Conditions for Processing Banking Transactions
through the Corporate Banking Portal

Vienna Branch, Issued: February 2017

1. Scope of services

(1) The Customer 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 Terms and Conditions for Payment Services for Corporate Customers, Special Conditions for Commerzbank Banking Securities Transactions, Special Conditions for Main Funders). The Customer can also access information from the Bank.

(2) The Customer and the authorised persons shall hereinafter be referred to as the "Participant" 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 deposit shall hereinafter be referred to as "Account(s)".

(3) For the use of the Corporate Banking Portal the regular limits or drawing limits separately agreed with the Bank for the agreed type of service shall be applicable

2. Preconditions for the use of the Corporate Banking Portal

For the execution of banking transactions, the Participant/User needs the personalised security features and authentication instruments agreed with the Bank in order to prove his/her identity as authorised Participant/User (see Sect. 3) and to authorise orders (see Sect. 4). Each Participant/User may agree with the Bank which personalised security feature and authentication instrument he/she is to use.

2.1 Personalised security features

The personalised security features, which may also be alphanumeric, are:

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

2.2 Authentication instruments

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

- a chipcard with signature function, or
- other 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 Participant/User by the Bank in the initialisation process.

3. Access to the Corporate Banking Portal

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

- the Participant/User has transmitted the participant number/registration name and the PIN
- the verification of this data by the Bank has shown that an access authorisation for the Participant/User exists, and

access has not been blocked (see Sects. 9.1 and 10). Once access to the Corporate Banking Portal has been granted, the Participant/User can retrieve information or place orders.

4. Execution of orders via the Corporate Banking Portal

4.1 Placing orders and authorisation

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

- photoTAN,
- PIN,
- electronic signature, or
- by simple clearance after signing in with the participant number and/or registration name and PIN.

4.2 Compliance with reporting regulations

When making payments in favour of non-residents, the Participant/User must comply with the reporting duties set out in the Reporting Regulations of the OeNB adopted according to Art. 6, Para. 2 and 3 of the Austrian Foreign Exchange Act (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.

4.3 Revocation of orders

The revocability of an order shall be governed by the Special Conditions applicable to the relevant 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 credit transfer or securities order).

(2) Payment orders (credit transfer, direct debit) shall be subject to the following special regulations: The Bank will execute the order subject to
the following conditions:

- the Participant/User has proved his identity by means of his personalised security feature,
- the Participant'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 drawing limit or the standard limit for the respective type of service has not been exceeded.
- the preconditions for execution according to the relevant special conditions applicable to the relevant order type are fulfilled, and
- sufficient account cover (credit balance or credit facility) is available.

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

(3) If the preconditions for execution according to Subsect. (2), sentence 1, bullet points 1–5 are not complied with, the Bank will not execute the payment order. The Bank will provide the Participant/User online or otherwise about the non-execution of the order and, to the extent possible, of the reasons for the non-execution as well as of the possibilities of correcting any errors that led to the non-execution. This shall not apply if the statement of reasons would violate any legal provisions.

6. Notification to the Customer on drawings

The Bank shall notify the Customer of drawings made via the Corporate Banking Portal in the form agreed for account and securities account information and in

accordance with the conditions applicable to the order.

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

7.1 Technical connection to the Corporate Banking Portal

The Participant/User shall be obliged to establish the technical connection to the Corporate Banking Portal only through the access channels (for example Internet address) separately notified by the Bank. The Customer shall be responsible for maintaining appropriate data backup for his 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 which the Bank has notified to the Customer. The Customer shall take responsibility for complying with the country-specific provisions for the use of the Internet.

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

(1) The Participant/User shall

- keep his personalised security features (see Sect. 2.1) secret and transmit them to the Bank only via the Corporate Banking Portal access channels notified by the Bank separately or via the apps issued by the Bank, and
- keep his authentication instrument safely (see Sect. 2.2) to prevent access by other persons.

This is essential because any other person who is in possession of the authentication instrument can misuse the Corporate Banking Portal procedure in combination with the related personalised security feature.

(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 system) by the Participant/User. The personal electronic key generated by the Participant/User shall be under the sole control of the Participant/User only 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 must be kept in a secure and appropriate technical environment. The "Technical User" shall not be entitled to issue the order itself. it 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.
- The personalised security features may not be entered outside the separately agreed Internet pages or on apps other than those of the Bank (for example not on online pages of traders).
- The personalised security features may not be transmitted outside the Corporate Banking Portal, for instance not by email.
- The signature PIN / password for the electronic signature may not be kept together with the authentication instrument.
- The Participant/User may not use more than one photoTAN for the authorisation of an order.

7.3 Security of the Customer system

The Participant/User must adhere to the security notices on the Internet pages of the Bank, particularly the measures to protect the hardware and software used, and 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 Participant/User contained in his/her Corporate Banking Portal order (for example amount, account number of payee, securities identification number) in the Customer system or via another device of the Participant/User (for example chip card reader with display) for confirmation, the Participant/User shall be obliged to verify that the displayed data conform with the data of the intended transaction prior to confirmation.

7.4 Additional duties of care of the Customer

The Customer shall ensure that the obligations of care arising from this contract are also observed by his/her authorised persons (i.e. all Participants/ Users).

8. Encryption technology abroad

The online access made available by the Bank may not be used in countries where the use, import and export for encryption technology is restricted. The Participant must, where appropriate, arrange for the necessary permits, notifications or other required measures. The Participant must inform the Bank of any prohibitions, permit obligations and notification duties of which he/she has become aware.

9. Notification and reporting duties

9.1 Blocking request

(1) If the Participant/User detects

- the loss or theft of the authentication instrument,
- the misuse, or

any other unauthorised use of his/her authentication instrument or personal security feature, the Participant/User shall immediately notify the Bank thereof (blocking request). The Participant/User may make blocking request to the Bank whenever required also by means of the blocking hotline notified to him/her separately. The Participant may in case of any technical faults any other means to contact the bank.
(2) The Participant/User shall report any theft or misuse to the police without delay.

(3) In the event that the Participant/User suspects that another person

- has gained possession of his authentication instrument or has otherwise gained knowledge of his personalised security feature, or
- has used the authentication instrument or personalised security feature, he/she must also transmit a blocking request.

9.2 Notifying of unauthorised or incorrectly executed orders

The Customer shall notify the Bank as soon as he/she detects an unauthorised or incorrectly executed order.

9.3 Evidence

The Bank shall provide the Customer with evidence that enables the Customer to prove within a period of 18 months after notification that he/she has complied with his notification duty according to the Sects. 9.1 and 9.2.

10. Blocking of access

10.1 Blocking of access at the request of the Participant/User

Upon request of the Participant/User, in particular in case of a blocking request according to Sect. 9.1, the Bank will block the following:

- the Corporate Banking Portal access for that Participant/User and, if the Participant/User so demands, the access for all Participants/Users of the Customer, or
- the Participant's/User's authentication instrument.

10.2 Blocking of access at the request of the Bank

(1) The Bank may block the Corporate Banking Portal access for a Participant/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 withthe security of the authentication instrument or the personalised security feature, or
- there is suspicion of unauthorised or fraudulent use of the authentication instrument or of the personalised security feature.

(2) The Bank will notify the Customer by stating the relevant reasons for blocking the access, if possible before the access is blocked, in writing, if agreed electronically or available for retrieval in a manner agreed with the customer but at the latest immediately afterwards.

10.3 Unblocking of access

The Bank will unblock the access or exchange the personalised security feature or authentication instrument if the reasons for blocking the access do no longer exist. It will immediately notify the Customer thereof.in writing, if agreed electronically or available for retrieval in a manner agreed with the customer.

10.4 Automatic blocking

(1) The chip card with signature function will be blocked if the signature PIN / password for the electronic signature has been entered incorrectly three times in succession. The chip card cannot be unblocked or re-activated by the Bank.

(2) The transmitted signature will be blocked if the signature PIN / password for the signature has been entered incorrectly three times in succession. In such case, the Participant/User must generate a new electronic signature, transmit it to the Bank again and clear it with the Bank by an initialisation letter (“INI-Brief”).

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

(4) The Participant is blocked from using the photoTAN procedure, if the TAN has been entered incorrectly five times in succession.

(5) The Participant/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 for unauthorised payment transactions prior to a suspension request

(1) In the event that unauthorised payment transactions prior to a blocking request is 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 the loss incurred by the Bank if the loss, theft, or otherwise missing or other misuse of the personalised security feature or authentication instrument is the Participant’s/User’s fault. The Customer shall also be liable if he/she has not been careful in selecting any of his nominated Participants and/or has not regularly checked the Participant’s 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.

(2) The Customer shall not be obliged to compensate a loss according to Sub-sects. (1) and (2) above if the Participant/User was unable to give the blocking request according to Sect. 9.1 because the Bank had failed in ensuring that the blocking request could be received and the loss was incurred as a result.

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

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

If unauthorised securities transactions or unauthorised payment transactions for the agreed type of service occur prior to a blocking request is made due to the use of lost or stolen or otherwise missing authentication instrument or any other misuse of the personalised security feature or authentication instrument and the Bank has incurred a loss as a result, the Customer shall be liable for the resulting loss to the Bank if the loss, theft, or other misuse of the personalised security feature or authentication instrument is the Participant's/User's fault. The Customer shall also be liable if he has not been careful in selecting any of his nominated participants and/or has not regularly checked the Participant's 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 the blocking request is made

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

12. Availability

The Bank will 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 server) beyond the Bank's control may cause temporary disruptions that prevent access.

13. Links to third-party websites

If the Internet page provides access to third-party websites, this is only done in order to allow the Customer and User easier access to information on the Internet. The contents of such sites shall not constitute own statements by the Bank and are also not examined by the Bank.

14. Rights of use

This Agreement does not permit the Customer to create links or frame links to its websites without the Bank's prior written consent. The Customer hereby undertakes to use the websites and their content for its own purposes. In particular, the Customer is not authorised to make the contents available to third parties, to incorporate it into other products or procedures or to decode the source code of individual Internet pages without the Bank's consent. References to the rights of the Bank or third parties may not be removed or made unrecognisable. The Customer will 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 does 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 will staff the Help Desk on bank days applicable to the banking industry (see https://www.oenb.at/Service/Bankfeiertage.html). Phone numbers and opening hours shall be communicated by the available through the usual access path (e.g. Firmenkunden-portal.de/kontakt)

16. Waiver of the Articles 9, 10 ECG

The provisions of Articles 9 and 10 ECG (E-Commerce-Gesetz) are hereby waived.

17. Changes to these Conditions for Processing Banking Transactions through the Corporate Banking Portal

(1) The Conditions for Processing Banking Transactions through the Corporate Banking Portal are available on the Internet under https://www.firmenkunden.commerzbank.de/portal/ The Bank will also forward these conditions to the Customer at any time if so requested.

(2) Changes to these Conditions for Processing Banking Transactions through the Corporate Banking Portal – excluding the main to the performance to be rendered by the bank and fees – shall be offered to the customer by the bank not later than two months before they are proposed to take effect. On that occasion, the provisions concerned by the offer of change as well as the proposed changes shall be presented in the form of a comparison of the respective provisions.
The customer's consent will be deemed to be given unless the bank has received an objection from the customer prior to the proposed entry into effect. The bank shall inform the customer of this consequence in the offer of change. In addition, the bank shall publish a comparison of the provisions concerned by the change to the aformentioned conditions as well as the complete version of the new aformentioned conditions on its website. The bank shall indicate this, too, in the offer of change. A customer will be informed of the offer in writing, if agreed electronically or available for retrieval in a manner agreed with the customer.

(3) Changes of aformentioned conditions must be made by taking into account all circumstances (such al legal requirements, regulatory requirements, the security of banking operations, technical developments or the substancial decrease in efficiency, substantially affecting cost recovery).