YapıKredi Deutschland

More detailed information on the Bank can be found in the "List of Prices and Services".

# Conditions for online banking

## 1 Range of services

(1) The customer and his authorized representative can carry out banking transactions via Online Banking to the extent offered by the Bank. They can also retrieve information from the Bank via online banking. Furthermore, in accordance with Section 675f (3) BGB, they are entitled to use payment initiation services and account information services in accordance with Section 1 (33) and (34) of the German Payment Services Supervision Act (Zahlungsdiensteaufsichtsgesetz - ZAG). In addition, they may use other third-party services selected by them.

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

(3) For the use of Online Banking, the disposal limits agreed separately with the Bank apply.

## 2 Requirements for using the online banking

(1) The Participant can use Online Banking if the bank has authenticated him/her.

(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 authorized use of an agreed payment instrument, including the use of the Participant's personalized security token. With the authentication elements agreed for this purpose, the Participant can identify himself to the Bank as an authorized Participant, access information (see Section 3 of these Terms and Conditions) and place orders (see Section 4 of these Terms and 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 subscriber possesses (e.g. device for generating or receiving one-time transaction numbers (TAN) that prove the possession of the subscriber, 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 characteristic of the Participant).

(4) The Participant is authenticated by transmitting the knowledge element, the proof of possession element and/or the proof of existence element to the Bank as requested by the Bank.

## 3 Access to online banking

(1) The Participant receives access to the Bank's Online Banking if
- he provides his individual participant identification (e.g. account number, registration name) and
- he/she shall register using the form(s) requested by the Bank. authentication element(s) and
- access is not blocked (see sections 8.1 and 9 of these terms and conditions).

Once access to Online Banking has been granted, information can be accessed, or orders can be placed in accordance with section 4 of these Terms and Conditions.

(2) For access to sensitive payment data within the meaning of Section 1 (26) sentence 1 Payment Services Oversight Act (Zahlungsdiensteaufsichtsgesetz – ZAG) (e.g. for the purpose of changing the customer's address), the Bank will ask the Participant to identify him/herself using an additional authentication element if only one authentication element was requested when accessing online banking. 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

The Participant must approve to an order (e.g. bank transfer) for it to be effective (authorization). On request, they must use authentication elements (e.g. entering a TAN as proof of ownership).
The bank confirms receipt of the order via online banking.

### 4.2 Revocation of orders

The revocability of an order is governed by the special conditions applicable to the respective order type (e.g. conditions for credit transfers). Orders can only be revoked outside of Online Banking unless the Bank expressly provides for a revocation option in.

## 5 Processing of orders by the bank

(1) Orders shall be processed on the business days specified for the processing of the respective order type (e.g. bank transfer) on the Bank's online banking page or in the "List of Prices and Services" as part of the normal course of business. 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 as specified on the Bank's online banking page or in the Bank's "List of Prices and Services", the order shall be deemed to have been received on the following business day. Processing shall only begin on this business day.

(2) The bank will execute the order if the following execution conditions are met:
- The Participant has authorized the order (see section 4.1 of these Terms and Conditions).
- The Participant is authorized for the respective order type (e.g. securities order).
- The online banking data format is complied with.
- The separately agreed online banking disposal limit has not been exceeded (cf. No. 1 (3) of these conditions).
- The other execution conditions in accordance with the special conditions applicable to the respective order type (e.g. sufficient account coverage in accordance with the conditions for credit transfers) have been met.

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

(3) If the execution conditions pursuant to paragraph 2 sentence 1 are not met, the Bank shall not execute the order. It shall provide the Participant with information on this via Online Banking and, as far as possible, state the reasons and options for correcting errors that led to the rejection.

## 6 Informing the customer about online banking transactions

The Bank shall inform the customer at least once a month about the transactions carried out via Online Banking in the manner agreed for account information.

## 7 Duty of care of the participant

### 7.1 Protection of the authentication elements

(1) The Participant must take all reasonable precautions to protect his/her authentication elements (see Section 2 of these Terms and Conditions) from unauthorized access. Otherwise, there is a risk that Online Banking may be misused or used in any other unauthorized manner (see sections 3 and 4 of these Terms and Conditions).

(2) To protect the individual authentication elements, the participant must pay particular attention to the following:
(a) Knowledge elements, such as the PIN, must be kept secret; they may in particular
- not be communicated verbally (e.g. by telephone or in person),
- not be passed on outside of online banking in text form (e.g. by e-mail, messenger service),
- are not stored unsecured electronically (e.g. storage of the PIN in plain text on the computer or mobile device) and
- not be noted on a device or kept as a copy together with a device that serves as a possession element (e.g. girocard with TAN generator, mobile terminal device, signature card) or for checking the being element (e.g. mobile terminal device with application for online banking and fingerprint sensor).

(b) Possession elements, such as the girocard with TAN generator or a mobile device, must be protected against misuse, in particular
- are the girocard with TAN generator or the signature card before from unauthorized access by other persons,
- it must be ensured that unauthorized persons cannot access the subscriber's mobile device (e.g. cell phone),
- it must be ensured that other persons cannot use the online banking application (e.g. online banking app, authentication app) on the mobile device (e.g. cell phone)
- the application for online banking (e.g. online banking app, authentication app) must be deactivated on the subscriber's mobile device before the subscriber gives up possession of this mobile device (e.g. by selling or disposing of the cell phone),
- the evidence of the possession element (e.g. TAN) may not be

passed on verbally (e.g. by telephone) or in text form (e.g. by e- mail, messenger service) outside of online banking and
- the Participant who has received a code from the Bank to activate the possession element (e.g. cell phone with application for online banking) must keep it safe from unauthorized 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) Being elements, such as the Participant's fingerprint, may only be used as an authentication element on the Participant's mobile device for online banking if no being elements of other persons are stored on the mobile device. If the mobile device used for online banking has being elements of other persons stored on it, the knowledge element issued by the Bank (e.g. PIN) must be used for online banking and not the being element stored on the mobile device.

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

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

(5) Notwithstanding the protection obligations under paragraphs 1 to 4, the Participant may use his authentication elements with a payment initiation service and account information service selected by him as well as with another third-party service (see number 1 paragraph 1 sentences 3 and 4 of these conditions). The Participant must select other third-party services with the care required in the course of transactions.

### 7.2 Security information from the bank

The Participant must observe the security instructions on the Bank's online banking site, in particular the measures to protect the hardware and software used (customer system).

### 7.3 Checking the order data with data displayed by the bank

The Bank shall 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 that the data displayed matches the data intended for the order before confirming.

## 8 Notification and information obligations

### 8.1 Block indicator

(1) If the Participant discovers
- the loss or theft of a possession element for authentication (e.g. girocard with TAN generator, mobile device, signature card) or
- the improper use or other unauthorized use of the data

the Participant must inform the Bank of this immediately (blocking notification). The Participant may also submit such a blocking notification at any time via the separately notified communication channels.

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

(3) If the subscriber suspects unauthorized or fraudulent use of one of his authentication elements, he must also submit a blocking notification.

### 8.2 Notification of unauthorized or incorrectly executed orders

The customer must inform the Bank immediately after discovering an order that has not been executed or has been executed incorrectly.

## 9 Usage block

### 9.1 Blocking at the instigation of the participant

The Bank shall block at the request of the Participant, in particular in the event of a blocking notification in accordance with 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 block online banking access for a participant if
- it is entitled to terminate the online banking agreement for good cause,
- objective reasons in connection with the security of the participant's authentication elements justify this,
- or the suspicion of unauthorized or fraudulent use of the use of an authentication element.

(2) The Bank shall inform the customer by the agreed means, stating the relevant reasons, if possible before, but at the latest immediately after the blocking. Reasons may not be given if this would result in the Bank breaching its statutory obligations.

### 9.3 Removing the block

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

### 9.4 Automatic blocking of a chip-based possession element

(1) A chip card with signature function locks itself if the usage code for the electronic signature is entered incorrectly three times in succession.

(2) A TAN generator as part of a chip card, which requires the entry of its own user code, blocks itself if this is entered incorrectly three times in succession.

(3) The possession elements referred to in paragraphs 1 and 2 can then no longer be used for Online Banking. The Participant may contact the Bank in order to restore the possibility of using Online Banking.

### 9.5 Access block for payment initiation service and account information service

The Bank may deny account information service providers or payment initiation service providers access to a payment account of the customer if objective and duly substantiated reasons relating to unauthorized or fraudulent access to the payment account by the account information service provider or payment initiation service provider, including the unauthorized or fraudulent initiation of a payment transaction, so justify. The Bank shall inform the customer of such a refusal of access by the agreed means. The notification shall be made if possible before, but at the latest immediately after, the refusal of access. No reasons may be given if this would result in the Bank breaching its legal obligations. As soon as the reasons for refusing access no longer exist, the Bank shall lift the access block. It shall inform the customer of this without delay.

## 10 Liability

### 10.1 Liability of the bank for the execution of an unauthorized order and an order that is not executed, executed incorrectly or executed late

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

### 10.2 Liability of the customer in the event of misuse of its authentication elements

#### 10.2.1 Liability of the customer for unauthorized payment transactions prior to the blocking notification

(1) If unauthorized payment transactions prior to the blocking notification are based on the use of a lost, stolen or otherwise misappropriated authentication element or on the misuse of an authentication element in any other way, the customer shall be liable for the loss incurred by the Bank as a result up to an amount of EUR 50, irrespective of whether the Participant is at fault.

(2) The customer is not obliged to compensate the damage in accordance with paragraph 1 if
- it was not possible for him/her to notice the loss, theft, misplacement or other misuse of the authentication element before the unauthorized payment transaction, or
- the loss of the authentication element was caused by an employee, an agent, a branch of a payment service provider or another entity to which the payment service provider's activities have been outsourced.

(3) If unauthorized payment transactions are made prior to the blocking notification and if the Participant has acted fraudulently or breached his/her duties of care and notification under these Terms and Conditions intentionally or through gross negligence, the customer shall bear the full extent of the resulting loss, notwithstanding paragraphs 1 and 2. Gross negligence on the part of the participant may be deemed to exist in particular if he fails to fulfill one of his duties of care under these terms and conditions.
- Number 7.1 paragraph 2,
- Number 7.1 paragraph 4,
- Number 7.3 or
- Section 8.1 paragraph 1 of

these terms and conditions.

(4) By way of derogation from paragraphs 1 and 3, the customer shall not be obliged to pay compensation if the Bank has not required the Participant to provide strong customer authentication within the meaning of Section 1 (24) ZAG. Strong customer authentication requires in particular 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 losses caused within the period for which the withdrawal limit applies is limited to the agreed withdrawal limit.

(6) The customer is not liable to pay compensation for the damage in accordance with paragraphs 1 and 3. if the subscriber has given the blocking notification in accordance with section 8.1 of these conditions because the bank had not ensured the possibility of receiving the blocking notice.

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

(8) If the customer is not a consumer, the following shall also apply:
- The customer shall be liable for losses due to unauthorized payment transactions in excess of the liability limit of EUR 50 in accordance with paragraphs 1 and 3 if the participant has negligently or intentionally breached its duties of disclosure and due diligence in accordance with these terms and conditions.
- The limitation of liability in paragraph 2, first indent, applies to no application.

#### 10.2.2 Liability of the customer for unauthorized

**transactions outside of payment services (e.g. securities transactions) prior to the blocking notification**

If unauthorized dispositions outside of payment services (e.g. securities transactions) are based on the use of the payment service prior to the blocking notification.

If the loss or theft of an authentication element or any other misuse of the authentication element causes damage to the Bank, the customer and the Bank shall be liable in accordance with the statutory principles of contributory negligence.

### 10.2.3 Liability from the blocking notification

As soon as the Bank has received a blocking notification from a Participant, it shall assume all subsequent losses arising from unauthorized online banking transactions. 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 it despite exercising due care.