

Corporate Banking

Conditions for Processing Banking Transactions via the Corporate Banking Portal and HBCI/FinTS Service

(Status 13 January 2018)

1. Scope of services

(1) The Customer and its authorised representatives may use the Corporate Banking Portal or HBCI/FinTS-Service and conduct banking business within the scope offered by the Bank. The execution shall be subject to the conditions for the relevant banking transactions (for example, Corporate Customer Terms and Conditions for Payment Services, special conditions for Commerzbank online banking securities transactions, special conditions for securities transactions). The Customer can also access information from the Bank. The Customer shall be entitled to also use a payment initiation service as defined in Section 1 (33) of the German Payment Services Supervision Act (Zahlungsdienstleistungsgesetz) to issue a payment order to the Bank and an account information service as defined in Section 1 (34) of the German Payment Services Supervision Act (Zahlungsdienstleistungsgesetz) for the provision of information on a payment account.

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

(3) The Customer and the Bank may agree on special limits for certain service limits.

2. Preconditions for the use of the Corporate Banking Portal and the HBCI/FinTS Service

In order to use the Corporate Banking Portal or the HBCI/FinTS Service, the Subscriber/User needs the Personalised Security Credentials and Authentication Instruments agreed with the Bank in order to prove his/her identity as the authorised Subscriber/User (cf. Number 3) and to authorise orders (cf. Number 4). Instead of a Personalised Security Credential, a biometric feature of the Subscriber may also be agreed for the purposes of authentication or authorisation.

2.1 Personalised Security Credentials

The Personalised Security Credentials, which may also be alphanumeric, are personalised features provided by the Bank to the Subscriber for the purposes of authentication. These are, for example:

- the personal identification number (PIN),

- transaction authorisation numbers (photoTAN), usable once only, and
- the signature PIN/code word 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 Subscriber/User via a mobile device or reading device. The Subscriber/User may use further Authentication Instruments to authorise transactions:

- a chipcard 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 Credentials and Authentication Instruments

Each Subscriber may agree with the Bank which Personalised Security Features and Authorisation Instruments they will use.

3. Access to the Corporate Banking Portal

The Subscriber/User is allowed 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 (cf. Nos. 9.1 and 10). After access to the Corporate Banking Portal has been enabled, the Subscriber/User can retrieve information or place orders.

Sentences 1 and 2 also apply if the Subscriber releases payment orders via a payment initiation service and requests payment account information via an account information service (cf. number 1 (1) sentence 4).

4. Execution of orders

4.1 Placing orders and authorisation

The authorisation to implement individual transactions (for example, credit transfer, time deposits) is carried out -

depending on the selected type of service – by the agreed Personalised Security Credentials:

- photoTAN,
- PIN,
- biometric signature, or
- by simple clearance after signing in with the subscriber number or registration name and PIN.

Sentence 1 also applies if the Subscriber initiates and transmits a payment order via a payment initiation service (cf. number 1 (1) sentence 4).

4.2 Supplementary regulations for long-distance 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 shall also be entitled to instruct a reliable service provider to do this. The code word necessary to authorise the personal key shall be replaced by a TAN in the photoTAN procedure.

4.2.2 The Conditions for Long-distance Data Transmission shall be supplemented as follows:

- Supplemental to No. 4. (2) of the Conditions for Long-distance Data Transmission, the storage of the electronic key in a technical environment provided by the Bank (or by a service provider authorised by the Bank) (see No. 2.2.1, (5) of Annex 1a to the Conditions for Long-distance Data Transmission) shall be permitted.
- To No. 7 (3), it is agreed that the Bank may verify whether the correct photoTAN was entered.

4.2.3 Annex 1a of the Conditions for Long-distance Data Transmission shall be supplemented as follows:

- The authentication signature in No. 1.2 may also be rendered in the photoTAN procedure in the technical environment of the Bank or of an authorised service provider. These will carry out the necessary verification for the Customer.
- To No. 2.2 (5), it is agreed that the photoTAN will be used instead of a code word 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 No. 3 may also be granted by entering the photoTAN shown on the mobile device or reading device and the electronic signature subsequently generated in the secure technical environment.
- In the case of a distributed electronic signature (VEU) in accordance with No. 3.1 para. 1, the approval and thus the authorisation with the second banking signature may take place by using the photoTAN or by authorising an order using the personalised app provided by the Bank.

4.3 Report according to the German Foreign Trade Ordinance (AWV)

In connection with payments in favour of non-residents, the Subscriber/User must report the transaction according to the Foreign Trade Ordinance (“Außenwirtschaftsverordnung”, AWV).

4.4 Revocation of orders

The revocability of an order shall be subject to the special conditions applicable for the relevant order type. Orders can only be revoked outside the Corporate Banking Portal and HBCI/FinTS Service, unless the Bank expressly provides for a revocation option in the Corporate Banking Portal or HBCI/FinTS Service.

5. Processing of orders by the Bank

(1) The orders placed within the scope of the Corporate Banking Portal shall be processed according to the regulations applicable for the processing of the relevant order 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 if the following conditions are met:

- the Subscriber/User has proved his identity by means of his Personalised Security Credential,
- 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 drawing limit for the service type or the standard limit is not exceeded,
- the further preconditions for execution according to the relevant special conditions applicable to the relevant order type are fulfilled, and
- sufficient cover in the account (credit balance or granted credit) is available.

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

(3) If the preconditions for execution according to para. (2), sentence 1, bullet points 1-5 are not complied with, the Bank will not execute the payment order. The Bank will inform the Subscriber/User about the non-execution of the order and, as far as possible, the reasons in this connection for the non-execution as well as specifying the possibilities for correcting any mistakes that led to the non execution. This shall not apply if the statement of reasons is in breach of any other legal provisions. If the Bank executes the order in the absence of sufficient cover in the account, a tolerated overdraft arises for which an agreed interest rate shall be payable.

6. Notification to the Customer on drawings

The Bank shall notify the Customer of the drawings made via the Corporate Banking Portal or HBCI/FinTS Service in the form agreed for account and securities account information and in accordance with the conditions applicable for the order.

7. Duties of care of the Subscriber/User

7.1 Technical connection

The Subscriber/User shall be obliged to establish the technical connection via access channels separately notified by Bank (for example, Internet address). To initiate a payment order and to call up information on a payment account, the Subscriber may make the technical connection to the Corporate Banking Portal also via a payment initiation service or an account information service (cf. number 1 (1) sentence 4). The Subscriber/User 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 such systems constantly up to date. The Bank's apps may be obtained only from app providers which the Bank has notified to the Customer. The Subscriber/User shall take responsibility for complying with the country-specific provisions for the use of the Internet.

7.2 Keeping the Personalised Security Credentials secret and careful safekeeping of the Authentication Instruments

(1) The Subscriber/User shall

- keep his Personalised Security Credentials (see No. 2.1) secret and
- keep his Authentication Instrument safe (see No. 2.1) to prevent access by other persons.

This is because any other person who is in possession of the Authentication Instrument can misuse the Personalised Security Credentials. The duty of secrecy regarding the Personalised Security Credentials pursuant to sentence 1 does not apply if the Subscriber transmits this to a payment initiation service or an account information service chosen by them to issue a payment order or to call up information on a payment account (cf. number 1 (1) sentence 4).

(2) In particular, the following points are to be observed for the protection of the Personalised Security Credential and the Authentication Instrument:

- The Personalised Security Credential PIN and the signature PIN/code word may not be insecurely stored electronically by the Subscriber/User. The personal electronic key generated by the Subscriber/User shall be under the control of the Subscriber/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 correspondingly suitable 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 Credential, it has to be ensured that no other person can spy it out.
- The Personalised Security Credential must not be forwarded by email.
- The signature PIN/code word for the electronic signature may not be kept together with the Authentication Instrument.

- The Subscriber/User may not use more than one photo-TAN for the authorisation of an order.

7.3 Security of the Customer system

The Subscriber/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 to the Subscriber/User data contained in his 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, photoTAN app, 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 Other obligations of care of the Customer

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

8. Encryption technology abroad

The online access made available by the Bank may not be used in countries where restrictions of use or import and export restrictions for encryption techniques exist. If appropriate, the Subscriber must arrange for the necessary permits, notifications or other necessary measures to be made. The Subscriber must inform the Bank about any prohibitions, permit obligations and notification obligations of which he becomes aware.

9. Notification and information 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 his Authentication Instruments or one of his Personal Security Credentials, the Subscriber/User shall notify the Bank thereof without delay (blocking request). The Subscriber/User may make a blocking request to the Bank whenever required also by means of the blocking hotline notified to him separately.

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

(3) If the Subscriber/User has the suspicion that another person

- has come into the possession of his Authentication Instrument in an unauthorised manner or has otherwise gained knowledge of his Personalised Security Credential, or
- has used the Authentication Instrument or Personalised Security Credentials, he must also make a blocking request.

9.2 Notification of unauthorised or incorrectly executed orders

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

10. Blocking of access

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

At the request of the Subscriber/User, especially in the event of a blocking request according to No. 9.1 above, the Bank will 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 Subscriber'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 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 Credentials, or
- there is suspicion of unauthorised or fraudulent use of the Authentication Instrument or the Personalised Security Credential.

(2) The Bank shall notify the Customer in text form, (e.g. by letter, fax or email) or by telephone, stating the relevant reasons for blocking the access, if possible, before access is blocked, but at the latest immediately afterwards.

10.3 Unblocking of access

The Bank will unblock the access or exchange the Personalised Security Credential or Authentication Instrument if the reasons for blocking the access are no longer applicable. It will notify the Customer thereof without delay.

10.4 Automatic blocking

(1) The chip card with signature function will be blocked if the user code for the electronic signature has been entered incorrectly three times in succession. The chip card cannot be unblocked by the Bank. The Subscriber/User must create a new electronic signature with a new chipcard and transmit this to the Bank anew and have this released by the Bank using an INI letter.

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

(3) The Subscriber 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 Corporate Banking Portal. The Bank shall notify the Customer at once that the account has been blocked, providing the reasons therefor, unless to do so would compromise objectively justified security consid-

erations or constitute a breach of provisions of community or international regulations or of official court or administrative orders.

11. Liability in the use of Personalised Security Credentials and/or Authentication Instruments

11.1 Liability of the Customer for unauthorised payment transactions before a blocking request is made

(1) If unauthorised payment transactions occur before a blocking request is made due to the use of an Authentication Instrument which has been lost or stolen or has otherwise gone missing or due to other misuse of the Personalised Security Credential 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 Credential or Authentication Instrument is the Subscriber's/User's fault. The Customer shall also be liable if he has not been careful in selecting any of his nominated Subscribers and/or has not regularly checked the Subscriber'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 must bear the loss.

(2) The Customer shall not be obliged to refund the loss according to para 1 above if the Subscriber/User was unable to give the blocking request according to No. 9.1 because the Bank had failed to ensure that the blocking request could be received.

(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 relevant limit.

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

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

If unauthorised securities transactions or unauthorised payment transactions for the agreed type of service occur before a blocking request is made due to the use of a lost or stolen or otherwise missing Authentication Instrument or any other misuse of the Personalised Security Credential 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 Credential or Authentication Instrument is the Subscriber's/User's fault. The Customer shall also be liable if he has not been careful in selecting any of his nominated Subscribers and/or has not regularly checked the Subscriber'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 must bear 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 Subscriber/User, it will bear all losses incurred after the date of the blocking request arising from unauthorised drawings. This shall not apply if the Subscriber/User has acted with fraudulent intent.

11.4 Preclusion of liability

Liability claims shall be precluded if the circumstances substantiating a claim are based upon an exceptional and unforeseeable event on which the party invoking this event has no influence and whose consequences could not be avoided even by exercising due diligence.

12. Availability

The Bank shall strive to keep the services provided available to the greatest extent possible. This does not imply guaranteed availability. In particular, technical problems, maintenance and network problems (for example, non-availability of a third-party server) over which the Bank has no control may cause intermittent 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 internal statements by the Bank and are not reviewed 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 only. 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. Notices of 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 these conditions, the Customer does not receive any irrevocable, exclusive or assignable rights of use.

15. Hotline ("Help Desk")

The Bank will set up a telephone hotline (the "Help Desk") to process technical, operational or functionality questions regarding the services provided. The Bank will staff the Help Desk on banking days applicable to the German banking industry. Phone numbers and opening hours shall be communicated by the normal information channels.

16. Miscellaneous

(1) In the interest of proper cooperation, the Bank hereby reserves the right to make changes of a technical or organisational nature, based on a general, standard modification in technical standards, in specifications applicable to the banking industry or in legal or regulatory provisions. For significant technical or organisational modifications that go beyond this and which have a significant impact on the rights and obligations of the Customer or of the Bank, the Bank shall notify the Customer of such modifications at least six weeks before the proposed date on which the modifications are to go into effect. The Customer's consent shall be deemed granted if he has not communicated his rejection within six weeks of receipt of the notification.

(2) These conditions shall be governed by the laws of the Federal Republic of Germany.

(3) If this Agreement should contain a loophole, or if a provision herein should be invalid or unenforceable, this fact shall not affect the validity of the remaining provisions. In such an event, the Parties to the agreement hereby oblige themselves to agree upon a valid or enforceable provision that comes as close as possible to fulfilling the spirit and purpose of the provision to be replaced.

Commerzbank AG