

General Terms and Conditions for the Use of Credit Cards of Cembra Money Bank AG on Mobile End Devices

These Terms and Conditions apply to the electronic storage of credit cards (hereinafter «Card») of Cembra Money Bank AG (hereinafter «Issuer») in a payment application developed for this purpose by a third-party provider (hereinafter «Payment Application») for mobile devices and the use of the electronically stored card for cashless payment transactions (hereinafter «Mobile Payment»).

Mobile Payment is offered by the provider of the Payment Application, including its group companies or commissioned third parties (hereinafter «Payment Application Provider») in accordance with its separate terms and conditions. The Issuer is not the provider of the Payment Application, but merely enables the card to be deposited in the Payment Application of the Payment Application Provider.

1 REGISTRATION, RENEWAL AND TERMINATION

1.1 Registration and Installation

The option of Mobile Payment via the Card is provided exclusively at the discretion of the Issuer and will only be approved for cardholders who already have a card relationship with the Issuer (primary or additional card) (hereinafter, «Cardholder»).

In order to use the option of Mobile Payment, the Cardholder must download the Payment Application (if not already preinstalled) onto a compatible mobile device (e.g. mobile phone, watch or tablet) (hereinafter «End Device») and accept the terms and conditions as well as the data protection declarations of the Payment Application Provider. The cardholder can then register the card in the Payment Application. In this process, a digital card number is generated, which is stored in the Payment Application. The card may only be used for Mobile Payment after successful registration. Cardholders who wish to use Mobile Payment must follow the instructions of the issuer or the Payment Application Provider during the installation and registration process for Mobile Payment. The Cardholder is fully liable for any failure to comply or any delay in complying with these Terms and Conditions. The cardholder may only store credit cards in their name in their Payment Application.

1.2 Expiry and replacement of cards

The renewal, blocking, unlocking or termination of the card generally also applies to its use for Mobile Payment.

Electronic registration of the card for Mobile Payment may be terminated, blocked or unlocked separately for each End Device and does not change the status of the card. However, each primary or additional card must be terminated, blocked or unlocked separately for each End Device by the respective Cardholder.

1.3 Termination of the contractual relationship

The Cardholder has the right to terminate the Mobile Payment Contract in writing at any time without any need to state reasons. If the card is terminated, Mobile Payment shall also be deemed to have been terminated.

The Issuer reserves the right to terminate the Mobile Payment contract at any time without stating reasons, to block individual Payment Applications and to block cards for Mobile Payment or to refuse registration of the Card in Payment Applications.

2 USE OF MOBILE PAYMENT

2.1 Use of the card and approval

Mobile Payment entitles the Cardholder to pay for goods and services via eligible cash terminals, to make in-app payments in compatible merchant apps and to use other payment methods provided by the Payment Application Provider within the credit limit set by the Issuer.

A transaction initiated via Mobile Payment shall be deemed to have been authorised by the Cardholder, even if the person initiating the transaction is not the Cardholder. All payments made via Mobile Payment shall be debited to the corresponding credit card account in the same manner as a normal transaction. The risks arising from misuse of the Card are borne by the Cardholder, subject to sec. 4.1 below.

2.2 Fees

The Cardholder shall bear all fees, costs or expenses charged by the mobile and/or telecommunications provider for or in connection with the installation and/or use of the Card for Mobile Payment. As regards data transfers by the Cardholder via the internet (including roaming) and other services of his/her mobile and/or telecommunications provider, the fees set forth in the agreement between the Cardholder and his/her provider shall apply. The amount of the Issuer's fees for the Card and the payments made thereunder are governed by the applicable fee schedule and the General Terms and Conditions for the Use of the Card.

2.3 Restriction or extension of the options for using the Card

The options for using the Card, Payment Application and Mobile Payment may be extended, restricted or cancelled by the issuer or the Payment Application Provider at any time.

3 CARDHOLDER'S DUTIES OF CARE

The Cardholder has the following duties of care:

3.1 Compatible End Device

The Cardholder is solely responsible for ensuring that he/she has a compatible End Device that supports the use of the Card for Mobile Payment. The Cardholder may not set up and/or use the Card on an End Device that contains illegally acquired, hacked, falsified and/or unauthorized apps or in which the software lock has been disabled (for example, but not exclusively, because a so-called jailbreak has been carried out or the device has been rooted). The original operating system and the Payment Application must be kept up to date at all times.

3.2 Safekeeping and Security Information

The Card and the cardholder's End Device are outside the Issuer's control. They must be stored carefully at all times. The Cardholder may not permit any third party to use Mobile Payment and shall keep the Card and the End Device under his/her personal control at all times. The End Device must be protected by setting up an unlocking mode using appropriate security information (e.g. secure and not easily ascertainable password, sample, iris or fingerprint, face ID, voice recognition) and other suitable means of protection (e.g. malware protection, firewall). Security information must not consist of easily identifiable combinations, e.g. telephone numbers, dates of birth, license plate numbers. The Cardholder is obliged to keep the security information secret at all times. Security information may not be disclosed to third parties or recorded, even in encrypted form. Furthermore, no security information from third parties (e.g. biometric data) may be stored on the End Device for unlocking. If the Cardholder suspects that someone else has security information that he or she is using for the device, the Cardholder must change the security information immediately.

3.3 Replacement, loss and theft of the End Device

The Cardholder is obliged to delete all card and transaction data prior to any (temporary or permanent) transfer (e.g. sale, donation, loan, deposit, pledge, repair) of the End Device.

If an End Device is lost or stolen, the Cardholder must immediately take the steps recommended by the device manufacturer to locate and lock the End Device and delete its content remotely. In addition, the Cardholder is obliged to inform the Issuer immediately if he or she loses the End Device and to arrange for the Card or Mobile Payment to be blocked by the Issuer. In addition, the Cardholder must immediately block the SIM card (or have it blocked by the network operator). The obligations set out in this section also apply in the event of any mere presumed loss or theft of the End Device.

3.4 Notification

If the Cardholder notices or suspects that the card, the End Device or the security information has come into the possession or control of an unauthorized person or that unauthorized contactless transactions have been carried out, he or she must inform the Issuer immediately by telephone. **Until such time as the Issuer actually receives such notification, the Cardholder remains fully liable for any use of the Card by unauthorized persons or for unauthorized purposes.**

4 RESPONSIBILITY AND LIABILITY

4.1 Assumption of losses in the event that the Cardholder is not at fault

If the Cardholder has complied with his or her duties of care specified in sec. 3 as well as the General Terms and Conditions for the Use of the Card and the terms and conditions of the Payment Application Provider and is not at fault for any other reason, the Issuer shall bear any losses incurred by the Cardholder as a result of misuse of Mobile Payment by third parties. For the purposes of this sec. 4.1, «third parties» do not include spouses or registered partners of the Cardholder and persons living in the same household as the Cardholder. Losses for which an insurance company is responsible, as well as any consequential losses of any kind, to the extent permitted by law, are not covered. In the event of any loss being assumed by the Issuer, the Cardholder must assign his claims arising from the loss event to the Issuer.

4.2 Breach of the duties of care

Any Cardholder who fails to comply with his or her duties of care shall be fully liable for all losses resulting from misuse of the Card until such time as a possible block is effective.

4.3 Lack of Technical Availability

The Issuer assumes no responsibility for continuous availability of the payment option via Mobile Payment and is not liable for losses resulting from disruptions, interruptions, breakdowns or overloads of the Issuer's IT systems or of those of third parties engaged by the Issuer, of Payment Application Providers, mobile radio and/or telecommunications providers or on the Internet, or if for other reasons payment with the Card cannot be executed via Mobile Payment. The same applies to cases where a payment in a foreign location or originating from abroad is subject to local legal restrictions or violates foreign law.

4.4 No liability for software and hardware

The Issuer shall not be liable for losses, damages or damage caused by viruses to the Cardholder's data, programs, End Devices or other devices as a result of the installation, commissioning and/or use of Mobile Payment or the Payment Application. In particular, the Issuer shall not be liable for any disruptions or security, availability or performance restrictions to the End Device.

4.5 No Liability for Third Parties

The Issuer is not responsible for the Payment Application itself or for the services, actions and omissions of the Payment Application Provider or the mobile and/or telecommunications provider.

4.6 Upon termination of the contractual relationship

The right to use Mobile Payment shall, in any event, expire upon termination of the Mobile Payment contractual relationship. Even after termination of the Agreement, the Cardholder shall be liable for any losses caused by him or her. Unlawful use of the Card may result in civil and/or criminal prosecution.

Termination as a result of the recall or return of the card shall be governed by the General Terms and Conditions governing the use of the card.

5 AMENDMENTS TO TERMS AND CONDITIONS

The Issuer reserves the right to amend these Terms and Conditions at any time. Such changes shall be notified to the Cardholder by written circular or by other appropriate means (e.g. letter, e-mail, SMS, on the Issuer's website (www.cembra.ch/legal), messages displayed on the display of the End Device or, where applicable, publication in the eService Portal) and shall be deemed to have been approved unless the Cardholder objects within 30 days or continues to use the Mobile Payment after notification.

6 DATA AND DATA PROTECTION

6.1 Data collection and processing

The cardholder acknowledges that the Issuer and the Payment Application Provider are independent and autonomous controllers with regard to the processing of personal data. When using Mobile Payment, the processing of the cardholder's personal data is carried out in accordance with the separate data protection provisions of the payment application provider. It is the holder's responsibility to consult these in order to obtain information about the data processing purposes of the payment application provider.

Upon registration and use of Mobile Payment, the Cardholder agrees that customer, card and transaction data as well as the digital card number, device information, data of a SIM or storage card and geodata as well as information from the business relationship between the Cardholder and the Payment Application Provider (including in its capacity as device manufacturer or operator of an operating system installed on the device) may be obtained, processed and disclosed.

The Cardholder instructs and authorizes the Issuer, in connection with the registration, renewal, blocking, unlocking and termination, the electronic storage of the Card and/or in connection with mobile payment transactions, to exchange the aforementioned data with the Payment Application Provider and the card network company, which may be located abroad, for the following purposes, insofar as necessary:

- verification of whether electronic storage is permissible,
- verification and reconciliation of the identity of the Cardholder and the holder of the device;
- prevention of abuse and fraud;
- compliance with supervisory provisions (e.g. national/international sanctions),
- creating/updating the digital card number and matching status information (renewal, termination, blocking or unlocking, etc.) between the card and the electronic storage thereof;
- creating a list in the Payment Application of past transactions (e.g. information about the merchant, transaction amount and date).

In addition, the Payment Application Provider and the card network company may use the exchanged data for their own further purposes (including e.g. marketing) in accordance with their applicable terms and conditions and data protection declarations. In this context, objections to all data processing must be addressed directly to the payment application provider or the card network company. The Issuer is not responsible for the procurement, processing and forwarding of data by the Payment Application Provider, the card network company or third parties engaged by them. In particular, the cardholder agrees that the Payment Application Provider and the card network companies may transfer this data to the United States of America and store and process it there.

The Cardholder acknowledges that the exchanged data is therefore not subject to bank-client confidentiality and that the Payment Application Provider and the card network company shall not be bound by bank-client confidentiality.

6.2 Data transfer

When the Cardholder downloads or uses the Payment Application and Mobile Payment, the Cardholder's data is transmitted over an open, possibly unencrypted network, which almost everyone can access. This means that third parties, irrespective of their location, may conclude that a business relationship exists, has existed or may exist in the future between the Cardholder and the Issuer. Even if the sender and the recipient are located in the same country, data transmission via such networks often takes place via third countries, i.e. including via countries whose legislation does not guarantee adequate data protection. The data may be lost during transmission or intercepted, manipulated and misused by unauthorized third parties, or the identity of the sender may be spoofed or manipulated. Even in the event of data encryption, the names of the sender and the recipient of a message remain unencrypted and thus visible. The Issuer assumes no liability for the security of the Cardholder's data during transmission over the internet. The Bank shall not be liable for direct or indirect losses resulting from the loss or unauthorized interception of the data by third parties.

7 FURTHER PROVISIONS

Should parts of these Terms and Conditions of Use be invalid in whole or in part, this shall not affect the validity of the remaining provisions. The Parties agree that any legally invalid provisions should be replaced by provisions coming as close as possible to the intended purpose.

The General Terms and Conditions for the Use of the Card shall otherwise apply in addition and shall take precedence over these Terms and Conditions of Use in the event of any discrepancies.