e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
- f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

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

Clause 3

Third-party beneficiary clause

- (1) The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
- (2) The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
- (3) The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
- (4) The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

- a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
- b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
- c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
- d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
- e) that it will ensure compliance with the security measures;
- f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
- g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
- h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
- i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
- j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer²

The data importer agrees and warrants:

- a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
- d) that it will promptly notify the data exporter about
 - i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
 - ii) any accidental or unauthorised access, and
 - iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
- e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
- f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
- g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
- h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

² Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

- i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;
- j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

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

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

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

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

Clause 7

Mediation and jurisdiction

(1) The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

- a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
- b) to refer the dispute to the courts in the Member State in which the data exporter is established.

(2) The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8**Cooperation with supervisory authorities**

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

Clause 9**Governing Law**

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

Clause 10**Variation of the contract**

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

Clause 11**Subprocessing**

- (1) The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses³. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
- (2) The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

³ This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.

(3) The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

(4) The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

(1) The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

(2) The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

COMMERZBANK

On behalf of the data exporter:

Roland Wolf

Name (written out in full): JAN: KUNIG (GEMAN)

Position:

Address: Kaiserplatz, 60261 Frankfurt/Main

Other information necessary in order for the contract to be binding (if any):

Commerzbank AG
Kaiserplatz
60261 Frankfurt/Main

(stamp of organisation)

Signature [Signature]

On behalf of the data importer:

Name (written out in full): MICHAEL BRUNKE

Position: DATA PROTECTION OFFICER

Address: 30 GRESHAM STREET LONDON EC2V 7PG

Other information necessary in order for the contract to be binding (if any):

Commerzbank AG London Branch
30 Gresham Street
London
EC2V 7PG

(stamp of organisation)

Signature [Signature]

Appendix 1

to the Standard Contractual Clauses

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

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

Financial institute, doing financial transactions for customers.as well as coordinating employees within all countries of Europe.

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

Financial institute, doing financial transactions for customers.

Data subjects

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

Customers, potential customers, subjects with power of attorney, beneficial owners, suppliers, employees, service providers.

Categories of data

The personal data transferred concern the following categories of data (please specify):

Personal master data, contract data, payment behaviour data, application data, income and credit standing data, bank account and payment data, communication data.

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

Health data of employees.

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

Account management, lending business, customer support, transaction settlement, asset management, documentary foreign business, marketing, suppliers processing, building and plant safety.

DATA EXPORTER

Name:

COMMERZBANK

DATA EXPORTER

Name: *ROLAND WOLF* Roland Wolf

Authorised Signature: *[Signature]* *[Signature]*

DATA IMPORTER

Name: *MICHAEL BRUNKE*

Authorised Signature: *[Signature]*

Appendix 2

to the Standard Contractual Clauses

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

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, this Annex specifies the technical and organisational measures under Article 32 of the EU General Data Protection Regulations ("GDPR") resulting from the data processing described in detail in the above-mentioned contract so as to guarantee a level of data protection commensurate with the risk.

The Annex is applicable to all activities where employees of the contract data processor (processor) or sub-processors hired by the processor might come in contact with personal or other data of the controller.

Moreover, the Annex designates sub-processors whose services in connection with the agreed assignment have already been approved when the agreement is signed and the data protection officer or the individual responsible for data protection.

Pursuant to Article 5 (2) and Article 28 (3h) of the GDPR, the controller is responsible for examining the reliability of the processor regarding the technical and organisational measures taken both when the assignment is placed and then at regular intervals.

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

(1a) Measures to pseudonymise and anonymise 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 anonymised sufficiently before transfer. The methods of anonymisation are decided case-by-case. Any deviations must undergo a standardised exception process.

Explanation:

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

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

(1b) Measures to encrypt personal data:

- Development of safety concepts via a centralised safety analysis application of Commerzbank for IT applications that process personal data and for IT infrastructures.
- Encoding measures as set forth in the policy of the bank (Information Security Control Framework). Depending on the data classification determined by the centralised safety analysis application of Commerzbank (confidentiality level of the data) of the IT applications and the type of processing (such as storing, transmitting), the data shall be encoded in accordance with the defined encoding matrix by the cryptographic processes allowed in the bank in accordance with the technical standard.

Explanation:

Encryption personal data is a common practice to protect such data from disclosure to unauthorised individuals. An existing documentation (e.g. in a data protection or security concept) can also be indicated.

(1c) Measures to ensure ongoing confidentiality:

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

Explanation:

This means measures ensuring adequate security of the personal data including protection against unauthorised or 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 safety concepts via a centralised safety analysis application of Commerzbank for IT applications that process personal data and for IT infrastructures.
- Conditions applicable to the development of software for the IT system for input validation.
- Any changes to software, hardware and other IT infrastructure used in production shall be made in accordance with a centralised/standardised Change Management Process.
- Security Logging and Monitoring shall be carried out in accordance with the method of Security Information and Event Management (SIEM) within the framework of operating a Security Operation Centre (SOC).
- Measures regarding input control; see Sec. 2 (2e).
- Measures regarding transfer control; see Sec. 2 (2d).

Explanation:

This means measures ensuring adequate security of the personal data including protection against unauthorised or unlawful processing as well as unintentional loss, unintentional destruction or unintentional damages as well as unauthorised changes. These measures must be designed to ensure ongoing integrity.
An existing documentation (e.g. in a data protection or security concept) can also be indicated.

(1e) Measures to ensure ongoing availability:

- Use of fire protection devices (smoke and fire detectors, fire extinguishers, fire doors, fire extinguishing systems) in the computing centre and the IT technology rooms.
- Use of a system to detect a break in.
- Use of the failsafe electricity supply (FES).
- Air conditioning in the computing centre and the IT technology rooms.
- System detecting damages caused by water.
- Data backup and data export (redundant data management).
- Threat and risk analysis per application with preventive measures.
- Use of backup processes.
- Use of antivirus systems (centralised and decentralised).
- Use of SPAM and content filters.
- Having an emergency, work-around and restart concept in place.
- Training, instructions, and annual exercises.
- Monitoring the availability of infrastructure components and application/databases through the system in accordance with the criticality of the data to be processed.
- Possible production failures will be documented, processed and, if necessary, escalated by a centralised incident/problem management process.

Explanation:

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

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

(1f) Measures to ensure ongoing resilience of the systems and services:

- Centralised capacity management (load balancing; for important applications, key performance indicators will be defined and monitored).
- Conducting penetration tests for web applications.

Explanation:

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

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

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

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

Explanation:

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

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

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

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

Explanation:

Measures especially designed to keep the measures for data security described here up to date.
An existing documentation (e.g. in a data protection or security concept) can also be indicated.

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

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

- Classification of the buildings/areas in different safety and protection zones.
- Using a system to detect break in.
- Camera surveillance of the grounds and entrance areas.
- The buildings of Commerzbank AG have electronic admission systems. These systems permit employees free access to the building during the regular working hours. Extraordinary assignments and associated admission to the buildings need to be applied for separately.
- Visitors, suppliers and other third parties must first register with reception. Their presence will be recorded in writing. Any visitors' passes must be worn openly and returned when leaving the building.
- In addition to safeguarding the buildings by the general electronic admission control, the entrances to the rooms of the computing centres are partly secured biometrically and by badge readers.
- Access to the computing centre by individual admission systems.
- External individuals will be accompanied by authorised employees in the special protection zones (such as, among others, the computing centre, the technology rooms).
- Special authorisation processes for access to certain special protection zones.
- Transparency and the possibility of analysing admissions.

Explanation:

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

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

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

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

Explanation:

This means measures preventing unauthorised individuals from using data processing facilities and processes. In this connection, measures are taken to ensure that only individuals with proper authorisation have access to the data processing facilities. These include, for example, suitable password rules and firewall configurations. An existing documentation (e.g. in a data protection or security concept) can also be indicated.

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

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

Explanation:

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

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

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

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

Explanation:

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

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

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

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

Explanation:

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

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

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

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

Explanation:

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

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

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

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

Explanation:

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

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

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

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

Explanation:

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

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

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

Sec. 3 Data protection officer or individual responsible for observing data protection regulations

First name, last name:	Contact details:
Michael Brunker	Commerzbank AG London Branch 30 Gresham Street London EC2V 7PG United Kingdom +44 20 7475 1243

Sec. 4 List of other approved contract data processors (sub processors)

Short job description:	Company name:	Company domicile, data processing site:	Data protection officer / individual responsible for data protection (First name, last name, contact details):
Business process processing	Various depending on the facts of the order processing. Can be requested.		
Hosting of IT systems	Various depending on the facts of the order processing. Can be requested.		
Disposal services	Various depending on the facts of the order processing. Can be requested.		
Call Center	Various depending on the facts of the order processing. Can be requested.		
Security services	Various depending on the facts of the order processing. Can be requested.		

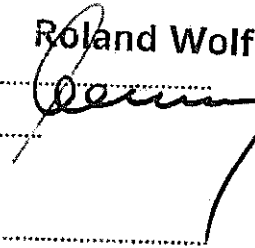
COMMERZBANK

DATA EXPORTER

Name:

Roland Wolf

Authorised Signature:



DATA IMPORTER

Name: MICHAEL BRUNKER

Authorised Signature:



Appendix 3

to the Standard Contractual Clauses

Commerzbank AG's EU branch offices include branch offices located in the following countries: Germany, Austria, Italy, France, Spain, Netherlands Belgium, Luxembourg, Poland, Czech Republic, Slovakia
Furthermore it applies to all branches in Switzerland.

The German branch offices with further details are listed at
<https://www.commerzbank.de/filialen/de/filial-uebersicht.html>.

The branch offices outside of Germany with further details are listed at
<https://www.worldwide.commerzbank.com/de/home/inhalte/weltkarteseite.jsp?type=outlet>; for the purpose of this document, only the branch offices in the countries listed above are relevant.

On behalf of the data exporter

Roland Wolf

Name (written out in full): ROLAND WOLF

Position: DATA PROTECTION OFFICER

Address: Kaiserplatz 1, 60261 Frankfurt/Main, Germany

Other information necessary in order for the contract to be binding (if any):

Commerzbank AG
Kaiserplatz
60261 Frankfurt/Main

(stamp of organisation)

Signature [Signature]

On behalf of the data importer:

Name (written out in full): MICHAEL BRUNKER

Position: DATA PROTECTION OFFICER

Address: 30 GRESHAM STREET LONDON EC2N 7PG

Other information necessary in order for the contract to be binding (if any):

Commerzbank AG London Branch
30 Gresham Street
London
EC2N 7PG

(stamp of organisation)

Signature [Signature]