

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.

Please refer to the "Schedule of Fees and Services" for further information about the bank.

## Conditions for the girocard (debit card)

### A. Guaranteed payment methods

#### I. Scope

The girocard issued by the bank is a debit card (hereinafter referred to as the "card"). The cardholder can use the card, provided it is appropriately equipped, for the following payment services.

##### **1. In connection with the personal identification number (PIN) in German debit card systems**

- a) To withdraw cash at ATMs that are part of the German ATM system and marked with the girocard logo.
- b) For use at automated checkouts in retail and service companies that are labeled with the girocard logo and are part of the German girocard system (girocard terminals).

\* The text in italics is only relevant if a digital card has been issued.

c) To top up a cash card at terminals marked with the cash card (GeldKarte) logo.

d) To top up a prepaid mobile phone account held by a mobile phone user with a mobile phone provider at an ATM, provided that the ATM operator offers this function and the mobile phone provider participates in the system.

## **2. In conjunction with the personal identification number (PIN) in foreign debit card systems**

a) To withdraw cash at ATMs within a third-party ATM system, provided that the card is equipped for this.

b) For use at automated checkouts in retail and service companies as part of a third-party system, provided that the card is equipped accordingly.

c) To top up a prepaid mobile phone account that a mobile phone user has with a mobile phone provider at the ATM of a third-party system, provided that the ATM operator offers this function and the mobile phone provider participates in the system.

The acceptance of the card in the context of a third-party system is subject to the acceptance logo applicable to the third-party system.

## **3. Without the use of a personal identification number (PIN)**

\* The text in italics is only relevant if a digital card has been issued.

- a) For contactless use at automated checkouts of retail and service companies that are part of the German girocard system and marked with the girocard logo, up to €50 per payment transaction, provided that a PIN is not required for the respective contactless use at the automated checkouts.
- b) For contactless use at the automated checkouts of retail and service companies as part of third-party debit card systems, up to €50 per payment transaction, provided that a PIN is not required for the respective contactless use at the automated checkouts. The acceptance of the card in the context of a third-party system is subject to the acceptance logo applicable to the third-party system.
- c) For use in electronic remote payment transactions via the internet at retail and service companies (online retailing). When used for online retail, the respective special authentication procedure intended for online retail is used instead of the PIN.
- d) As a GeldKarte for cashless payments at automated cash registers in the retail and service sectors in Germany that are marked with the GeldKarte logo (GeldKarte terminals).
- e) Aside from the provision of payment services and with no guarantee from the bank associated with the function,

\* The text in italics is only relevant if a digital card has been issued.

- the account will be debited in euros regardless if the card is used for transactions not denominated in euros or
- as a storage medium for the bank's additional applications in accordance with the contract concluded with the bank (bank-generated additional application).

## II. General Rules

### 1. Issuing the card

The card can be issued as a physical card or as a digital card for storage on a telecommunications, digital or IT device (mobile device). These special conditions apply equally to both card types, unless otherwise expressly stated. The terms of use for the digital card, which have been agreed separately with the bank, also apply to the digital card.

### 2. Cardholder and power of attorney

The card is valid for the account indicated on it. It can only be issued in the name of the account holder or a person whom the account holder has authorised to operate the account. If the account holder revokes the account authorisation, he is responsible for ensuring that the card issued to the authorised representative is returned to the bank. The bank will electronically block the card after revoking

\* The text in italics is only relevant if a digital card has been issued.

the power of attorney for use within the girocard system and for topping up the cash card. A company-generated additional application can only be blocked by the company that has stored the additional application on the chip of the card, and this is only possible if the company has provided for the option of blocking its additional application. The blocking of an additional Bank-generated application of the Bank can only be considered vis-à-vis the Bank and is governed by the contract concluded with the Bank. As long as the card has not been returned, there is a possibility that it may continue to be used to spend the amounts still stored on the cash card. It is also still possible to use the additional applications stored on the card.

### **3. Financial usage limit**

The cardholder may only make withdrawals with his card within the limits of the account balance or a credit facility previously granted for the account. Even if the cardholder does not comply with this spending limit, the bank is entitled to demand compensation for expenses incurred as a result of the card use. Posting such dispositions to the account results in a tolerated overdraft.

### **4. Conversion of foreign currency amounts**

If the cardholder uses the card for transactions not denominated in euros, the account will nevertheless be debited in euros. The determination of the exchange rate for foreign currency transactions is based on the "Price and Service List". Any change to the reference exchange rate specified in the

\* The text in italics is only relevant if a digital card has been issued.

conversion regulation will take effect immediately and without prior notification to the customer.

## 5. Return of the card

The card remains the property of the bank. It is not transferable. The card is only valid for the period specified on the card.

When the new card is issued, but no later than the expiry date of the card, the bank is entitled to demand the return of the old card; *alternatively, it can request that the digital card be deleted or arrange for it to be deleted itself\**. If the authorisation to use the card ends before this (e.g. due to the termination of the account or the card contract), the cardholder must return the card to the bank immediately *or delete the digital card\**. Any amount still stored on the cash card at the time of its return will be refunded to the cardholder. The cardholder must immediately remove any additional company-generated applications stored on the card from the company that has stored the additional application on the card. The possibility of continuing to use a bank-generated additional application depends on the contractual relationship between the cardholder and the bank.

## 6. Blocking and confiscation of the card

(1) The bank may block the card and arrange for it to be confiscated (e.g. at ATMs), or request that the digital card be deleted or *arrange for it to be*

\* The text in italics is only relevant if a digital card has been issued.

*deleted itself*\*,

- If it is entitled to terminate the card contract for good cause,
- If objective reasons relating to the security of the card justify this or
- If there is suspicion of unauthorised or fraudulent use of the card.

The bank will inform the account holder of this, stating the relevant reasons for doing so, if possible before the account is blocked or *closed*\* and at the latest immediately thereafter. The bank will unblock the card or replace it with a new card if the reasons for blocking no longer apply. The cardholder shall be informed of this without delay.

(2) Any amounts still stored on the cash card at the time of its withdrawal will be refunded to the cardholder.

(3) If the card for online banking has a TAN generator or a signature function, blocking the card will also result in blocking online banking access.

(4) If the cardholder has stored an additional application on a card that is withdrawn, the withdrawal of the card means that he can no longer use the additional application. The cardholder may request from the card-issuing institution company-generated additional applications stored on the card at the time of its withdrawal, once the card-issuing institution has received the card from the party that withdrew it. The

\* The text in italics is only relevant if a digital card has been issued.

Bank is entitled to meet the request for release of the company-generated additional applications by issuing the cardholder with the card stripped of its payment transaction functions. The possibility of continued use of a bank-generated additional application is governed by the rules applicable to that additional application.

## **7. Duty of care and cooperation of the cardholder**

### **7.1 Signature**

If the card has a signature field, the cardholder must sign the card in the signature field immediately after receiving it.

### **7.2 Safekeeping of the card**

The card must be stored with particular care to prevent it from being lost or misused. In particular, it must not be left unattended in a motor vehicle, as it may be misused (e.g. within the framework of the girocard system). Furthermore, anyone in possession of the card can, for example, use up the amount stored on the cash card and carry out transactions at automated checkouts without a PIN until the card is blocked or *deleted*\*.

### **7.3 Confidentiality of the personal identification number (PIN)**

The cardholder must ensure that no other person gains knowledge of the personal identification number (PIN). In particular, the PIN must not be written on the card, *and in the case of a digital card, it must not be stored in the mobile device or in another communication device\** or otherwise kept together with it. This is because anyone who knows the PIN and comes into possession of the card can make transactions at the expense of the

\* The text in italics is only relevant if a digital card has been issued.



account indicated on the card (e.g. withdraw money from ATMs). *If the cardholder uses a digital card and access to the mobile device or another communication device can be secured by an authentication medium selected by the cardholder, the cardholder may not use the same PIN to secure access as is required for using the debit card.\**

## 7.4 Information and notification obligations

(1) If the cardholder discovers that his card, *mobile device with digital card\**, has been lost or stolen, or that the PIN has been misused or otherwise used without authorisation, the bank must be notified immediately (blocking notification), if possible to the account-holding branch. The cardholder can also submit the blocking notification to the Central Blocking Service at any time (Tel. 116 116 from within Germany and +49 116 116 from abroad). In this case, a card can only be blocked if the name of the bank and the IBAN are provided. The central blocking service blocks all cards issued for the account in question from further use at ATMs and electronic cash terminals. To limit the block to the lost card, the cardholder must contact their bank. The contact details under which a blocking notice can be submitted will be communicated separately to the cardholder. The cardholder must report any theft or misuse to the police immediately.

(2) If the cardholder suspects that another person has gained unauthorised possession of his card, or that the card or PIN are being

\* The text in italics is only relevant if a digital card has been issued.

misused or otherwise used without authorisation, he must also submit a blocking request immediately.

(3) When special authentication procedures are used in online retail in accordance with Section 8, sentence 3, the cardholder must check that the transaction data provided for authentication (e.g. payment amount, date) matches the data intended for the transaction prior to authorisation. If any discrepancies are detected, the transaction must be cancelled and the suspicion of unauthorised use reported to the bank.

(4) For the replacement of a lost, stolen, misused or otherwise unauthorised card, the bank shall charge the account holder the fee shown in the bank's 'Price and Service List', which covers only the costs directly and exclusively associated with the replacement. Sentence 1 shall not apply if the Bank is responsible for the circumstances that led to the replacement card being issued or if these are attributable to it.

(5) If the card is used for online banking, a TAN generator or signature function is also included, blocking the card will also block online banking access.

(6) *Blocking the card with the bank or the central card-blocking service does not block access to the mobile device. Blocking of other functions on the mobile device can only be done by contacting the respective provider of these functions.\**

(7) A company that has stored an additional company-generated application on the chip of the card is solely responsible for ensuring that

\* The text in italics is only relevant if a digital card has been issued.

the application is blocked. This is only possible if the company has provided the option for blocking its additional application. The blocking of an additional bank-generated application can only be considered by the bank and is based on the contract concluded with the bank.

(8) The account holder must notify the bank immediately upon discovering any unauthorised or incorrectly executed card transactions.

## **8. Authorisation of card payments by the cardholder**

By using the card, the cardholder authorises the execution of the card payment. If an additional PIN is required for this, consent is only granted when the PIN is used. When using a debit card for online shopping, the special authentication procedures provided for this purpose are to be used. Once consent has been given, the cardholder can no longer revoke the card payment. The authorisation also includes the express consent for the bank to process, transmit and store the cardholder's personal data required for the execution of the card payment.

## **9. Blocking of an available sum of money**

The bank is authorised to block the amount of money available on the account holder's account within the financial limit of use in accordance with Section II.3 if

- the payment transaction is initiated by or through the payee; and
- The cardholder has also agreed to the exact amount of money to be blocked.

\* The text in italics is only relevant if a digital card has been issued.

The bank shall release the blocked amount of money without delay, without prejudice to other legal or contractual rights, after it has been informed of the exact amount of the payment or after it has received the payment order.

#### **10. Rejection of card payments by the bank**

The Bank is entitled to refuse a card payment if

- the cardholder has not authorised the card payment in accordance with Section II.8,
- the spending limit applicable to the card payment or the financial usage limit has not been complied with, or
- the card has been blocked.

The cardholder will be informed of this during the payment process.

#### **11. Execution period**

The payment transaction is initiated by the payee. Upon receipt of the payment order by the bank, the latter is obliged to ensure that the card payment amount is received by the payee's payment service provider no later than the time specified in the "Price and Service List".

#### **12. Fees and changes thereto**

- (1) The fees owed by the account holder to the bank are set out in the bank's "Price and Service List".

\* The text in italics is only relevant if a digital card has been issued.

(2) Changes in fees for consumers:

Any changes in fees shall be offered to the account holder in text form no later than two months before their date of entry into force. If the account holder has agreed an electronic communication channel (e.g. online banking) with the bank within the framework of the business relationship, the changes may also be offered through this channel.

The changes offered by the bank will only become effective if the account holder accepts them. The Bank may only expressly enter into an agreement with the account holder to amend a fee that is based on a payment by the account holder in excess of the principal service.

The change of fees for the payment services framework agreement (current account agreement) is governed by Section 12 paragraph 5 of the General Terms and Conditions.

(3) Changes in fees for customers who are not consumers: The provisions of Section 12, paragraphs 2 to 6 of the General Business Terms and Conditions shall continue to apply to charges and changes in charges for payments by account holders who are not consumers.

### **13. Information for the account holder about the card payment transaction**

The bank shall inform the account holder of the payment transactions carried out with the card at least once a month via the agreed account information channel. The manner and timing of the information to be provided to account holders who are not consumers shall be agreed separately. The bank does not

\* The text in italics is only relevant if a digital card has been issued.

inform the account holder about the individual payments made with the cash card or the payee. The cardholder can track the payments made with the cash card using a chip card reader.

## **14. Claims for reimbursement, correction and damages by the account holder**

### **14.1 Refund for unauthorised card transactions**

In the event of an unauthorised card transaction in the form of

- a cash withdrawal at an ATM,
- use of the card at the electronic point of sale of commercial and service enterprises and/or in online retail,
- Cash card top-up,
- using the card to load a prepaid mobile phone account,

the Bank shall have no claim against the account holder for reimbursement of its expenses. The bank is obliged to refund the account holder the full amount. If the amount has been debited to his account, the bank will restore the balance to what it would have been without the unauthorised card transaction. This obligation shall be fulfilled no later than by the end of the business day as indicated in

the "Price and Service List" that follows the day on which the Bank was notified that the card payment is unauthorised or the Bank has otherwise become aware of this. If the Bank has informed a competent authority in writing of justified reasons for suspicion that the cardholder has engaged in fraudulent conduct, the Bank shall be required to review and fulfil its

\* The text in italics is only relevant if a digital card has been issued.

obligation arising from sentence 2 without undue delay if the suspicion of fraud is not confirmed.

#### **14.2 Claims in the event of non-execution, incorrect execution or delay of an authorised card transaction**

(1) In the event of non-execution or incorrect execution of a Authorised card transaction in the form of

- a cash withdrawal at an ATM,
- use of the card at the electronic point of sale of commercial and service enterprises and/or in online retail,
- Cash card top-up or
- using the card to top up a prepaid mobile phone account

the account holder can request the bank to refund the transaction amount without delay and in full insofar as the card transaction was not made or was incorrect. If the amount has been debited from his account, the bank will restore it to the balance it would have been in had the card transaction not been made or been incorrect.

(2) The account holder may demand that the bank reimburse the fees and interest in excess of the amount specified in paragraph 1 insofar as these were charged to him in connection with the non-execution or incorrect execution of the authorised card transaction or debited to his account.

(3) If the amount of the payment is not received by the payee's payment service provider until after the execution period specified in Section II.11 (delay), the payee may request their payment service provider to credit

\* The text in italics is only relevant if a digital card has been issued.

the amount of the payment to the payee's account as if the card payment had been properly executed.

(4) If an authorised card transaction is not executed or is executed incorrectly, the bank will review the card transaction at the cardholder's request and inform him of the result.

### **14.3 Indemnification for breach of duty**

In the event of an unauthorised card transaction or the non-execution, incorrect execution or delayed execution of an authorised card transaction, the account holder may request the Bank to provide compensation for any loss or damage not already covered by Section II.14.1 or II.14.2. This shall not apply if the Bank is not responsible for the breach of duty. In this context, the Bank is responsible for any fault on the part of an intermediary body as if it were its own fault, unless the main cause lies with an intermediary body specified by the cardholder. If the account holder is not a consumer or if the card is used in a country outside Germany and the European Economic Area<sup>1</sup>, the bank's liability for the fault of an institution involved in the processing of the payment transaction is limited to the careful selection and instruction of such an institution. If the cardholder has contributed to the occurrence of the loss through culpable conduct, the principles of contributory negligence shall determine the extent to which the bank and the account holder must bear

---

<sup>1</sup> EEA = European Economic Area. These currently include the EU countries Belgium, Bulgaria, Denmark, Germany, Estonia, Finland, France (including French Guiana, Guadeloupe, Martinique, Mayotte, Réunion), Greece, Ireland, Italy, Croatia, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Austria, Poland, Portugal, Romania, Sweden, Slovakia, Slovenia, Spain, Czech Republic, Hungary, as well as Cyprus and the countries Iceland, Liechtenstein and Norway.

\* The text in italics is only relevant if a digital card has been issued.



the loss. Liability under this paragraph is limited to €12,500 per card transaction. This limitation of liability does not apply

- For unauthorised card transactions,
- in the event of intent or gross negligence by the bank,
- for risks which the bank has assumed in particular and
- for the interest loss incurred by the account holder, insofar as the account holder is a consumer.

#### **14.4 Disclaimer and exclusion of objections**

(1) Claims against the Bank under Sections II.14.1 to 14.3 are excluded if the account holder fails to inform the Bank that a card transaction was unauthorised, not executed or executed incorrectly within a maximum of 13 months after the date of the debit entry for the card transaction. The 13-month period shall only commence if the bank has notified the account holder of the debit entry resulting from the card transaction via the agreed account information channel no later than one month after the debit entry; otherwise the 13-month period shall not commence for the start of the period the day of notification is decisive. The account holder may still assert liability claims in accordance with Section II.14.3 after the expiry of the deadline in sentence 1 if the account holder was unable to meet this deadline through no fault of his own.

\* The text in italics is only relevant if a digital card has been issued.

(2) Claims lodged by the account holder against the bank are excluded if the circumstances giving rise to a claim

- are based on an unusual and unforeseeable event over which the bank has no influence and the consequences of which could not have
- been avoided by the bank despite the application of due care, or were brought about by the bank due to a legal obligation.

## **15. Account holder's liability for unauthorised card transactions**

### **15.1 Account holder's liability until the blocking notification**

(1) If the cardholder loses his card or PIN, if they are stolen or otherwise go missing, or if they are misused in any other way, and if this results in unauthorised card transactions in the form of

- a cash withdrawal at an ATM,
- use of the card at the electronic point of sale of commercial and service enterprises and/or in online retail,
- Cash card top-up,
- Using the card to top up a prepaid mobile phone account,

the account holder shall be liable for losses caused up to the time of the blocking notification, up to a maximum amount of €50, regardless of whether the cardholder was at fault in the event of loss, theft or other misplacement or other misuse.

\* The text in italics is only relevant if a digital card has been issued.

(2) The account holder shall not be liable under paragraph 1 if

- it was not possible for the cardholder to notice the loss, theft, mislaying or other misuse of the card or mobile device with the digital card\* before the unauthorised card transaction, or
- The loss of the card was caused by an employee, an agent, a branch of the bank or another entity to which the bank's activities have been outsourced.

(3) If the account holder is not a consumer or if the card is used in a country outside Germany and the European Economic Area<sup>2</sup>, the account holder shall bear the loss arising from unauthorised card transactions in accordance with paragraph 1, even in excess of an amount not exceeding €50, if the cardholder has negligently breached the obligations incumbent upon him under these terms and conditions. If the bank has contributed to the occurrence of the damage by breaching its obligations, the bank shall be liable for the damage incurred to the extent of its contributory negligence.

(4) If unauthorised transactions are made before the card-blocking notification is made and the cardholder has acted with fraudulent intent or has deliberately or through gross negligence breached his/her duty of care under these terms and conditions, the account

---

<sup>2</sup> EEA = European Economic Area. These currently include the EU countries Belgium, Bulgaria, Denmark, Germany, Estonia, Finland, France (including French Guiana, Guadeloupe, Martinique, Mayotte, Réunion), Greece, Ireland, Italy, Croatia, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Austria, Poland, Portugal, Romania, Sweden, Slovakia, Slovenia, Spain, Czech Republic, Hungary, as well as Cyprus and the countries Iceland, Liechtenstein and Norway.

\* The text in italics is only relevant if a digital card has been issued.

holder shall bear the full extent of the losses incurred as a result. Gross negligence on the part of the cardholder may occur in particular if

- he has culpably failed to report the loss or theft of the card or its unauthorised use to the bank or the central card-blocking service immediately after becoming aware of this,
- He has noted the personal PIN on the physical card or kept it together with the physical card (for example in the original letter in which it was communicated to the cardholder),
- *he has stored the personal PIN of the digital card in the mobile device or in another device\**,
- he has disclosed the personal identification number of another person and the misuse has been caused by this.

(5) Liability for damages caused within the period for which the credit limit applies is limited to the credit limit applicable to the card.

(6) Notwithstanding paragraphs 1 and 3, the account holder shall not be liable for damages if the Bank has not requested strong customer authentication within the meaning of Section 1 (24) of the German Payment Services Supervision Act (Zahlungsdiensteaufsichtsgesetz – ZAG) from the cardholder (e.g. in the case of small value payments pursuant to Section A.I.3 of these terms and conditions) or the payee or his payment service

\* The text in italics is only relevant if a digital card has been issued.

provider has not accepted it, although the Bank was obliged to use strong customer authentication in accordance with Section 55 ZAG. In particular, strong customer authentication requires the use of two independent authentication elements from the categories of knowledge (that is the PIN), possession (that is the card) or being (something that the cardholder is, for example a fingerprint).

(7) The account holder shall not be obliged to provide compensation for the losses under paragraphs 1, 3 and 4 if the cardholder was unable to submit the blocking request because the bank had not ensured the possibility of receiving the blocking request.

(8) Paragraphs 2 and 5 to 7 shall not apply if the cardholder has acted fraudulently.

## **15.2 Liability of the account holder from the blocking request**

As soon as the bank or the central blocking service has been notified of the loss or theft of the card, the misuse or any other unauthorised use of the card or PIN, the bank shall assume all costs incurred thereafter as a result of transactions in the form of

- a cash withdrawal at an ATM,
- use of the card at the electronic point of sale of commercial and service enterprises and/or in online retail,

\* The text in italics is only relevant if a digital card has been issued.

- Cash card top-up and
- using the card to top up a prepaid mobile phone account

resulting damages. If the cardholder acts with fraudulent intent, the account holder shall also bear the losses arising after the card-blocking notification.

### **15.3 Liability of the account holder for the amount stored in the cash card**

It is not possible to block the cash card for payment at automated payment terminals. In the event of loss, theft, misuse or any other unauthorised use of the cash card for payment at automated pay points, the bank will not refund the amount stored on the cash card, because anyone in possession of the card can consume the amount stored on the cash card without using the PIN.

## **III. Special rules for individual types of use**

### **1. ATM service and use at automated checkouts in retail and service companies**

#### **1.1 Card limit**

The cardholder may only make withdrawals at ATMs, automated payment terminals and top up the cash card (GeldKarte) within the spending limit set for the card. Each time the card is used at cashpoints and automated cash registers, a check is carried out to determine whether the card's

\* The text in italics is only relevant if a digital card has been issued.

credit limit has already been exhausted by previous transactions. Transactions that would exceed the card's spending limit are rejected regardless of the current account balance and any credit previously granted to the account. The cardholder may only utilise the card's transaction limit within the scope of the account balance or a previously granted credit for the account. The account holder can agree with the account-managing office a change to the card's spending limit for all cards issued to his account. Anyone with a power of attorney who has received a card can only arrange a reduction for that card.

### **1.2 Incorrect PIN entry**

The card can no longer be used at ATMs or electronic cash terminals where the PIN has to be entered in connection with the use of the card if the personal PIN has been entered incorrectly three times in succession. In this case, the cardholder should contact his or her bank, preferably the branch that holds the account.

### **1.3 Bank's payment obligation; complaints**

The bank has a contractual obligation to the operators of ATMs and electronic cash terminals to reimburse the operators for the amounts obtained by using the card issued to the cardholder. Any objections or other complaints by the cardholder arising from the contractual relationship with the company at which a cashless payment was made at an electronic cash terminal must be asserted directly to that company.

### **1.4 Pre-selection of automated payment terminals**

\* The text in italics is only relevant if a digital card has been issued.

Retailers and service providers can install mechanisms in their automated payment terminals that preselect a specific payment brand or payment application for the cards they accept. In doing so, they must not prevent the cardholder from overriding this pre-selection.

## 2. Cash Card

### 2.1 Service description

The card, which is equipped with a chip, can also be used as a cash card. The cardholder can make cashless payments at cash card terminals in the retail and service sectors.

### 2.2 Cash card top-up and unloading

The cardholder can top up his/her cash card at the top-up terminals marked with the GeldKarte (cash card) logo within the credit limit granted by the corresponding bank (Section III.1.1) by debiting the account specified on the card up to a maximum amount of €200. Before top-up, the personal identification number (PIN) must be entered. The cardholder can also top up the cash card with cash or in conjunction with another card, debiting the account through which the transactions with this card are settled. Amounts on the card that the cardholder no longer wishes to access using the cash card may only be unloaded at the card-issuing bank.

If the cash card is not working, the card-issuing bank will refund the unused amount to the cardholder. When the cardholder uses his card to

\* The text in italics is only relevant if a digital card has been issued.



load his own or someone else's cash card, the personal identification number (PIN) must be entered at the top-up terminal. The top-up option is no longer available if the PIN is entered incorrectly three times in a row. In this case, the cardholder should contact his or her bank, preferably the branch that holds the account.

### **2.3 Immediate debit of top-up amount**

If the cardholder uses his card to load his own or someone else's cash card, the amount loaded will be debited to the account indicated on the card.

### **2.4 Payment transaction using a cash card**

When paying with the cash card, the PIN does not need to be entered. Each time you make a payment, the amount stored on the cash card is reduced by the amount used.

## **3. Top up prepaid mobile phone accounts**

### **3.1 Service description**

Using his card and personal identification number (PIN), the cardholder can top up a prepaid mobile phone account with a mobile phone provider, to which prepaid phone credit units are added, at ATMs within the spending limit granted to him by his bank (Section III.1.1) and at the expense of the account specified on the card. The prerequisite is that the cashpoint selected by the cardholder has a corresponding top-up

\* The text in italics is only relevant if a digital card has been issued.

function and that the mobile phone provider that manages the prepaid mobile phone account that is to be topped up participates in the system. To top up a prepaid mobile phone account, the cardholder must select the menu item for topping up the prepaid mobile phone account on the ATM display, enter the mobile phone number and select a top-up amount from the amounts displayed. After the top-up transactions have been authorised by the cardholder's bank, the prepaid mobile phone account is topped up by the mobile phone provider. This procedure allows the cardholder to top up both his own prepaid mobile phone account and that of a third party. If the bank does not authorise the top-up, for example because there are insufficient funds in the account, a message to this effect will appear on the display.

### **3.2 Incorrect PIN entry**

The card can no longer be used at cashpoints if the PIN has been entered incorrectly three times in a row. In this case, the cardholder should contact his or her bank, preferably the branch that holds the account.

### **3.3 Bank's payment obligation; complaints**

The bank is contractually obliged to pay loading amounts for a prepaid mobile phone account that have been authorised using the card issued to the cardholder. The payment obligation is limited to the respective authorised amount. Any objections or other complaints that the cardholder may have arising from the contractual relationship with the mobile phone provider that manages the prepaid mobile phone account must be asserted directly against that company.

\* The text in italics is only relevant if a digital card has been issued.

## B. Additional bank services

### 1. Special conditions

Special conditions apply to other services provided by the bank for the card, which are agreed with the account holder before use.

### 2. Agreement on the types of use

The bank and the account holder agree which services the account holder can access with the card.

## C. Additional applications

### 1. Storage of additional applications on the card

(1) The cardholder has the option of using the chip on the card as a storage medium for a bank-generated additional application (e.g. in the form of a parental control feature) or as a storage medium for a company-generated additional application (e.g. in the form of an electronic ticket).

\* The text in italics is only relevant if a digital card has been issued.

(2) The use of an additional bank-generated application is governed by the legal relationship between the cardholder and the bank. The cardholder may use an additional company-generated application in accordance with the contract concluded with the company. It is up to the cardholder to decide whether they want to use their card to store additional company-generated applications. Additional company-generated applications can be stored on the card at the company's terminal, subject to agreement between the cardholder and the company. Credit institutions have no knowledge of the content of the data communicated at the company terminal.

## **2. Liability of the company for the content of company-generated additional applications**

With the chip on the card, the card-issuing bank merely provides the technical platform that enables the cardholder to store additional company-generated applications on the card. Any services that the company provides to the cardholder via the company-generated additional application shall be governed exclusively by the content of the contractual relationship between the cardholder and the company.

## **3. Complaint handling in relation to additional applications**

(1) The cardholder must raise any objections relating to the content of a company-generated additional application exclusively with the company that stored the additional application on the card. The company processes any complaints on the basis of the data stored therein. The cardholder must not hand over the card to the company for the purpose of processing the complaint.

\* The text in *italics* is only relevant if a digital card has been issued.

(2) The cardholder must raise any objections relating to the content of a bank-generated additional application exclusively with the bank.

#### **4. No indication of the PIN issued by the bank to the customer for company-generated additional applications**

When a company-generated additional application is stored, modified or used on the card, the PIN issued to the cardholder by the card-issuing bank is not entered. If the company that has stored an additional company-generated application on the card, allows the cardholder to secure access to this additional application with a separate identification medium of his choice, the cardholder may not use the PIN provided to him by the card-issuing bank for the payment transaction applications to secure the company-generated additional application.

#### **5. Possibility to block additional applications**

Additional company-generated applications can only be blocked by the company that has stored the additional application on the chip of the card, and only if the company has provided for the option of blocking its additional application. The blocking of bank-generated additional applications can only be considered in relation to the bank and is based on the contract concluded with the bank.

\* The text in italics is only relevant if a digital card has been issued.