COMMERZBANK
The bank at your side

Conditions for Processing Banking Transactions through the Corporate Banking Portal

As at: June 2018, Commerzbank AG Vienna Branch, Austria

1. Scope of services

(1) The Customer (account holder who is not a consumer within the meaning of ZaDiG [Payment Services Act] 2018) may use the Corporate Banking Portal and execute banking transactions within the scope of services offered by the Bank. Execution of such transactions shall be subject to the conditions for the relevant banking transactions (for example General Business Conditions, Special Conditions for Commerzbank Online Banking Securities Transactions, Main Funders). The Customer may also access information from the Bank via the Corporate Banking Portal. In addition, for purposes of activating payment orders, the Customer is entitled to use a payment activation service in accordance with Section 1 para. 2 (7) ZaDiG 2018 and, for the purposes of communicating information about payment accounts, an account information service provider in accordance with Section 1 para. 2 (8) ZaDiG 2018.

(2) The Customer and the authorised persons shall hereinafter be collectively referred to as the "Subscriber" or "User". This also includes the "User" pursuant to the Terms and Conditions for Remote Data Transmission who uses the remote data transmission made available through the Corporate Banking Portal. The account and custody account shall hereinafter be collectively referred to as the "Account".

(3) The Customer and the Bank may agree on separate disposal limits for certain types of services.

2. Preconditions for use of the Corporate Banking Portal

For use of the Corporate Banking Portal, the Subscriber/User needs the personalised security features and authentication instruments agreed with the Bank in order to prove the Subscriber's/User's identity as an authorised party (see Section 3) and to authorise orders and issue transactional declarations (see Section 4). In place of a personalised security feature, a biometric feature of the Subscriber/User may also be agreed as a means of authentication and/or authorisation.

With effect from 1 December 2019, the Bank shall only accept authentication instruments on the basis of strong authentication within the meaning of Section 4 line 28 ZaDiG 2018 for the authorisation of payment transactions pursuant to Section 87 ZaDiG 2018.

2.1. Personalised security features

Personalised security features, which may also be alphanumeric, are personalised features that the Bank provides to the Subscriber for purposes of authentication. These may include the following:

- Personal Identification Number (PIN)
- Non-reusable Transaction Authorisation Numbers (photoTAN)
- Signature PIN/password and the data of the personal electronic key for the electronic signature

2.2. Authentication instruments

A photoTAN can be generated and made available to the Subscriber/User via a mobile or reading device. The Subscriber/User may use further authentication instruments to authorise transactions:

- a chip card with signature function, or
- another authentication instrument containing the signature key, including the storage of the electronic signature key in a technical environment provided by the Bank (or by a service provider authorised by the Bank) that is protected against unauthorised access,
- an app personalised for the Subscriber/User by the Bank in the initialisation process.

2.3. Agreement of personalised security features and authentication instruments

Each Subscriber/User may agree with the Bank which personalised security feature and authentication instrument is to be used.

3. Access to the Corporate Banking Portal

The Subscriber/User is given access to the Corporate Banking Portal if:

- the Subscriber/User has transmitted the Subscriber number/registration name and the PIN
- the verification of this data by the Bank has shown that an access authorisation for the Subscriber/User exists
- and access has not been blocked (see sections 9.1 and 10).

Once access to the Corporate Banking Portal has been granted, the Subscriber/User can retrieve information or place orders. Sentences 1 and 2 also apply if the Subscriber activates payment orders via a payment activation service or requests payment account information via an account information service provider (see Section 1 para. 1 sentence 4).

4. Execution of orders via the Corporate Banking Portal

4.1. Placing orders and authorisation

The authorisation to conduct individual transactions (for example, transfers) is carried out – depending on the selected type of service – via the agreed personalised security features:

- photoTAN
- PIN
- electronic signature
- biometric signature or

- by simple clearance after signing in with the Subscriber number and/or registration name and PIN

Sentence 1 also applies if the Subscriber activates and transmits a payment order via a payment activation service (see Section 1 para. 4).

4.2. Supplementary regulations for remote data transmission in the EBICS standard when using the photoTAN procedure

4.2.1. The Customer instructs the Bank to save the personal key of the Subscriber/User in a technical environment that is protected against unauthorised access. The Bank is also entitled to instruct a reliable service provider to do this. The password required to authorise the personal key shall be replaced by the TAN using the photoTAN procedure.

4.2.2. The Terms and Conditions for Remote Data Transmission shall be supplemented as follows:

- Supplemental to Section 4 (2) of the Terms and Conditions for Remote Data Transmission, it is permissible for the electronic key to be stored in a technical environment provided by the Bank (or by a service provider authorised by the Bank) (cf. Section 2.2.1 (5) of Annex 1a of the Terms and Conditions for Remote Data Transmission).
- Supplemental to Section 7 (3), it is agreed that the Bank may verify whether the correct photoTAN was entered.

4.2.3. Annex 1a of the Terms and Conditions for Remote Data Transmission shall be supplemented as follows:

- The authentication signature in Section 1.2 may also be rendered in the photoTAN procedure in the technical environment of the Bank or of an authorised service provider. These shall carry out the necessary verification for the Customer.
- Supplemental to Section 2.2.1 (5), it is agreed that the photoTAN will be used instead of a password if the security medium of the Subscriber is saved by the Bank in a technical environment that is protected against unauthorised access.
- The authorisation of orders in accordance with Section 3 may also be granted by entering the photoTAN shown on the mobile or reading device and the electronic signature subsequently generated in the secure technical environment.

4.3. Compliance with reporting regulations

When making payments in favour of non-residents, the Subscriber/User shall comply with the reporting duties set out in the Reporting Regulations of the OeNB adopted according to Section 6 para. 2 and 3 of the Austrian Foreign Exchange Act 2004 (currently “ZABIL 1/2013” in its version “ZABIL 1/2016” as well as according to the Ordinance regarding statistical surveys on the imports and exports of services and cross-border financial relations).

4.4. Revocation of orders

The extent to which an order can be revoked shall be governed by the special conditions applicable for the respective order type. Orders can only be revoked outside the Corporate Banking Portal unless the Bank expressly provides for a revocation option in the Corporate Banking Portal.

5. Processing of orders by the Bank

(1) Orders placed in the Corporate Banking Portal shall be processed according to the regulations governing the processing of orders under the agreed service type (for example, transfer or securities order).

(2) Payment orders (transfer, direct debit) shall be subject to the following special regulations:
The Bank shall execute the payment order subject to the following conditions:
- The Subscriber/User has submitted identification proof via a personalised security feature.
- The Subscriber’s/User’s authorisation for the relevant order type has been verified.
- The data format for the agreed type of service is adhered to.
- The separately agreed disposal limit for the service type has not been exceeded.
- The additional preconditions for execution according to the special conditions for the order type have been fulfilled.
- Sufficient account cover (credit balance or credit facility) is available.

If the preconditions for execution according to sentence 1 are complied with, the Bank shall execute the payment order. Such execution may not violate any other legal provisions.

(3) If the preconditions for execution according to para. 2 sentence 1 (1–5) are not complied with, the Bank shall not execute the payment order. The Bank shall notify the Subscriber/User online or otherwise of the non-execution of the order and, to the extent possible, of the reasons for the non-execution and the possibilities of correcting any errors that led to the non-execution. This shall not apply if the statement of reasons is in breach of other statutory provisions. If the Bank executes the order despite a lack of account cover, this shall result in a tolerated overdraft subject to an agreed interest charge.

6. Notification of the Customer regarding transactions effected via the Corporate Banking Portal

The Bank shall inform the Customer of the transactions effected via the Corporate Banking Portal using the channel agreed for account and custody account information and in accordance with the conditions applicable for the order.

7. Duties of care to be observed by the Subscriber/User

7.1. Technical connection to the Corporate Banking Portal

The Subscriber/User shall be obliged to establish the technical connection to the Corporate Banking Portal only through the access channels (for example, internet address) separately communicated by the Bank. For purposes of activating payment orders and accessing information about payment accounts, the Subscriber may also establish the technical connection to the Corporate Banking Portal via a payment activation service and/or an account information service provider (see Section 1 para. 1 sentence 4). The Subscriber/User shall be responsible for maintaining appropriate data backup for their

own systems and for taking sufficient precautions against viruses and other harmful programs (for example, Trojans, worms etc.) and keeping them constantly up to date. The Bank's apps may be obtained only from app providers of which the Bank has notified the customer. The Subscriber/User shall take responsibility for complying with the country-specific provisions for use of the internet.

7.2. Maintaining the secrecy of personalised security features and careful custody of authentication instruments

(1) Subscribers/Users shall
- keep their personalised security features (see Section 2.1) secret, and
- keep their authentication instruments (see Section 2.2) safe from access by other persons.

This is essential because any other person who is in possession of an authentication instrument can misuse the Corporate Banking Portal procedure in combination with the related personalised security feature. The secrecy obligation relating to personalised security features, as according to sentence 1, does not apply if the Subscriber transmits such features to a payment activation service or account information service provider appointed by the Subscriber (see Section 1 para. 1 sentence 4) for purposes of issuing a payment order or accessing information about a payment account.

(2) In particular, the following shall be observed to protect the personalised security feature and the authentication instrument:
- The personalised security features PIN and the signature PIN/password may not be stored electronically (for example in the Customer's system) by the Subscriber/User. The personal electronic key generated by the Subscriber/User shall be kept under the sole control of the Subscriber/User or in a technical environment made available by the Bank (or by a service provider authorised by the Bank) that is protected against unauthorised access.
- If a "Technical User" is used in the course of fully automated data transmission, the electronically stored signature shall be kept in a secure and appropriate technical environment. The "Technical User" is not entitled to issue the order itself, but may merely transmit the order data.
- When entering the personalised security features, it has to be ensured that no other person can spy out such features.
- Personalised security features may not be transmitted by email.
- The signature PIN/password for the electronic signature may not be kept together with the authentication instrument.
- The Subscriber/User may not use more than one photoTAN for the authorisation of an order.

7.3. Customer obligations regarding the security of the Customer's system

The Subscriber/User shall adhere to the security notices on the Bank's website at https://www.firmenkunden.commerzbank.de/portal/en/cb/de/footer/sicherheit/home.html, particularly the measures to protect the hardware and software used, and shall install up-to-date, state-of-the art virus protection and firewall systems. In particular, the operating system and security precautions of the mobile device may not be modified or deactivated.

7.4. Verification of the order data by means of the data displayed by the Bank

If the Bank displays data to the Subscriber/User contained in their Corporate Banking Portal order (for example, amount, account number of payee, securities identification number) in the Customer system or via another device of the Subscriber/User (for example, photoTAN reader, photoTANApp, chip card reader with display) for confirmation, the Subscriber/User shall be obliged to verify that the displayed data conform with the data of the intended transaction prior to confirmation.

7.5. Additional duties of care of the Customer

The Customer shall ensure that the duties of care arising from this Agreement are also observed by the authorised person(s) (i.e. all Subscribers/ Users).

8. Encryption technology abroad

The online access made available by the Bank may not be used in countries that restrict the use or the import/export of encryption techniques. Subscribers shall, where appropriate, arrange for the necessary permits, notifications or other required measures. Subscribers shall inform the Bank of any prohibitions, permit obligations and notification duties of which they become aware.

9. Notification and reporting duties

9.1. Blocking request

(1) If the Subscriber/User detects
- the loss or theft of the authentication instrument,
- the misuse, or
- any other unauthorised use of their authentication instrument or personal security feature, the Subscriber/User shall immediately notify the Bank thereof (blocking request).

the Subscriber/User may also submit a blocking request to the Bank whenever required by means of the blocking hotline communicated separately. If a connection to the hotline cannot be established, or in the event of disturbances, the Customer shall be obliged to promptly try all other lines of communication (e.g. telephoning a customer advisor) for purposes of damage mitigation.

(2) The Subscriber/User shall report any theft or misuse to the police without delay.

(3) In the event that the Subscriber/User suspects that another person
- has gained possession of their authentication instrument or has otherwise gained knowledge of their personalised security feature, or
- has used the authentication instrument or personalised security feature, the Subscriber/User shall also transmit a blocking request.

9.2. Notification of unauthorised or incorrectly executed orders

Customers shall notify the Bank as soon as they detect an unauthorised or incorrectly executed order.

9.3. Evidence

Upon request, the Bank shall provide the Customer with evidence that enables the Customer to prove, for up to 18 months

after notification, that the Customer has complied with the notification duty according to sections 9.1 and 9.2.

10. Blocking of access

10.1. Blocking of access at the request of the Subscriber/User

Upon request of the Subscriber/User, in particular in case of a blocking request according to Section 9.1, the Bank shall block the following:

- the Corporate Banking Portal access for that Subscriber/User and, if the Subscriber/User so demands, the access for all Subscribers/Users of the Customer, or
- the authentication instrument of the Subscriber/User.

10.2. Blocking of access at the request of the Bank

(1) The Bank may block the Corporate Banking Portal access for a Subscriber/User if
- the Bank is entitled to terminate the cooperation agreement for foreign and transaction business for good cause,
- this is justified due to objective reasons in connection with the security of the authentication instrument or the personalised security feature,
- there is suspicion of unauthorised or fraudulent use of the authentication instrument or of the personalised security feature, or
- the account holder has not satisfied their payment obligations relating to a line of credit in connection with e-banking in the Corporate Banking Portal (exceeded line of credit or overdraft) and the satisfaction of these payment obligations is jeopardised due to deterioration or endangerment of the Customer's financial circumstances or those of a co-obligated party; or because the Customer has become insolvent or there is an imminent risk of this.

(2) The Bank shall notify the Customer of the block in writing (e.g. via letter, fax or email) or by telephone, and provide the relevant reasons for it, if possible before but no later than immediately after the block is implemented.

(3) The Bank is also entitled to refuse access to the Customer's payment account to an account information services provider or a payment activation service if there is a reasonably justified suspicion of unauthorised access or the fraudulent activation of a payment transaction. The Bank shall inform the Customer of such refusal of access to the Customer's payment account in a form agreed upon with the Customer, as soon as possible but no later than immediately after access has been refused, provided that disclosure of the refusal or the grounds for refusal does not violate Austrian or Community legal provisions or objectively justified security considerations.

10.3. Unblocking of access

The Bank shall unblock the access or replace the personalised security feature or authentication instrument if the reasons for blocking the access no longer exist. It shall immediately notify the Customer thereof in writing (e.g. via letter, fax or email) or by telephone.

10.4. Automatic blocking

(1) The chip card with signature function is blocked if an incorrect user code is entered incorrectly three times in succession. The chip card cannot be unblocked or re-activated by the Bank. In such a case, the Subscriber/User shall generate a new electronic signature, transmit it to the Bank again and clear it with the Bank by an initialisation letter ("INI-Brief").

(2) The PIN is blocked if it has been entered incorrectly three times in succession.

(3) The Subscriber/User is blocked from using the photoTAN procedure, if the TAN has been entered incorrectly five times in succession.

(4) The Subscriber/User may contact the Bank in order to restore the functionality of the Business Customer Portal. The Bank shall notify the Customer at once that the account has been blocked, providing the reasons, unless to do so would compromise objectively justified security considerations or constitute a breach of provisions of Community or international regulations or of official court or administrative orders.

11. Liability when using personalised security features and/or authentication instruments

11.1. Liability of the Customer in the event of unauthorised payment transactions prior to a blocking request

(1) In the event that unauthorised payment transactions prior to a blocking request are made due to the use of an authentication instrument that has been lost, stolen or has otherwise gone missing, or due to the misuse of the personalised security feature or authentication instrument, the Customer shall be liable for any resulting losses incurred by the Bank if the loss, theft or other misplacement or other misuse of the personalised security feature or authentication instrument is the Subscriber's/User's fault. The Customer shall also be liable in the event of failing to select Subscribers with due care and/or failing to regularly check Subscribers' compliance with the obligations under these Conditions. The Customer shall further be liable to the Bank even if the Customer has culpably breached their duties of care pursuant to Section 63 ZaDiG 2018. If the Bank has contributed to the occurrence of a loss through any fault of its own, the principles of contributory negligence shall determine the extent to which the Bank and the Customer shall share the loss.

(2) The Customer is not obliged to provide compensation for the loss pursuant to Section 1 if the Subscriber/User was unable to lodge a blocking request in accordance with Section 9.1 because the Bank failed to ensure that a blocking request could be submitted, thereby causing the loss.

(3) The liability for losses caused during the period for which the Corporate Banking Portal disposal limit applies, as agreed with the Customer, shall be restricted to the amount of the respective limit.

(4) The paragraphs 2 and 3 shall not apply if the Subscriber has acted with fraudulent intent.

11.2. Liability for unauthorised securities transactions or other service types before a blocking request is made

In the event that unauthorised securities transactions or unauthorised transactions for the agreed service types prior to a blocking request are made due to the use of an authentication instrument that has been lost, stolen or has otherwise gone

missing, or due to the misuse of the personalised security feature or authentication instrument, the Customer shall be liable for any resulting losses incurred by the Bank if the loss, theft, other misplacement or other misuse of the personalised security feature or authentication instrument is the Subscriber's/User's fault. The Customer shall also be liable in the event of failing to select Subscribers with due care and/or failing to regularly check Subscribers' compliance with the obligations under these Conditions. If the Bank has contributed to the occurrence of a loss through any fault of its own, the principles of contributory negligence shall determine the extent to which the Bank and the Customer shall share the loss.

11.3. Liability of the Bank after a blocking request is made

As soon as the Bank receives a blocking request by a Subscriber/User, it shall bear all losses arising from unauthorised transactions incurred after receipt of the blocking request. This shall not apply if the Subscriber/User has acted with fraudulent intent.

12. Availability

The Bank shall make every effort to keep the services provided by the Corporate Banking Portal available to the greatest extent possible. However, this does not imply guaranteed availability. In particular, technical problems, maintenance and network problems (for example, non-availability of third-party servers) beyond the Bank's control may cause temporary disruptions that prevent access.

13. Links to third-party websites

If the internet pages provide access to third-party websites, this is only carried out in order to allow the Customer and User easier access to information on the internet. The contents of such sites do not constitute statements by the Bank itself and are not examined by the Bank.

14. Rights of use

This Agreement does not permit the Customer to create links or frame links on its websites without the Bank's prior written consent. The Customer undertakes to use the websites and their content for the Customer's own purposes. In particular, the Customer is not authorised without the Bank's consent to make the content available to third parties, to incorporate it into other products or procedures, or to decode the source code of individual web pages. References to the rights of the Bank or third parties may not be removed or made unrecognisable. The Customer may not use brand names, domain names or other trademarks of the Bank or third parties without the Bank's prior consent. Under the present Conditions, the Customer shall not receive any irrevocable, exclusive or assignable rights of usage.

15. Hotline ("Help Desk")

The Bank provides a telephone hotline (the "Help Desk") to process technical, operational or functionality questions regarding the services provided by the Corporate Banking Portal. The Bank staffs the hotline on bank days applicable to the banking industry in Austria, as found at https://www.oenb.at/en/Services/Bank-Holidays.html (Monday to Friday, except public holidays, 24th December and Good Friday).

Phone numbers and opening hours are communicated via the normal channels (e.g. https://www.commerzbank.at/portal/en/cb/at/firmenkunden/oesterreich.html).

16. Waiver of Sections 9 and 10 ECG, the discretionary provisions of the E-Commerce Act and ZaDiG 2018

The provisions of sections 9 and 10 of the Austrian E– Commerce Act (ECG) are hereby waived.

The following provisions of the Austrian Payment Services Act (ZaDiG) 2018 do not form an integral part of the contract for the Customer: the provisions of the third main section of ZaDiG 2018 as well as sections 32-54 [information requirements], Section 56 (1) [prohibition against charging fees for the fulfilment of information requirements or for corrective and safeguarding measures], Section 58 (3) [withdrawal of authorisation], Section 66 (1) and (3) [proof of authentication and execution of payment transactions], Section 68 (2),(5) and (6) [liability for unauthorised payment transactions], Section 70 (1) and (3) [refunds for a payment transaction initiated by the payee] and Section 80 [payment service providers' liability for non-execution, defective or late execution of payment transactions]. In Section 68 (1), the words "up to the amount of EUR 50" shall not apply to entrepreneurs.

17. Amendment clause

These Conditions for Processing Banking Transactions through the Corporate Banking Portal (hereinafter "Conditions") are available online at https://www.commerzbank.at.. The Bank shall also forward these Conditions to the Customer at any time if so requested.

Changes to these Conditions for Processing Banking Transactions through the Corporate Banking Portal – excluding the primary services rendered by the Bank and fees – shall be offered to the Customer by the Bank no later than two months before they are proposed to take effect. In that case, the provisions concerned by the amendment offer and by the proposed changes shall be presented in the form of a comparison of the respective provisions. The Customer's consent shall be deemed given unless the Bank receives an objection from the Customer prior to the proposed entry into effect. The Bank shall inform the Customer of this consequence in the amendment offer. In addition, the Bank shall publish a comparison of the provisions concerned by the changes to the Conditions as well as the complete version of the new Conditions on its website. The Bank shall also indicate this in the amendment offer. The offer may be communicated to the Customer in paper form, or electronically if so agreed, or made available for retrieval in a manner agreed with the Customer.

Amendments to the aforementioned Conditions shall be objectively justified in light of all circumstances (such as legal, regulatory and other official requirements, court rulings, the security of banking operations, technical developments, changes in predominant customer needs, or a substantial decrease in use of the service, considerably affecting cost recovery).