COMMERZBANK
The bank at your side

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

(Status 14 September 2019)

1. Scope of services

(1) The Customer and their authorised representatives may settle bank transactions using the Corporate Banking Portal or the HBCI/FinTS-Service in 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). You can also call up bank information.

(2) The Customer and authorised representatives shall be uniformly referred to as the "Subscribers" or "Users". This also includes the "User" as pursuant to the Conditions for Remote Data Transmission, who use Remote Data Transmission made available through the Corporate Banking Portal. The account and deposit shall be uniformly referred to as the "Account", unless anything to the contrary is explicitly set.

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

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

(1) The Subscriber/User may use the Corporate Banking Portal or the HBCI/FinTS-Service if they have been authenticated by the Bank.

(2) Authentication is the procedure separately agreed with the Bank which the Bank can use to check the identity of the Subscriber/User or the authorised use of an agreed payment instrument, including the use of the Personalised Security Credentials of the Subscriber/User. Using the authentication elements agreed for this purpose, the Subscriber/User can identify themselves to the Bank as an authorised Subscriber/User, access information (see number 3 of these Conditions) and issue orders (see number 4 of these Conditions).

(3) Authentication elements are
- knowledge elements, i.e. something only the Subscriber/User knows (e.g. Personal Identification Number [PIN]),
- possession elements, i.e. something only the Subscriber/User owns (e.g. device for generating or receiving single-use transaction numbers [TAN], that verify the ownership of the Subscriber/User, such as mobile terminals) or
- inherence elements, i.e. something the Subscriber/User is (e.g. fingerprints as a biometric credential of the Subscriber).

(4) The Subscriber/User is authenticated by the Subscriber/User transmitting the knowledge element, evidence of the possession element and/or evidence of the inherence element to the Bank as per the Bank's requirements.

3. Access to the Corporate Banking Portal

(1) The Subscriber/User is allowed access to the Corporate Banking Portal, if
- he gives his individual subscriber number/registration name and
- he discloses the authentication element(s) requested by the Bank and
- access has not been blocked (see Numbers 9.1 and 10 of these Conditions).

After access to the Corporate Banking Portal has been enabled, information can be accessed or orders issued as per number 4 of these Conditions.

(2) To access sensitive numerical data in accordance with section 1 (26) 1 German Payment Services Supervision Act [Zahlungsdiensteaufsichtsgesetz, or ZAG] (e.g. for the purposes of changing the Customer's address), the Bank will request the Subscriber/User to identify themselves using an additional authentication element, if only one authentication element was requested when accessing the Corporate Banking Portal. The name of the account holder and the account number are not sensitive data for the payment initiation services and account information services used by the Subscriber/User (section 1 (26) 2 ZAG).

4. Orders

4.1 Placing orders

The Subscriber/User has to agree to the effectiveness of an order (e.g. a credit transfer) issued via the Corporate Banking Portal or the HBCI/FinTS-Service (authorisation). On request, he has to use authentication elements (e.g. entering a TAN as evidence of the possession element).

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 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 remote data transmission shall be supplemented as follows:
- Supplementing to No. 4 (2) of the Conditions for Remote 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) shall be permitted (see No. 2.2.1, (5) of Annex 1a to the Conditions for Remote Data Transmission).
- To No. 8 (3) of the Conditions for Remote Data Transmission it is agreed that the Bank may verify whether the correct TAN was entered.

4.2.3 Annex 1a to the Conditions for Remote Data Transmission shall be supplemented as follows:
- The authentication signature in No. 1.1.2 of Annex 1a to the Conditions for Remote Data Transmission 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. 2.2.1 (5) of Annex 1a to the Conditions for Remote Data Transmission it is agreed the TAN 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.

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 shall be processed according to the regulations applicable for the processing of the relevant order type (e.g. credit transfer or securities order).

(2) The Bank will execute the order if the following execution conditions are met:
- The Subscriber/User has authorised the order (see number 4.1. of these Conditions).
- The Subscriber's/User's authorisation for the relevant order type (e.g. securities order) has been verified. The data format for the agreed type of service is adhered to.
- The further preconditions for execution according to the relevant special conditions applicable to the relevant order type are fulfilled.
- The additional execution conditions as per the special terms and conditions applicable to the relevant type of order (e.g. sufficient funds in the account as per the Corporate Banking Terms and Conditions for Payment Services) are met.

If preconditions for execution according to para. (2), sentence 1 are complied with, the Bank will execute the orders as per the special terms and conditions applicable to the relevant type of order.

If preconditions for execution according to para. (2), sentence 1 are not complied with, the Bank will not execute the order. The Bank will inform the Subscriber/User of this 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.

6. Customer information about disposals issued

The Bank shall notify the Customer at least once a month 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 Protecting authentication elements

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.

(1) The Subscriber/User must take all reasonable precautions to protect their authentication elements (see number 2 of these Conditions) against unauthorised access. Otherwise, there would be a danger that the procedure could be misused or otherwise used without authorisation (see number 3 and 4 of these Conditions).

(2) Above all the Subscriber/User has to comply with the following to protect the individual authentication elements:

(a) Knowledge elements, e.g. the PIN, must be kept secret; in particular they must
- not be given verbally (e.g. by telephone or in person),
- not be forwarded outside the procedure in text form (e.g. by email, messenger service),
- not be stored unsecured electronically (e.g. storing the PIN in clear text on a computer or in a mobile terminal) and
- not noted on a device or stored as a written note together with a device that serves as a possession element (e.g. mobile terminal, signature card) or to check an inherence element (e.g. mobile terminal with application for online banking and a fingerprint sensor).

(b) Possession elements, such as a mobile terminal, must be protected against misuse, in particular
- the signature card must be kept secure from unauthorised access by other persons,
- it must be ensured that other unauthorised persons cannot access the mobile terminal of the Subscriber/User (e.g. mobile telephone),
- it must be ensured that other persons cannot use the application for the Corporate Banking Portal (e.g. application app, authentication app) on the mobile terminal,
- the application for the Corporate Banking Portal (e.g. application app, authentication app) on the mobile terminal of the Subscriber/User must be deactivated before the Subscriber/User gives up possession of this mobile terminal (e.g. by selling or disposing of the mobile telephone),
- the evidence of the possession element (e.g. TAN) must not be forwarded outside the Corporate Banking Portal or the HBCI/FinTS-Service verbally (e.g. by telephone) or in text form (e.g. by email, messenger service) and
- the Subscriber who has received a code from the Bank to activate the possession element (e.g. mobile telephone with application for the Corporate Banking Portal) must safeguard this from unauthorised access; otherwise there would be a danger that other persons could activate their device as a possession element for the Corporate Banking Portal of the Subscriber/User.

(c) Inherence elements, such as the Subscriber's fingerprints, may only be used on a mobile terminal of the Subscriber/User for the Corporate Banking Portal as an authentication element if no inherence elements of other persons are stored on the mobile terminal. If inherence elements of other persons are stored on the mobile terminal used for the Corporate Banking Portal, the knowledge element issued by the Bank for the Corporate Banking Portal (e.g. PIN) must be used and not the inherence element stored on the mobile terminal.

(d) Please note the following in addition:
- 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 Personalised Security Credentials, it has to be ensured that no other persons can spy it out.
- 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 TAN for the authorisation of an order.

(3) The Bank's app for encrypting the TAN graphic must be sourced directly from the Bank or from a provider notified to the Customer by the Bank.

7.2 Security notices from the Bank

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 (customer system) 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.

7.3 Checking order data by means of the data displayed by the Bank

The Bank will show the Subscriber/User the order data it has received from them (e.g. amount, account number of the payee, securities identification number) on the device of the Subscriber/User separately agreed (e.g. using a mobile device). The Subscriber/User shall be obliged to verify the data shown corresponds with the data planned for the order before confirming.

7.4 Other obligations of care of the Customer

The Customer shall ensure that the obligations of care arising from this Conditions 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 notices

(1) If the Subscriber/User detects
- the loss or theft of a possession element for authentication (e.g. mobile terminal) or
- the misuse or
- any other unauthorised use of an authentication element,

the Subscriber/User shall notify the Bank thereof without delay (blocking request). The Subscriber/User can give such a blocking notice at any time including via the separately notified communications channels.

(2) The Subscriber/User shall report every theft or misuse of an authentication element to the police without delay.

(3) If the Subscriber/User suspects unauthorised or fraudulent use of one of their authentication elements, they must also issue a blocking notice without delay.

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 Block 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 of these Conditions, the Bank will block the following,

- the access for them or all Subscribers/Users or
- the Subscriber's/User's authentication element to use the Corporate Banking Portal and the HBCI/FinTS-Service.

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 agreement with cause,
- this is justified due to objective reasons in connection with the authentication elements of the Subscriber/User,
- there is suspicion of unauthorised or fraudulent use of the authentication elements,
- the control value to approve the HBCI signature is entered incorrectly three times in a row. In this case the Subscriber/User has to create a new electronic signature and transmit it to the Bank once again,
- the PIN has been entered incorrectly three times in a row or
- the TAN has been entered incorrectly five times in a row.

(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. The disclosure of grounds may be omitted if the Bank would breach legal obligations by doing so.

10.3 Unblocking of access

The Bank will unblock the access or authentication elements affected if the reasons for blocking the access are no longer applicable. It will notify the Customer thereof without delay.

10.4 Automatic blocking of a chip-based possession element

(1) A chip card with signature function blocks itself if the user code for the electronic signature is 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 possession element can then no longer be used for the Corporate Banking Portal or the HBCI/FinTS-Service. The Subscriber/User may contact the Bank in order to restore the functionality.

11. Liability

11.1 Liability of the Bank when executing an unauthorised order and an order that is not executed, is executed incorrectly or too late

The liability of the Bank when executing an unauthorised order and an order that is not executed, is executed incorrectly or too late is oriented on the special conditions agreed for the relevant type of order.

11.2 Liability of the Customer in the event of misuse of his authentication elements

11.2.1 Liability of the Customer for unauthorised payment transactions before blocking request

(1) If unauthorised payment transactions occur before a blocking request is made due to the use of an authentication elements which has been lost or stolen or has otherwise gone missing or due to other misuse of the authentication element, the Customer shall be liable for the loss incurred by the Bank if the loss, theft, or otherwise missing or other misuse of the authentication elements 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 Subscriber's/User's and/or has not regularly checked the Subscriber's/User'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. If the Customer is a businessperson as per section 14 BGB (German Civil Code), the limitation of liability to €50 as per section 675v (1) BGB shall not apply.

(2) The Customer shall not be obliged to refund the loss according to para. 1 above if
- it was not possible for them to identify the loss, theft, missing or other misuse of the authentication elements before the unauthorised payment procedure, or
- the loss of the authentication elements was caused by an employee, an agent, a branch of a payment service provider or any other point to which the activities of the payment service provider have been outsourced.

(3) If an unauthorised payment procedure occurs before a blocking notice and if the Subscriber/User acted with fraudulent intent or deliberately, or with gross negligence breached their duties of care in accordance with these Conditions, in variance from paragraphs 1 and 2, the Customer shall bear the loss incurred in full. Gross negligence of the Subscriber/User may exist in particular if they have breached one of their duties of care in accordance with
- number 7.1 (2),
- number 7.1 (3),
- number 7.3,
- number 9.1 (1) or
- number 9.2

of these Conditions.

(4) In variance from paragraphs 1 and 3, the Customer is not obliged to render compensation if the Bank did not demand strong authentication from the Subscriber/User in accordance with section 1 (24) ZAG. Strong customer authentication requires in particular the use of two independent authentication elements from the categories knowledge, possession or inherence (see number 2 (3) of these Conditions).

(5) 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.

(6) The Customer is not obliged to render compensation for a loss in accordance with paragraph 1 and 3 if the Subscriber/User could not issue the blocking notice

in accordance with number 9.1 of these Conditions because the Bank did not ensure the possibility to receive the blocking notice.

(7) Paras 2 and 4 to 6 shall not apply if the Subscriber/User acted with fraudulent intent.

11.2.2 Liability of the Customer for unauthorised disposals outside payment services (e.g. securities transactions) before the blocking request

If unauthorised disposition outside payment services (e.g. securities transactions) before a blocking request is made due to the use of a lost or stolen or otherwise missing authentication element or any other misuse of an authentication element 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 authentication element 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/Users and/or has not regularly checked the Subscriber's/User'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.

11.2.3 Liability from the issue of a blocking notice

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.

11.2.4 Preclusion of liability

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.

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 Subscriber/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