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.

Supplementary conditions for the use of the digital girocard by means of authentication with the cardholder's mobile device

1. Scope and authentication elements

The digital girocard issued by the Bank is a debit card (hereinafter referred to as the 'digital card') that is provided to the cardholder for storage on a mobile device (telecommunications, digital or IT device). The cardholder can use this to access payment services in accordance with Section 2 of these terms and conditions.

When using the digital card by means of authentication with the cardholder's mobile device, the following are used to prove the identity of the cardholder as authentication factors:

- digital map on mobile device (possession factor) and
- a cardholder's unique identifier (inherence factor) that can be verified on their mobile device (e.g. fingerprint, facial recognition) or, alternatively, an unlocking mechanism for the mobile device (e.g. unlock code).

The following rules apply to the use of the digital map by means of authentication with the mobile device and inherence factor. Unless these terms and conditions contain any special provisions, the general provisions in the "Conditions for the girocard (debit card)".

Contractual agreements between the cardholder and third parties (e.g. device manufacturers, mobile phone providers or providers of payment platforms in which digital cards can be stored) remain unaffected. The contractual service of the bank does not affect

the functionality or operation of the mobile device, as well as payment platforms such as apps for digital wallets in which the digital card can be stored.

2. Possible uses

The cardholder can use the digital card with a mobile device and its element for the following payment services:

a. For contactless use in retail and service companies at automated cash registers within the framework of the German girocard system, which are marked with the girocard logo (girocard terminals).
b. For use in electronic remote payment transactions via the internet at retail and service companies (online retailing) that are identified by the girocard logo and are part of the German girocard system. If the cardholder has added the digital card to a digital wallet, the digital card can only be used in e-commerce if the retail and service company has indicated this by means of the acceptance mark of the respective digital wallet.
c. For contactless use by retail and service companies at automated checkouts and in online retailing as part of a third-party system, provided that the digital card is equipped accordingly. The acceptance of the digital card in the context of a third-party system is subject to the acceptance logo applicable to the third-party system.

3. Authorisation of card payments by the cardholder

The digital card is used by bringing the mobile device in which the digital card is stored close to the contactless terminal of the retail or service company or, in the case of online retailing, by selecting and confirming the girocard payment application. In doing so, the cardholder authorises the execution of the card payment. If requested by the bank, the cardholder's PIN or, alternatively, the unlock code for the mobile device must also be used for authorisation. In this case, authorisation is only granted when it is used. Once the authorisation has been granted, 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 personal data of the cardholder necessary for the execution of the card payment.

If the cardholder or the bank discontinues the use of the inherence factor, the contactless use of the digital card with two authentication factors is still possible, but only by entering the personal identification number (PIN) applicable to the digital card at the automated payment terminal (see Section A.I.1 of the terms and conditions for the girocard (debit card).

4. Blocking the digital map for use with mobile devices and inherence factors

a. The Bank may block the digital card for use with a mobile device and inherence factor (e.g. by deleting it) if it is entitled to terminate the card contract for good cause, if justified by objective reasons related to the security of the cardholder's inherence factor or the digital card, or if there is suspicion of unauthorised or fraudulent use of an inherence factor or the digital card. The bank will inform the account holder of this, stating the relevant reasons, if possible before the account is frozen, but at the latest immediately afterwards. The reasons may be omitted if doing so would cause the bank to violate legal obligations. The bank will unblock the digital card or provide a new digital card if the reasons for blocking no longer apply. The cardholder shall be informed of this without delay.

b. Blocking only the digital card does not block the physical debit card.

5. Cardholder's duty of care and co-operation

5.1. Special protective obligations of the cardholder

The cardholder must take all reasonable precautions to prevent unauthorised use of his digital card through improper use of his mobile device or inherence factor. Please note the following in this regard:

a. The unlock code for the mobile device must be kept secret. In particular, it may not be
   - passed on orally (e.g. by telephone) or in text form (e.g. by e-mail, messenger service),
   - Not be stored electronically in an unsecured manner (e.g. stored in plain text on a computer or mobile device) and
   - nor may it be written down on a device or stored as a copy together with a device that serves as a mobile device with a digital card.

b. The mobile device with a digital card must be protected against misuse, in particular
   - It must be ensured that unauthorised persons cannot access the cardholder's mobile device (e.g. mobile phone),
   - It must be ensured that other persons cannot use the digital card stored on the mobile device,
   - the digital card on the mobile device must be deleted before the cardholder permanently gives up possession of this mobile device (e.g. by selling or disposing of it),
   - the cardholder must install the software updates offered to him by the manufacturer of the mobile device with a digital card in each case,
   - If the cardholder has received a code from the bank to activate the digital card, he or she must keep it safe from unauthorised access by other persons.

c. Inherence factors, such as the cardholder's fingerprint, for example, may only be used on a cardholder's mobile device to authorise payment orders if no other person's inherence factors are stored on the mobile device.

5.2. Information and notification obligations

The information and notification requirements are set out in section A.II.7.4 of the terms and conditions for the girocard (debit card). In addition, the cardholder must also notify the bank immediately if any of his/her inherence

factors are suspected of unauthorised or fraudulent use (blocking notification).

6. Claims for reimbursement, correction and damages by the account holder

The account holder's claims for reimbursement, correction and compensation arise from section A.II.14 of the Terms and Conditions for the girocard (debit card).

7. Account holder's liability for unauthorised card transactions

In addition to the general liability provisions in section A.II.15 of the terms and conditions for the girocard (debit card), the account holder shall be liable in the event of a breach of the duty of care for the protection of his mobile device and his inherence factor in accordance with the following provisions.

7.1. **Account holder's liability until the blocking notification**

(1) If the cardholder breaches his/her obligations under Section 5 of these terms and conditions and this results in unauthorised card transactions, the account holder shall be liable for losses incurred 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 unauthorised use of the digital card in connection with its use with a mobile device and its element.

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

- it was not possible for the cardholder to notice the misuse of the digital card in connection with the use of the mobile device and its inherence factor before the unauthorised card transaction, or
- the unauthorised use of the digital card in connection with the use of a mobile device and its inherent factors by an employee, an agent, a branch of the bank or any other 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, the account holder shall bear the damage resulting from unauthorised card transactions in accordance with paragraph 1, even if the card holder has negligently violated 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 as set out in these terms and conditions, the account holder shall bear the full extent of the losses incurred as a result. Gross negligence on the part of the cardholder in connection with the use of a mobile device and its inherent factor can be particularly present if

- He has negligently failed to immediately report the loss or theft of the mobile device with the digital card or the unauthorised transaction to the bank or the Central Blocking Service after he became aware of it,
- he has passed on the unlock code for the mobile device orally or in text form or stored it unsecured in electronic form, or written it down on a device or kept it as a transcript together with a device that serves as a mobile device with a digital card, or

- He permanently gives up possession of this mobile device (e.g. by sale, disposal) without first deleting the digital card on the mobile device,
- he used his biometric features on his mobile device to authorise payment orders, even though the biometric features of other persons were stored on the mobile device.

(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 is not liable for damages if the bank has not required the cardholder to provide strong customer authentication within the meaning of Section 1 paragraph 24 of the Payment Services Supervision Act (ZAG) (e.g. in the case of small-value payments pursuant to Section A.I.3 of the conditions for the girocard (debit card) or the payee or his payment service provider has not accepted this, although the bank is required to provide strong customer authentication in accordance with Section 55 of the German Payment Services Supervision Act (Zahlungsdiensteaufsichtsgesetz - ZAG). In particular, strong customer authentication requires the use of two independent authentication elements from the categories of knowledge (the PIN), ownership (the card) or inherence (something the cardholder is, such as 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.

7.2. **Liability of the account holder from the blocking request**

As soon as the unauthorised use of the digital card in connection with use with a mobile device and Seinselement has been reported to the bank or the central blocking service, the bank shall assume all losses arising thereafter as a result of transactions carried out in accordance with the options for use described in Section 2 of these conditions. If the cardholder acts with fraudulent intent, the account holder shall also bear any damages incurred after the card has been blocked.