

Terms and Conditions for banking transactions via Berenberg Corporate Portal



BERENBERG
PARTNERSHIP SINCE 1590

1. Service

(1) The Customer may conduct banking business via Berenberg Corporate Portal by using the range of banking services offered by the Bank. The use of the offered range of services is subject to the terms and conditions of such services (e.g. Conditions for Credit Transfers). In addition, the Customer may use Berenberg Corporate Portal to obtain information from the Bank.

(2) If the Berenberg Corporate Portal shall include further accounts maintained by the Customer with other banks, the Customer shall instruct such banks to transfer the relevant information to the Bank and entitle such banks to receive such data that has been transmitted by the Bank. The Bank will act in such circumstances solely as receiving or transmitting agent. The Customer shall inform the Bank in due time about the necessary details.

(3) The Customer and attorney(s) are hereinafter collectively referred to as »Participant(s)«. Account(s) and safe custody account(s) are hereinafter collectively referred to as »Account(s)«.

(4) The use of Berenberg Corporate Portal is subject to the transaction limits agreed separately with the Bank.

2. Preconditions for the use of Berenberg Corporate Portal

To use Berenberg Corporate Portal, the Participant requires the personalized security features and authentication media agreed with the Bank in order to identify himself/herself as an authorised Participant (see No. 3) and to authorise orders (see No. 4).

2.1 Personalised security features Personalised security features, which can also be in alphanumeric format, are the personal password to be chosen during the initialisation process and the electronic key.

2.2 Authentication media The Participant can currently store the electronic key on the following authentication instruments using the technical framework specified by the Bank:

- mobile device (e.g. smartphone)
- Security Token App on desktop systems.

3. Accessing the Berenberg Corporate Portal

The Participant is given access to the Berenberg Corporate Portal once

- the Participant enters the individual Customer identification number on the input screen provided for this purpose and identifies himself/herself by using the personalised security feature(s) requested by the Bank,
- a check of this data by the Bank establishes that the Participant is authorized to access the Berenberg Corporate Portal, and
- the access is not blocked (see Nos. 9.1 and 10).

Once the Participant has been granted access to the Berenberg Corporate Portal, the Participant is authorised to query information or issue orders.

4. Processing of orders via the Berenberg Corporate Portal

4.1 Issuing orders and authorisation For orders (e.g. credit transfers) to be effective, the Participant must authorise them using the agreed personal password and the electronic key.

4.2 Reporting regulations under German foreign trade ordinance (AWV) In case of payments to non-residents the Participant is obliged to comply with the requirements under the German foreign trade ordinance (AWV).

4.3 Revocation of orders Whether or not an order can be revoked is governed by the special conditions applicable to the relevant type of order. Orders can only be revoked outside the Berenberg Corporate Portal unless the Bank expressly provides a facility for revoking them as part of the Berenberg Corporate Portal.

5. Processing of banking orders by the Bank

(1) Orders received by the Bank via the Berenberg Corporate Portal are processed in accordance with the provisions of the special conditions applicable to the relevant type of order.

(2) For payment orders (credit transfers, direct debits) the following shall apply:

The Bank will execute such orders when the following conditions for execution have been met:

- the Participant has proven his/her identity by means of the personalised security features requested by the Bank;
- the Participant is authorised to issue the relevant type of order;
- the data format has been adhered to;

- the separately agreed transaction limit has not been exceeded;
- the conditions for execution as set out in the special conditions applicable to the relevant type of order have been met; and
- there are sufficient funds in the account.

If the conditions for execution set out above have been met, the Bank executes the online banking orders. The execution must not breach any further regulation.

(3) If the conditions for execution set out under para. 2 sentence 1 are not met, the Bank will not execute the order. The Bank will notify the Participant online or by other means of information about the non-execution and, as far as possible, state the reasons for rejection as well as the possibilities for rectifying the errors that led to rejection. Such statement will not be given if the Bank is not allowed to give such information. If due to a lack of sufficient funds the execution of an order leads to a tolerated overdraft a higher interest rate has to be paid.

6. Account holder notification of transactions

The Bank shall inform the account holder at least once a month about the transactions executed via Berenberg Corporate Portal through the agreed account information channel and in accordance with the conditions applicable to the relevant type of order.

7. Participant's duties of care and attention

7.1 Technical connection to the online banking service Berenberg Corporate Portal The Participant shall establish the technical connection to the Berenberg Corporate Portal exclusively via the channels notified separately by the Bank (e.g. Internet address). The Customer is responsible for ensuring that he/she maintains an adequate backup for his/her own systems and always state of the art precautions against viruses and other malicious programs (such as Trojans, worms etc.). The Customer has sole responsibility to comply with the local regulations governing the use of Internet.

7.2 Secrecy of the personalised security features and safe storage of the authentication media

(1) The Participant shall

- take all reasonable precautions to keep his/her personalised security features (see No. 2.1) secret and transmit them to the Bank exclusively using the channels notified to him/her separately by the Bank for communication within the Berenberg Corporate Portal, and
- safely store his/her authentication medium (see No. 2.2) in a place where it cannot be accessed by third parties.

This is due to the fact that anyone who is in possession of the authentication medium, and also has the relevant personalised security feature, can misuse the Berenberg Corporate Portal.

(2) Particular note should be taken of the following information on the protection of the personalised security feature and the authentication medium:

- The personalised security feature »personal password« must not be stored unsecured electronically (e.g. in the Customer systems or on a mobile device) by a Participant. The electronic key generated by the Participant must remain within the sole power of disposal of the relevant Participant.
- If a so-called »Technical Participant« is acting in connection with an automatic transfer of data, the electronically stored signature of such Technical Participant is to be stored in a safe technical environment. The Technical Participant has no right to give orders on his/her own. He/she is acting solely as a transmitting agent.
- The personalised security feature is only to be entered in a manner that assures that it may not be detected by anyone else.
- The personalised security feature must not be entered on Internet pages other than the ones agreed upon separately (e.g. not on online broker websites).
- The personalised security feature must not be forwarded outside the online banking system, i.e. by e-mail, for example.
- If the electronic key is stored on a mobile device (e.g. smartphone) of the Participant, it must be ensured that unauthorised persons cannot access and use this device.
- It must be ensured that other persons cannot use the authentication instruments on the mobile device.



7.3 Checking the order data against the data shown by the Bank To the extent that the Bank shows data from the Participant's order transmitted via the Berenberg Corporate Portal (e.g. amount, creditor account number, securities identification number) to the Participant in the Customer system for confirmation, the Participant is obliged, before giving his/her confirmation, to check that the data shown corresponds to the data intended for the transaction.

7.4 Further duties of care and attention The Customer shall ensure that the duties of care under are met this agreement by the authorised representatives (ie the Participants).

8. Encryption techniques used abroad

In countries where the use, import and/or export of encryption techniques is restricted, the online-access provided by the Bank must not be used. If necessary, the Participant must arrange for the necessary permits, notices or other necessary measures. The Participant has to inform the Bank about any prohibitions, licensing and notification requirements known to him/her.

9. Disclosure and notification obligations

9.1 Blocking notice

(1) If the Participant becomes aware

- that the authentication medium is missing, has been stolen or misused, or
- that the authentication medium or personal security feature has been used without authorisation,

the Participant must notify the Bank thereof without delay (blocking notice). The Participant can also give a blocking notice to the Bank at any time using the telephone number +49 40 350 60-0.

(2) The Participant must immediately report any theft or misuse to the police.

(3) Should the Participant suspect that a third party has, without authorisation,

- gained possession of his/her authentication medium or become aware of his/her personalised security feature, or
- used the authentication medium or the personalised security feature, the Participant must also send a blocking notice.

9.2 Notification of unauthorised or incorrectly executed orders The Customer shall inform the Bank without delay on finding that an order was unauthorised or executed incorrectly.

10. Blocking

10.1 Blocking at the Participant's request At the Participant's request, particularly in the case of a blocking notice as set out in No. 9.1, the Bank will block

- the Berenberg Corporate Portal access for him/her or for all Participants, or
- his/her authentication medium.

10.2 Blocking by the Bank

(1) The Bank is authorised to block the Berenberg Corporate Portal access for a Participant in cases where

- the Bank is entitled to terminate any agreement on cooperation in cross-border and transaction business for reasonable cause,
- this appears justified on account of factual reasons relating to the security of the authentication medium or the personalised security feature, or
- unauthorised or fraudulent use of the authentication medium or the personalised security feature is suspected.

(2) The Bank will notify the Customer if possible prior to but at the latest immediately subsequent to the blocking, stating the reasons for the blocking.

10.3 Lifting the block The Bank will lift a block, or replace the personalised security feature or the authentication medium, if the reasons for the blocking are no longer given. The Bank shall notify the Customer hereof without delay.

10.4 Automatic blocking The personal password blocks itself if the password is entered incorrectly three times in succession. In this case, the Participant can contact the Bank in order to arrange for the Berenberg Corporate Portal access to be reactivated.

11. Liability in connection with the use of personalised security features and/or authentication media

11.1 Liability of the Customer for unauthorised payment transactions prior to the blocking notice

(1) If the unauthorised payment transactions prior to blocking notice pertain to use of a lost, stolen or otherwise misplaced authentication medium or other misuse of an authentication medium or a personalised security feature, the Customer is liable to the Bank for damage thus incurred if a Participant is at fault for the loss, theft or other misplacement of the authentication medium or the misuse of the authentication medium or the personalised security feature. In addition, the Customer is liable if he/she has not chosen the named Participants carefully and/or did not check regularly that such Participant did comply with the obligations under these conditions. If the Bank has contributed to the incurred damage by own fault, the principles of contributory negligence shall determine the extent to which Customer and the Bank have to bear the damage.

(2) The Customer is not obliged to compensate the damage according to paragraph 1 if the Participant was unable to submit the blocking notice in accordance with No. 9.1 due to failure of the Bank to enable receipt of the blocking notice and if the damage was incurred thereby.

(3) The liability for damages is restricted to the agreed transaction limit, if the incurred damage was caused within the period for which the transaction limit applies.

11.2 Liability for unauthorised transactions other than payment transactions prior to the blocking notice

If unauthorised transactions other than payment transactions prior to the blocking notice pertain to use of a lost or stolen or otherwise misplaced authentication medium or other misuse of the personalised security feature or the authentication medium and if the Bank suffers a loss as a result, the Customer is liable to the Bank for damage thus incurred if a Participant is at fault for the loss, theft or other misplacement of the authentication medium or the misuse of the authentication medium or the personalised security feature. In addition, the Customer is liable if he/she has not chosen the named Participants carefully and/or did not check regularly that such Participant did comply with the obligations under these conditions. If the Bank has contributed to the incurred damage by own fault, the principles of contributory negligence shall determine the extent to which Customer and the Bank have to bear the damage.

11.3 Liability of the Bank as from the blocking notice As soon as the Bank has received a blocking notice from a Participant, it shall assume all losses arising after this time as a result of unauthorised online banking transactions. This does not apply if the Participant acted with fraudulent intent.

12. Availability

The Bank aims to keep the services offered under the Berenberg Corporate Portal widely available. However, the availability shall not be guaranteed. In particular, due to technical problems, maintenance works or network problems (such as non-availability of third-party servers) out of the Bank's control, may cause temporary disruptions that prevent access.

13. Reference to third party websites

If the Berenberg Corporate Portal website enables access to the third party websites, this is only to allow the Participants to access information on the Internet easily. The contents of such pages do not represent the Bank's own statements; they are not checked by the Bank.

14. Right of use

The Customer is not entitled by this agreement to set links or frame links on his/her website without the prior written consent of the Bank. The Customer undertakes to use the website and its contents solely for his/her personal use. In particular, the Customer is not entitled without the prior consent to share the contents with third parties, to embed such contents into other products or processes or to discover the source code of the websites. References to rights of the Bank or third parties may not be deleted or made illegible. The Customer will not use trademarks, domain names and other marks of the Bank or third parties without the prior consent of the Bank. Under these terms and conditions the Bank does not grant any irrevocable, exclusive and transferable rights of use.

15. Hotline (»Helpdesk«)

The Bank offers a telephone hotline (so-called »help desk«) for answering questions about the technology, operation and functionality offered in the Berenberg Corporate Portal services. The hotline which is available on German banking days at telephone number +49 40 350 60-788.