The following translation is provided for the customer's convenience only. The contractual language is German. Therefore, German legal documents are binding in all respects and constructions, meanings or interpretations in the German legal documents shall prevail in case of inconsistency with the English version.

Further information about the bank is contained in the "List of prices and services".

Terms and conditions for online banking and telephone

1. Range of services

(1) The customer and his authorized representatives may conduct banking transactions by means of online banking and telephone banking to the extent offered by the bank. They can also call up information from the bank via online and telephone banking. Furthermore, with regard to online banking, in accordance with Section 675f (3) of the German Civil Code (BGB), they are entitled to use payment initiation services and account information services in accordance with Section 1 (33) and (34) of the Payment Services Supervision Act (ZAG). In addition, they can use other third-party services selected by them.

(2) Customer and authorized representative shall be uniformly referred to as "Participant", account and custody account uniformly as "Account", unless expressly stated otherwise.

(3) For the use of online and telephone banking, the disposal limits separately agreed with the bank apply.

2. Requirements for using online and telephone banking

(1) The participant can use online and telephone banking if the bank has authenticated him.

(2) Authentication is the procedure agreed separately with the Bank by means of which the Bank can verify the identity of the Participant or the authorised use of an agreed payment instrument, including the use of the Participant's personalised security feature. With the

authentication elements agreed for this purpose, the participant can identify himself to the bank as an authorised participant, access information (see point 3 of these conditions) and place orders (see point 4 of these conditions).

(3) Authentication elements are

- Knowledge elements, i.e. something that only the participant knows (e.g. personal identification number (PIN)),
- Possession elements, i.e. something that only the participant possesses (e.g. a device for generating or receiving one-time transaction numbers (TAN) that prove the subscriber's ownership, such as the girocard with TAN generator or the mobile device), or
- Elements of being, i.e. something that the participant is (inherence, e.g. fingerprint as a biometric feature of the participant).

(4) The authentication of the participant shall be carried out by the participant submitting to the bank the knowledge element, the proof of the possession element and/or the proof of the element of being in accordance with the bank's request.

3. Access to online and telephone banking

(1) The participant shall have access to the bank's online banking and telephone banking if:

- they enter their individual participant ID (e.g. account number, registration name) and
- identify themselves using the authentication element(s) required by the bank, and
- there is no blocking of access (see points 8.1 and 9 of these conditions).

After access to online and telephone banking has been granted, information can be accessed or orders can be placed in accordance with No. 4 of these Terms and Conditions.

(2) For access to sensitive payment data within the meaning of Section 1 (26) sentence 1 ZAG (e.g. for the purpose of changing the customer's address), the Bank shall request the subscriber to identify himself using an additional authentication element if only one authentication element is requested when accessing Online Banking.became. The name of the account holder and the account number are not sensitive payment data for the payment initiation service and account information service used by the participant (Section 1 (26) sentence 2 ZAG).

4. Orders

4.1. Placing an order

(1) The participant must agree to an order (e.g. bank transfer) in order to be effective (authorisation). Upon request, he must use authentication elements (e.g. entering a TAN as proof of the possession element). The bank confirms receipt of the order via online banking.

(2) The participant can only issue telephone banking orders after successful authorization with the personalized security feature provided by the Bank. The Bank confirms receipt of the order via the access channel selected by the participant for the order. The telephone communication transmitted between the Bank and the account holder is automatically recorded and stored for evidence purposes.

4.2. Revocation of orders

The revocability of an order is based on the special conditions applicable to the respective order type (e.g. conditions for transfer transactions). Orders can only be revoked outside of online and telephone banking, unless the bank expressly provides for a revocation option in online and telephone banking.

5. Processing of orders by the bank

(1) Orders shall be processed on the business days announced for the processing of the respective type of order (e.g. bank transfer) on the Bank's online banking website or in the

"List of Prices and Services" within the framework of the proper course of work. If the order is received after the time specified on the Bank's online banking page or in the "List of Prices and Services" (acceptance period), or if the time of receipt does not fall on a business day according to the Bank's online banking page or the Bank's "List of Prices and Services", the order shall be deemed to have been received on the following business day. Processing does not begin until that business day.

(2) The Bank shall execute the order if the following conditions of execution are met:

- The participant has authorised the order (see point 4.1 of these conditions).
- The participant is authorised to carry out the respective order type (e.g. securities order).
- The online banking data format is adhered to.
- The separately agreed online and telephone banking disposal limit has not been exceeded (cf. No. 1 paragraph 3 of these Terms and Conditions).
- The other execution conditions in accordance with the special conditions applicable to the respective type of order (e.g. sufficient account funds in accordance with the conditions for transfer transactions) are in place.

If the execution conditions pursuant to sentence 1 are met, the Bank shall execute the orders in accordance with the provisions of the special conditions applicable to the respective type of order (e.g. conditions for credit transfers, conditions for securities transactions).

(3) If the execution conditions pursuant to subsection (2) sentence 1 are not met, the Bank shall not execute the order. It will provide information to the participants via online or telephone banking and, as far as possible, indicate the reasons and the possibilities by which errors that have led to the rejection can be corrected.

6. Informing the customer about online and telephone banking - dispositions

The term of the overdraft credit is not limited and is granted until further notice. With the termination of the current account agreement, the overdraft credit shall also end accordingly.

7. Participant's duties of care

7.1. Protecting the Authentication Elements

(1) The participant must take all reasonable precautions to protect his authentication elements (see number 2 of these conditions) from unauthorized access. Otherwise, there is a risk that online and telephone banking will be misused or otherwise used in an unauthorised manner (see numbers 3 and 4 of these conditions).

(2) In order to protect the individual authentication elements, the participant must pay particular attention to the following:

a. Elements of knowledge, such as the PIN, must be kept secret; in particular, they must be

- are not outside of online banking communicated orally (e.g. by telephone or in person),
- are not passed on in text form (e.g. by e-mail, messenger service) outside of online banking,
- are not stored electronically in an unsecured manner (e.g. storage of the PIN in plain text on the computer or mobile device) and
- are not recorded on a device or stored as a copy together with a device that serves as a possession element (e.g. girocard with TAN generator, mobile device, signature card) or for verification of the element of being (e.g. mobile device wit

b. Possession elements, such as the girocard with TAN generator or a mobile device, must be protected against misuse, in particular

- the girocard with TAN generator or the signature card must be kept safe from unauthorised access by other persons,
- ensure that unauthorised persons cannot access the participant's mobile device (e.g. mobile phone),
- ensure that other persons cannot use the online banking application (e.g. online banking app, authentication app) located on the mobile device (e.g. mobile phone),
- the application for online banking (e.g. online banking app, authentication app) must be deactivated on the

participant's mobile device before the participant gives up possession of this mobile device (e.g. by selling or disposing of the mobile phone),

- Proof of ownership (e.g. TAN) may not be passed on outside online banking orally (e.g. by telephone) or in text form (e.g. by e-mail, messenger service) outside of online banking, and
- the subscriber who has received a code from the bank to activate the possession element (e.g. mobile phone with application for online banking) must keep it safe from unauthorised access by other persons; otherwise, there is a risk that other persons will activate their device as a possession element for the participant's online banking.

c. Elements of being, such as the participant's fingerprint, may only be used as an authentication element on a participant's mobile device for online banking if no other persons' elements of being are stored on the mobile device. If other people's elements of being are stored on the mobile device used for online banking, the knowledge element issued by the bank (e.g. PIN) must be used for online banking and not the element of being stored on the mobile device.

(3) In the case of the mobileTAN procedure, the mobile device with which the TAN is received (e.g. mobile phone) may not be used for online banking at the same time.

(4) The telephone number stored for the mobile TAN procedure shall be deleted or changed if the subscriber no longer uses this telephone number for online banking.

(5) Notwithstanding the duties of protection under paragraphs 1 to 4, the subscriber may use its authentication elements vis-à-vis a payment initiation service and account information service selected by it as well as another third-party service (see number 1 paragraph 1 sentences 3 and 4 of these conditions). The subscriber must select other third-party services with the care required in traffic.

7.2. Security instructions from the bank

The participant must observe the security instructions on the bank's online banking page, in particular the measures taken to protect the hardware and software used (customer system).

7.3. Verification of order data with data displayed by the bank

The bank will display the order data it has received (e.g. amount, account number of the payee, securities identification number) to the participant via the participant's separately agreed device (e.g. by means of a mobile device, chip card reader with display). The Participant is obliged to check the correspondence of the displayed data with the data intended for the order before confirming.

8. Notification and notification obligations

8.1. Lock Indicator

(1) If the participant

- the loss or theft of a possession element for authentication (e.g. girocard with TAN generator, mobile device, signature card) or
- If the misuse or other unauthorised use of an authentication element is detected, the participant must inform the bank of this immediately (blocking notice). The participant can also submit such a blocking notice at any time via the separately communicated communication channels.

(2) The participant must immediately report any theft or misuse of an authentication element to the police.

(3) If the participant suspects an unauthorised or fraudulent use of one of its authentication elements, it must also submit a blocking notice.

8.2. Notification of Unauthorized or Incorrectly Executed Orders

The Client shall inform the Bank of this immediately upon discovery of an unauthenticated or incorrectly executed order.

9. Suspension of use

9.1. Blocking at the instigation of the participant

The Bank shall block at the instigation of the Participant, in particular in the case of the blocking notice pursuant to Section 8.1 of these Terms and Conditions,

- the online banking access for him or all participants, or
- its authentication elements for the use of online banking.

9.2. Blocking at the instigation of the bank

(1) The Bank may suspend online and telephone banking access for a Participant if:

- they are entitled to terminate the online and telephone banking contract for good cause,
- objective reasons related to the security of the participant's authentication elements justify it, or
- there is a suspicion of unauthorized or fraudulent use of an authentication element.

(2) The Bank shall inform the Client by the agreed means, stating the relevant reasons for this, if possible before, but no later than immediately after the severance. The statement of reasons may be omitted if the bank would thereby violate statutory obligations.

9.3. Lifting the Suspension

The bank will lift a block or replace the affected authentication elements if the reasons for the block no longer apply. It shall inform the customer of this without delay.

9.4. Automatic locking of a chip-based possession element

(1) A chip card with a signature function blocks itself if the usage code for the electronic signature is entered incorrectly three times in a row.
(2) A TAN generator as part of a chip card that requires the entry of its own usage code will block itself if it is entered incorrectly three times in a row.
(3) The ownership elements referred to in subsections (1) and (2) can then no longer be used for online banking. The participant can contact the bank to restore the possibilities of using online banking.

9.5. Access Blocking for Payment Initiation Service and Account Information Service

The Bank may deny access to a customer's payment account to account information service providers or payment initiation service providers if objective and duly substantiated reasons relating to unauthorised or fraudulent access to the payment account by the account information service provider or payment initiation service provider, including the unauthorised or fraudulent initiation of a payment transaction, justify it. The Bank will inform the Client of such a refusal of access by the agreed means. Information shall be provided as far as possible before and at the latest immediately after the refusal of access. The statement of reasons may be omitted if the bank would thereby violate legal obligations. As soon as the reasons for denying access no longer exist, the bank lifts the access block. It shall inform the customer of this without delay.

10. Liability

10.1. Liability of the Bank in the event of the execution of an unauthorised order and an order that has not been executed, has been executed incorrectly or has been executed late.

The Bank's liability in the event of an unauthorised order and an order that is not executed, executed incorrectly or is executed late is governed by the special conditions agreed for the respective type of order (e.g. conditions for transfer transactions, conditions for securities transactions).

10.2. Liability of the Customer in the event of improper use of its authentication elements

10.2.1. Liability of the customer for unauthorized payment transactions prior to the blocking notice

(1) If unauthorised payment transactions prior to the blocking notice are based on the use of a lost, stolen or otherwise lost authentication element or on the other misuse of an authentication element, the customer shall be liable for the damage incurred by the bank as a result up to an amount of EUR 50, regardless of whether the participant is at fault.

(2) The customer shall not be obliged to compensate for the damage pursuant to subsection (1) if:

- it was not possible for him to notice the loss, theft, loss or other misuse of the authentication element before the unauthorized payment transaction, or

- the loss of the authentication element has been caused by an employee, an agent, a branch of a payment service provider or any other entity to which the payment service provider's activities have been outsourced.

(3) If unauthorized payment transactions occur prior to the blocking notice and the participant has acted fraudulently or violated his duties of care and disclosure under these Terms and Conditions intentionally or through gross negligence, the Customer shall bear the resulting damage in full, in derogation from paragraphs 1 and 2. Gross negligence on the part of the participant may exist in particular if he or she has fulfilled one of his duties of care according to

- point 7.1 paragraph 2,
- point 7.1 paragraph 4,
- point 7.3 or
- has violated Section 8.1 (1) of these Terms.

(4) By way of derogation from subsections 1 and 3, the customer shall not be obliged to pay compensation for damages if the bank has not required the subscriber to provide strong customer authentication within the meaning of Section 1 (24) ZAG. In particular, strong customer authentication requires the use of two independent authentication elements from the categories of knowledge, possession or being (see number 2 paragraph 3 of these conditions).

(5) Liability for damages caused within the period for which the disposal limit applies shall be limited to the agreed disposal limit.

(6) The customer shall not be obliged to compensate for the damage pursuant to subsections 1 and 3 if the participant was unable to submit the blocking notice pursuant to number 8.1 of these Terms and Conditions because the bank had not ensured the possibility of receiving the blocking notice.

(7) 2 and 4 to 6 shall not apply where the participant has acted fraudulently.

(8) If the customer is not a consumer, the following shall apply in addition:

- The customer is liable for damages due to unauthorized payment transactions beyond the liability limit of 50 euros according to paragraphs 1 and 3 if the participant has negligently or

intentionally violated his notification and due diligence obligations under these conditions.

- The limitation of liability in the first indent of paragraph 2 does not apply.

10.2.2. Liability of the customer in the event of unauthorized dispositions outside payment services (e.g. securities transactions) prior to the blocking notice

If unauthorised dispositions outside of payment services (e.g. securities transactions) are based on the use of a lost or stolen authentication element or on the other misuse of the authentication element prior to the blocking notice, and the Bank has suffered damage as a result, the customer and the Bank shall be liable in accordance with the statutory principles of contributory negligence.

10.2.3. Liability from the blocking notice

As soon as the bank has received a blocking notice from a participant, it will cover all subsequent damages caused by unauthorized online and telephone banking arrangements. This does not apply if the participant has acted fraudulently.

10.2.4. Disclaimer

Liability claims are excluded if the circumstances giving rise to a claim are based on an unusual and unforeseeable event over which the party invoking this event has no influence, and the consequences of which could not have been avoided by the party despite exercising due care.