



Cembra App Terms and Conditions of Use

1 Subject matter

1.1 General provisions

Cembra Money Bank Ltd. (hereinafter the "Bank") offers its customers (hereinafter the "User(s)") the option of viewing their bank products existing at the Bank - insofar as this is permitted for the use of this application (hereinafter the "Cembra App") - on compatible end devices (e.g. mobile phone or tablet) (hereinafter the "End Device") and to obtain certain services and functionalities from the Bank.

1.2 Scope of application

These Cembra App Terms and Conditions of Use (hereinafter "Terms and Conditions of Use") supplement the General Terms and Conditions ("Product GTCs") for the use of the respective products of the Bank and govern, as part of the contractual relationship, the relationship between the Bank and the User in relation to the use of the Cembra App.

By downloading, registering and using the Cembra App, the User consents to the Terms and Conditions of Use valid at the time of download, use or access. The current version of the Terms and Conditions of Use may be viewed whenever the Cembra App is used. The latest version of the relevant Product GTCs may be accessed from our website at the following www.cembra.ch.

2 Registration and login

2.1 General provisions

The Cembra App is accessed via End Devices that have network access (e.g. by means of mobile phone cards or Wi-Fi networks). The Cembra App is available for download and installation on the User's End Device from Google's "Google Play" and Apple's "App Store" platforms.

The User acknowledges that he/she complies with the applicable provisions of the Google Play Terms of Use (in accordance with the local version applicable to the User, for Switzerland: www.play.google.com/intl/de_ch/about/play-terms/, hereinafter referred to as "Google Play Terms of Use") and for the Apple App store (in accordance with the local version applicable to the User, for Switzerland: www.apple.com/chde/legal/internet-services/itunes/chde/terms.html, hereinafter "Apple Store Terms of Use") at the time of downloading, using or accessing the Cembra App, and acknowledges that those terms may apply in addition to these Terms of Use. In the event of any inconsistency between these Terms of Use and the Apple Store Terms of Use and/or the Google Play Terms of Use, the latter shall prevail over these Terms of Use.

2.2 Initial registration of the Cembra App

For the initial registration of the Cembra App on an End Device, the Bank shall send the User his/her login information by post or otherwise. In the registration process, the User shall define a personal access code (hereinafter "Access Code"). To the extent provided by the Bank as access functions, access may also take place using biometric data, e.g. Face ID or Touch ID (hereinafter "biometric information"). If the User selects such biometric information for logging in, it will replace entering the Access Code in future. The use of biometric information for access can be adjusted in the Cembra app. In future, the Bank may provide the User with other biometric access options for login purposes.

2.3 Login for use of the Cembra App

Every login to use the Cembra App is made via an authentication process. In the authentication process, the User uses his/her Cembra App access data (hereinafter "Access Data"), which is intended to enhance security when accessing and using the Cembra App and serves as a means of authentication when using the Cembra App. The use of the access data is governed by Sections 3.3 and 3.4.

3 General security notices and duties of care of the User

3.1 Unauthorized access by third parties

The User is aware that unauthorized access to the Cembra App by third parties may result in misuse of the Cembra App. This includes, for example, access by unauthorized third parties to the User's bank client data or misuse of his/her End Device for checking or confirming transactions in the Cembra App (e.g. by using the Mastercard ID check or sending SMS codes) or debiting the user's credit card account by paying QR-bills in the Cembra App (Scan2Pay). In order to avoid the risk of unauthorized access to or unauthorized use of the Cembra App, the User must take all such security measures as are necessary and appropriate.

3.2 Protection against unauthorized access

The User shall take the following security measures, in particular, to prevent unauthorized access to the Cembra App by third parties:

- a) logging out of the Cembra App after each use.
- b) In the event of the loss or theft of the End Device, the User must inform the Bank immediately of the loss of his/her End Device. If the Access Data is lost or stolen and/or there is a suspicion of misuse of any kind, the User must notify the Bank immediately. All telephone notifications by the User in connection with the loss or theft of the End Device or the Access Data must then be confirmed in writing to the Bank.

3.3 Duties of care upon first registration

When registering the Cembra App for the first time, the User must provide the Issuer with his/her current personal mobile phone number. This is required in order to provide the User with the mTAN code and any further information. The mTAN code and any other information is provided to the User exclusively via the last mobile telephone number he/she has indicated to the Bank or notified the Bank of in writing. The User must either inform the Bank immediately of any change to the mobile phone number or must update his/her mobile phone number in the Cembra App himself/herself.

3.4 Duties of care as regards the Access Data

When using the Access Data, the User must comply, in particular, with the following duties of care:

- a) The security recommendations of the Bank must be complied with during the registration process in order to create the Access Code. If the Access Code consists of easily identifiable combinations (e.g. telephone numbers, dates of birth, vehicle registration numbers), the Bank disclaims all liability in the event of access of the Cembra App by unauthorized third parties.
- b) The User must keep the Access Code secret at all times. The Access Code may not be passed on to third parties or recorded, even in encrypted or unencrypted form. The Access Code may not be recorded in writing or stored electronically. Furthermore, no biometric information from third parties may be stored on the End Device in order to unlock the Cembra App.
- c) If the User suspects, or should have suspected, had he/she exercised due care, that another person is aware of his/her Access Code or has biometric information that he/she uses for the End Device, the User's Access Code and/or biometric information must be changed immediately and the Bank must be notified immediately.

- d) Upon request by the Bank, the User shall immediately change the Access Code used for logging in to the Cembra App.
- e) The User must always ensure that he/she is not being monitored when entering the Access Code.

3.5 Duties of care as regards bank products

- a) The Bank may offer the User a virtual credit card (simultaneously with the standard physical credit card). The use of a virtual card corresponds to that of a standard physical credit card. Any use of a virtual card shall be deemed to have been authorized by the Cardholder. The Cardholder has the right to prove the contrary. Virtual cards must be used in accordance with the instructions of the Bank or merchant (e.g. by entering a security code or using biometric information). **The User must therefore treat the End Devices and virtual cards used with care and ensure that they are protected.**
- b) The End Devices used must be used as intended and kept securely protected from any third-party access. Virtual cards, like physical cards, are personal and non-transferable. They may not be passed on to third parties for use (e.g. by storing fingerprints or by scanning the faces of third parties in order to unlock the End Device used). In the event of a change or transfer of a mobile device (e.g. in the event of a sale), every virtual card must be deleted in the Cembra App or on the End Device. Any suspected misuse of a virtual card or an End Device used with it must be reported to the Bank immediately so that the affected virtual card can be blocked.
- c) The Mastercard ID Check is a service for secure online payment. Registration for this service occurs automatically when using the Cembra App and cannot be terminated. Upon receipt of a push message to authorize the transaction, the Cardholder must ensure that the transaction information contained in the notification (e.g. dealer name, transaction amount) is consistent with the transaction executed by him/her. In case of doubt, the User may not confirm the transaction. Every confirmed transaction shall be deemed to have been executed by the Cardholder. The Customer acknowledges all authorized transactions confirmed in this manner and the resulting claims of card acceptors.

3.6 Security

The Cembra App is protected by appropriate encryption technology and security certificates. However, absolute security cannot be guaranteed. The User acknowledges, in particular, the following:

- a) The Bank offers the Cembra App in its current state, only as a self-executing software application, i.e. without representations and warranties or liabilities of any kind. In particular, the Bank does not offer any telecommunication services or electronic transmission of information. This is the task of the telecommunications service provider from which the User obtains services for the respective End Device, as part of that service provider's current range of services. The Bank assumes no liability in relation to telecommunications services provided to the User.
- b) The User's End Device is beyond the control of the Bank. The User is responsible for taking the appropriate measures (e.g. security updates) to ensure the best possible protection of his/her End Device. The User shall bear the risk of unauthorized interception or spying of his/her data, provided that the Bank has exercised such degree of care as is customary in business. The Bank declines any liability in this regard. Likewise, the Bank does not accept any liability for damages incurred by the User as a result of transmission errors, careless handling of biometric information as per Section 3.4.b) and c) above, technical defects, overload, interruptions (including system-related maintenance work), disruptions, as well as unlawful interference or as a result of data transfer via unprotected communication channels, in particular e-mail and SMS, and in relation to errors/problems that may arise in the normal design/or presentation of the Cembra App or that relate to programs that affect the hardware or software involved in the use of the Cembra App (i.e. programs for which the Bank is not responsible and which therefore do not fall within the Issuer's sphere of control). **The Bank never requests the User by e-mail or SMS to provide usernames, login keys, mTAN codes, Access Code, PIN, Mastercard ID check code, account number or card number.**

- c) The User may not set up and/or use the Cembra App on a 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 Cembra App must be kept up to date at all times.

4 Use of the Cembra App

4.1 Scope of license

- a) Following full installation of the Cembra App and successful completion of the registration and authentication process, the Bank grants the User a non-exclusive, non-transferable and non-sub-licensable right to access and use the Cembra App and the Cembra App functionalities and services (“App Functionalities”) on his/her End Device. The User is entitled to download and install one (1) copy of the Cembra App and to use the Cembra App for personal, non-commercial use and only in accordance with these Terms and Conditions of Use.
- b) The Bank reserves the right to discontinue offering the Cembra App and the App Functionalities at any time and without stating reasons. Upon discontinuation of the Cembra App and the App Functionalities for whatever reason, the right granted to the User in accordance with these Terms of Use for the use of the Cembra App or the App Functionalities shall automatically lapse.
- c) The Cembra App, including source code, layout, structure, software, and the content provided by the Bank via the Cembra App shall remain the intellectual property of the Bank (or of its licensors who have granted a sub-licensable right to use the Cembra App). All trade marks, copyrights, patents, know-how and other or similar intellectual property rights shall remain vested in the Bank or its licensors. The User acknowledges that he/she does not acquire any of the aforementioned intellectual property rights, but only a license to access and use the Cembra App and the App Functionalities.
- d) The User grants the Bank a worldwide, unlimited, non-exclusive, royalty-free, sub-licensable and transferable right specifically to use, reproduce, distribute, create derivative works and display the information (and the content thereof) uploaded and sent by the User which the User stores, sends or receives via the Cembra App and services. The rights granted by the User are limited to the purpose of operating and providing the Cembra App and the App Functionalities. The User confirms that he/she holds all necessary rights in relation to the uploaded content.

4.2 General Terms and Conditions of Use of the Cembra App

- a) The Cembra App may only be installed on an End Device owned by the User and to which he/she alone has permanent access.
- b) Any person who installs and uses the Cembra App in accordance with the Terms and Conditions of Use shall be deemed by the Bank to be the authorized user of the Cembra App. The User acknowledges that third parties who register or log in using his/her End Device or Access Data shall be deemed to be authorized to issue binding instructions to the Bank. This also applies to the verification or confirmation of movements in the credit card account that the Bank obtains from the User via SMS or push messages (e.g. Mastercard ID check for transaction verification). Accordingly, the instructions received from third parties shall be deemed to have been issued by the User unless he/she has complied with all the security and due diligence obligations specified in Section 3 above and in the Product GTCs.
- c) The User may only use the Cembra App and the App Functionalities for personal, non-commercial and non-public purposes and in accordance with these Terms and Conditions of Use and the Product GTCs.

In particular, the User:

- i) may not use the Cembra App and the App Functionalities in an unlawful manner or in a manner that goes beyond or differs from a natural person’s non-commercial use for private purposes. If such use proves to have taken place, the Bank reserves the right to ban the User from using the Cembra App and the App Functionalities.
- ii) may not decompile the Cembra App source code (reverse-engineer it, i.e. create a human-readable

source code from the Cembra App machine or object code using a computer program or other technical process) or disassemble it (i.e. convert the binary encoded machine language of the Cembra App into human-readable assembly language using a computer program or other technical process), may not access, decode, modify or edit the Cembra App, except as permitted by applicable law, or create derivative software based on the source code, in order to produce, transmit and/or sell derivative works or to visualize the Cembra App or parts thereof using technical aids or functions (e.g. "framing").

- iii) may not modify, copy, recite, transfer, share, display, perform, reproduce, publish, send, offer, lease, sell, sublicense, distribute or otherwise commercially exploit or make available for sale the content provided by the Bank (including but not limited to texts, tables, pictures, videos, graphics, programs and other app services) to or for third parties without the express written consent of the Bank.
 - iv) may not disclose his/her Access Data (in particular, the access code or biometric information) of the Google Play Store and the Apple Store to third parties without the prior written consent of the Bank. The User is responsible for safeguarding the Access Data and must protect it from unauthorized access.
- d) The User may upload the credit card(s) in his/her name to payment applications (e.g. Apple Pay or Samsung Pay) and to other payment solutions (e.g. Mastercard Click to Pay) via the Cembra App. In doing so, the User must comply with the relevant product terms and conditions for the use of Bank credit cards on mobile end devices (hereinafter "Mobile Payment Terms") and the terms and conditions for the use of Cembra credit cards for Click to Pay payments ("Click to Pay Terms"). The current versions of the Mobile Payment and Click to Pay Terms are available at the following link: www.cembra.ch/agb. In order to use the payment application and the Click to Pay payment solution, the User may activate the credit card via various channels (e.g. via app, SMS or telephone call). To this end, the User may be sent a one-time activation code to the last mobile telephone number that the User notified the Bank of. The Bank is not obliged to allow the User's credit card to be registered on payment applications and on other payment solutions.

4.3 Notifications when using the Cembra App

Using the Cembra App means that the Bank may send the User electronic messages (hereinafter "Notifications"). Notifications from the Bank may be sent to the User via the following electronic communication channels:

- Push messages, provided they have been activated by the User in the course of registering or using the Cembra App as a communication channel;
- In-app messages, insofar as they have been activated by the User for certain functions of the Cembra App, or insofar as the notification to be sent by the Bank is made in order to safeguard the Bank's own legitimate interests and provided the interests of the User do not override them;
- SMS, for registration purposes and updating the User's contact information on the Cembra App. Furthermore, the Bank may send the User SMS Notifications in order to safeguard its own legitimate interests, insofar as the interests of the User do not override them;
- e-mail, insofar as the User has provided the Bank with his/her e-mail address and has consented to its use in order to communicate with the Bank and/or to receive information about the products and services offered by the Bank, Group companies and third parties.

The selection or activation of push or in-app messages shall apply to all existing and future bank products of the User in the Cembra App.

4.4 Functionalities of the Cembra App

a) In the Cembra App, the User may generally:

- access his/her personal information (e.g. telephone number, residence or e-mail address) and change it;
- manage his/her bank product(s) and inspect his/her transactions and monthly statements;
- send the Bank certain enquiries or documents (e.g. objections as regards monthly statements) ;
- Pay bills with your credit card account (Scan2Pay function).

This list is not exhaustive. The User is free to choose additional App Functionalities in relation to his/her bank product(s). **The User acknowledges that the use of certain app functionalities may incur fees that are directly associated with his/her bank product. For further information, please refer to the fee schedule in the corresponding Product GTCs.**

In addition, the User may, inter alia, switch on and off certain functionalities in relation to sending notifications in the Cembra App. These include, in particular, Notifications:

- regarding product-relevant information;
- with customized information and offers from the Bank, Group companies and third parties based on the User's preferences;
- about products and services offered by the Bank, Group companies and third parties;
- which require the User's consent (e.g. push messages).

Notifications sent in the Bank's own interest and that of the User and which cannot be activated or deactivated by the User. This includes, but is not limited to, Notifications:

- in relation to collection measures of the Bank;
- to verify or confirm transactions (e.g. by using the Mastercard ID check);
- in the event of maintenance work that does not enable access to the Cembra App.

- b) The Cembra App shall be further developed on an ongoing basis. Existing and new functionalities of the Bank may be replaced or expanded. The registered User may be provided or shown new functionalities introduced by the Bank upon updating his/her End Device or in the Cembra App itself. The Bank shall inform the User in an appropriate manner, e.g. by means of Notifications, of further developments of the Cembra App and, where applicable, about any changes to these Terms and Conditions of Use. If the User's consent is required for the use of a new Cembra App Functionality, the Bank will obtain such consent accordingly in advance.

4.5 Transaction overview and details of the monthly bill

- a) The Cembra App may display transactions from the current and past billing periods of all existing bank products of the User with the Bank (e.g. cash withdrawals and payments, including the amount of the specific transaction and the name of the specific merchant). In addition, the Cembra App may display information on the monthly bill from previous billing periods (e.g. billing date, balance on invoice date, amount of minimum payment, cash withdrawals and payments made by the User). The Bank may also provide further information concerning the product relationship and the accounts held at the Bank.
- b) The User acknowledges that the Bank does not undertake to display information older than 12 months in the Cembra App.
- c) Transactions from the current billing period pursuant to Section 4.5.a) are not legally binding and are generally not displayed in real time in the Cembra App.
- d) The monthly bills provided to the User via the Cembra App are binding, subject to material errors and billing errors. The Bank shall notify the User via his/her End Device when new monthly bills are available. It is the User's responsibility to check the availability of new bills by accessing the Cembra App. The monthly bill or any other documents shall be deemed to have been delivered to the User as soon as they are provided in the Cembra App. If the amount of a bill is not paid on time, the Bank may, in its discretion, send reminders by push or SMS, display them in the Cembra App or send them to the last known email or postal address.

5 Terms and Conditions for the Use of Electronic Communication Channels

5.1 Acceptance of the Terms and Conditions / Revocation / Termination

By providing the e-mail address and electing to use his/her e-mail address for communication with the

Bank (hereinafter "Election"), the User agrees to the provisions of this Section 5. This Election and thus the scope of these provisions may relate either to e-mail or SMS as communication channels.

5.2 Scope of use

For the Bank, emails and SMS whose electronic sender address matches the email address provided by the User to the Bank shall be deemed to have been written by the User. This does not apply to cases of identity fraud (e.g. as a result of hacker attacks), provided that the User has complied with the duties of care specified in Section 3.4. Changes to the email address may be made by the User himself/herself in the Cembra App. The Bank reserves the right in individual cases to determine which information/data is communicated to the User via electronic communication channels. Notifications from the Bank shall be deemed to replace other forms of communication to the User unless otherwise specified.

The User must continue to comply with other forms of communication as set out in specific contractual provisions. Electronic communication channels do not replace such forms of communication.

5.3 Risks in communication via electronic communication channels

The Bank draws the User's attention to the following risks, in particular, when using electronic communication channels:

- Internet data transfer is only encrypted if a secure https connection is established. In many cases (including transmission via e-mail), however, unencrypted and open communication takes place via the Internet. The transmission of SMS is only partially encrypted, and the encryption is weak;
- the Internet is a worldwide, open network accessible to anyone. The way in which emails and SMS are transferred cannot be controlled, and transfer may also take place abroad. Accordingly, the confidentiality of data transferred by email and SMS is not guaranteed;
- emails and their attachments, as well as SMS, can be falsified or forged by third parties unnoticed the sender and recipient can be changed, and the authenticity can thus be misrepresented;
- emails and SMS can be deleted, misdirected or garbled during transfer due to technical errors/faults;
- by accessing websites, including clicking on links embedded in emails/SMS and opening data attachments, harmful computer programs such as viruses and Trojan horses may be implanted on the User's computer.

5.4 Duties of care

In cases of electronic communication, the User shall particularly comply with the following duties of care:

- Operating systems and browsers must be kept up to date (particularly security settings and updates). State-of-the-art security measures must be used (e.g. firewall and antivirus program);
- in case of doubt as to whether an email or SMS was actually sent by the Bank, the email or text message should only be opened or the information contained therein followed after consultation with the Bank.

5.5 Exclusion of liability

The Bank shall only be liable in connection with electronic communication and the exchange of data via electronic means in cases of wrongful intent and gross negligence. The Bank excludes any liability for losses arising out of or in connection with communication and the exchange of data via electronic means, to the extent permitted by law. **In connection with open communication via email and SMS, the User also expressly accepts the risk that his data may be intercepted or published by third parties during transfer and that confidentiality is not guaranteed in this respect.** The Bank, in turn, cannot guarantee that e-mails or SMS showing the sender as the Bank were actually sent by the Bank; or the e-mails and SMS sent by or to the Bank are received unchanged, on time and by the correct recipient.

5.6 Revocation and termination

The User may, at any time, revoke his/her consent to reciprocal communication with the Bank and to the receipt of information about the products and services offered by the Bank, Group companies and third parties. In individual cases, the User revoke his/her consent by deactivating certain functionalities in the

Cembra App itself. The Bank may suspend the use of electronic communication at any time and the exchange of data via electronic communication channels without stating reasons. The Bank will inform the User about such suspension in an appropriate manner.

6 Fees

The Bank is at all times entitled to adapt or introduce fees in connection with existing and future App Functionalities. Any new fees or adjustments to fees shall be notified to the User via appropriate means (e.g. via the Cembra App or by post).

The User shall be responsible for paying all fees, costs or expenses charged by the mobile and/or telecommunications provider for or in connection with downloading and/or using the Cembra App. As regards data transfers by the User 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 User and his/her provider shall apply.

7 Exclusions of warranty and liability

7.1 No representations or warranties by the Bank

All warranties, representations and guarantees on the part of the Bank are, to the extent permitted by law, hereby fully disclaimed.

Use of the Cembra App and its content and App Functionalities is at the User's own risk. The User is solely responsible for the security of his/her login credentials and for backing-up the uploaded data.

7.2 Non-availability of the Cembra App

The Bank shall endeavor to ensure the uninterrupted availability of the Cembra App. However, it cannot guarantee unrestricted access to the Cembra App or unlimited use of the Cembra App. The User has no claim of right against the Bank to undisrupted operability, compatibility with other systems, fast reaction time or availability of the Cembra App or its contents or the App Functionalities at any time.

The Bank reserves the right to change or discontinue the Cembra App, its content and the App Functionalities at any time and without prior notice. The availability of the Cembra App may also be interrupted at any time, for example for purposes of undertaking maintenance, repairs and improvements.

Furthermore, the Bank does not provide any warranty on behalf of network operators, the manufacturers of the End Device of the User or for the software operated therewith, or on behalf of other third parties.

7.3 Exclusion of liability

To the extent permitted by law, the Bank hereby disclaims any and all liability on its part (regardless of the legal basis thereof). In particular, the Bank does not accept any responsibility for the availability of the Cembra App and shall not be liable for damages (including direct or indirect damages and losses, consequential losses, lost profits, loss of use or unrealized savings) resulting from disruptions, interruptions, failures or overloads of the IT systems of the Bank or of third parties commissioned by it, of mobile and/or telecommunication providers or the internet, or where it is not possible for other reasons to use the Cembra App, or otherwise in connection with the use, functionality or availability of Cembra App, its contents and the App Functionalities.

If unauthorised third parties access the Cembra App and carry out transactions using Scan2Pay, such transactions shall be deemed to have been carried out by the Cardholder unless the Cardholder can prove that he has complied with all due diligence obligations at all times. The Bank is expressly not liable for such transactions.

The liability provisions of the relevant Product GTC shall apply unchanged.

8 Data protection and confidentiality, waiver of bank-client confidentiality

8.1 Categories of personal data

When registering, logging in or using the Cembra App, the Bank may process the following personal data of the User (hereinafter “User Data”):

- Data relating to the User’s mobile End Devices (e.g. information about the device manufacturer and type, operating system, device ID and IP address);
- Data for accessing the Cembra App (e.g. username, login key) or the desired settings of the User (e.g. saving of the username or login key or use of other login functions (e.g. Face or Touch ID));
- Data concerning the use of the Cembra App (e.g. number of accesses to the Cembra App, including date and time), changes to the User’s personal details (e.g. telephone number, residence address or email address), consent to the Terms and Conditions of Use of the Cembra App or to other terms and conditions of the Bank;
- Data relating to the bank product registered on the Cembra App (e.g. credit-card transaction data, monthly bills or payments);
- Data relating to communications (e.g. if the User communicates with the Bank by email, the Bank stores the exchanged information and the contact details of the User);
- Data relating to the habits and/or preferences of the User (e.g. information concerning the use of the Cembra App or the bank products, which the Bank analyses and in some cases is also supplemented with information from third parties).

8.2 Purposes of data processing

The Bank processes the user data listed in Section 8.1. for the purpose of implementing the contractual relationship and particularly:

- To enable registration of, login to or use of the Cembra App;
- To ensure the authentication of the User before using the Cembra App and before issuing instructions to the Bank;
- To provide the User with a secure connection between the Cembra App and the mobile End Device;
- For sending confirmation requests (e.g. sending notifications or SMS codes to verify or confirm a suspected credit card transaction) or information in connection with the User’s bank product (e.g. new bills, replacement of credit cards);
- To receive the information or enquiries transmitted by the User to the Bank via electronic channels.

The Bank may evaluate your use of the Cembra App and of the bank product registered on the Cembra App in order to better align its products and services to the User. If the Bank intends to send offers to the User electronically, it will obtain the User’s consent in advance. After the User has given his/her consent for this purpose, it may be revoked at any time.

8.3 Protection of user data

- a) The transmission of personal data and information between the Bank or the Cembra App and/or the User’s End Devices is encrypted. However, this does not apply to sending data and information by SMS and e-mail.
- b) Even if the sender and the recipient of Notifications (e.g. e-mail or SMS) are located in the same country, data transmission over the Internet often also occurs via third countries, i.e. even 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 faked 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.

8.4 Data processing abroad

The Bank may at any time outsource its services in connection with downloading, registering or operating the Cembra App in Switzerland or abroad. The recipients of the User's personal data may also be located abroad, including outside the European Union (EU) or the European Economic Area (EEA, including e.g. the Principality of Liechtenstein). The countries concerned may not have laws in place that protect the User's personal data to the same extent as in Switzerland or in the EU/EEA. If the Bank transfers the User's personal data to such a third country, it shall ensure the protection of the User's personal data in an appropriate manner. One means of this is the conclusion of data transfer agreements known as standard contractual clauses, which have been issued or recognized by the European Commission and the Federal Data Protection and Information Commissioner (FDPIIC), with recipients of the User's personal data in third countries which guarantee the necessary data protection.

8.5 Exclusion of liability and waiver of bank-client confidentiality

The Bank assumes no liability for the security of the User's data during transmission over the Internet. The Bank shall not be liable for direct or indirect damages resulting from the loss or unauthorized interception of the data by third parties. With regard to the data processing pursuant to Sections 8.1 to 8.4 above in connection with the Cembra App, the User expressly waives bank-client confidentiality.

9 Google Play Terms of Use and Apple Store Terms of Use

9.1 General provisions

The provisions of this Section 9 shall not result in any further obligations on the part of the Bank towards the User that do not already arise from other provisions in these Terms of Use.

9.2 Google Play Terms of Use

- a) Notwithstanding anything to the contrary in these Terms of Use: (i) the User has no further rights to the Cembra App or to use same, except as provided by the Google Play Terms of Use; (ii) the Cembra App may not be used in any manner contrary to the Google Play Terms of Use; and (iii) the Cembra App may only be used with products as permitted by the Google Play Terms of Use.
- b) Both the User and the Bank, as the provider of the Cembra App, acknowledge and agree that: (i) these Terms and Conditions of Use constitute an agreement between the User and the Bank; (ii) Google LLC is not a party to these Terms of Use; (iii) solely the Bank, and not Google LLC, is responsible for the Cembra App in accordance with these Terms and Conditions of Use; (iv) Google LLC is under no obligation to maintain the Cembra App or to provide support for the Cembra App; (v) Google LLC shall not be liable for non-compliance with any applicable guarantees or warranties for the Cembra App, and the Bank shall be solely responsible in accordance with these Terms of Use for any claims, losses, damages, liabilities, costs or expenses resulting from non-compliance with any applicable warranties for the Cembra App; (vi) the Bank, and not Google LLC, is liable under these Terms of Use for any obligations relating to the Cembra App or to the access to and use of same, including but not limited to: (1) product liability claims; (2) claims resulting from the Cembra App failing to comply with applicable legal or regulatory requirements; and (3) claims arising from consumer protection law and similar provisions; (vii) in the event that third-party claims are asserted based on an alleged infringement of intellectual property rights by the Cembra App or the User's disposal and use of the Cembra App, the Bank, and not Google LLC, shall be solely responsible in accordance with these Terms of Use for the investigation, defense, settlement and discharge of disputes in connection with such infringement claims; and (viii) Google LLC and its affiliates are third parties to these Terms of Use, and the User, by consenting to these Terms of Use, grants Google LLC and its affiliates the right to enforce these Terms of Use against the User as a third-party beneficiary under these Terms of Use.
- c) The User represents and warrants that: (i) he/she is not located in a country subject to a U.S. government embargo or classified by the U.S. government as a "terrorist-supporting country"; and (ii) he/she is not included in a U.S. government-issued list of prohibited or restricted parties.

9.3 Apple Store Terms of Use

- a) Notwithstanding anything to the contrary in these Terms of Use, the User has no further rights to use the Cembra App beyond the rules of use set out in the Apple Store Terms of Use (hereinafter "Apple Rules of Use"). The User may not use the Cembra App in any manner contrary to the Apple Rules of Use, and the User may only use the Cembra App on an Apple product with iOS which the User owns or controls as permitted by the Apple Terms of Use.
- b) The User and the Bank each acknowledge and agree that (i) these Terms of Use are being concluded between the User and the Bank and not with Apple Inc., (ii) the Bank, and not Apple, is solely responsible for the Cembra App, (iii) Apple shall have no obligation whatsoever to provide any maintenance or support services with respect to the Cembra App, (iv) if the Cembra App fails to conform to any applicable representation, the User may notify Apple, and Apple will refund to the User the purchase price paid by the User for the Cembra App and, to the extent permitted by applicable law, Apple shall have no further warranty obligation with respect to the Cembra App, and, as between the Bank and Apple, any other claims, losses, liabilities, damages, costs or expenses attributable to any failure to comply with any warranty, on the provisions of these Terms of Use, shall be the sole responsibility of the User, (v) the Bank, not Apple, shall be responsible for addressing any claims made by the User or any third party in connection with the Cembra App or its possession and/or use of the Cembra App, such as: (1) product liability claims, (2) the assertion that the Cembra App is in violation of applicable statutory or regulatory requirements, (3) claims arising from consumer protection or similar laws, (vi) in the event of claims made by third parties that the Cembra App or the fact that the User owns and is using the Cembra App infringes the intellectual property rights of that third party (in relations between the Bank and Apple, the Bank, and not Apple, is solely responsible for investigating, defending against, settling and discharging such intellectual property infringement claims, and (vii) Apple and its affiliates are third-party users of these Terms of Use; if the User accepts the terms of these Terms of Use, Apple and its subsidiaries shall have the right (and Apple and its subsidiaries have accepted such right) to enforce these Terms of Use against the User as a third-party beneficiary of the Terms of Use. The User represents and warrants that: (i) he/she is not located in a country that is subject to an embargo by the U.S. government or that has been identified by the U.S. government as a "terrorist-supporting country"; and (ii) he/she is not included in a U.S. government-issued list of prohibited or restricted parties.
- c) The User must comply with the applicable terms and conditions of third parties when using the Cembra App. The use of the Cembra App is at the User's own risk. Data (including geolocation data) may be imprecise.

10 Further provisions

10.1 Blocking and termination

The Bank is entitled to block access to the Cembra App or individual App Functionalities temporarily or permanently for all or individual Users at any time, without prior notice and without stating reasons. The User may give notice to terminate these Terms of Use at any time.

10.2 Amendments to the Terms of Use

The Bank reserves the right to amend these Terms and Conditions of Use at any time. Such changes shall be notified to the User by appropriate means (e.g. letter, email, SMS or Notification in the Cembra App) and shall be deemed to have been approved unless the User objects within a period of 30 days.

10.3 Invalidity / Further provisions

Should parts of these Terms of Use be invalid in whole or in part or if these Terms of Use contain gaps, this shall not affect the validity of the remaining provisions. In lieu of the invalid or missing provision, such valid provision shall be deemed to have been agreed as best reflects the commercial objectives pursued by the parties.

In all other respects, the relevant Product GTCs shall apply, which shall take precedence over these Terms

of Use in the event of any conflicts. The above provisions of Sections 8.1. to 8.4 shall apply to data processing to supplement to the data protection provisions of the relevant Product GTC. For further information concerning data processing and data protection standards in relation to the use of the Cembra App, please refer to the Cembra App Privacy Policy. The current version of the Cembra App Privacy Policy can be viewed in the Cembra App and via the following link: www.cembra.ch/cembra-app-privacy-policy-en.

10.4 Assignment of the Terms and Conditions of Use

These Terms and Conditions of Use and parts thereof, as well as rights and obligations arising from these Terms and Conditions of Use, may not be assigned by the User to third parties without the prior written consent of the Bank.

10.5 Applicable law and jurisdiction

Exclusive jurisdiction over all disputes in connection with these Terms of Use is vested in the courts of Zurich 1. Swiss law shall apply, to the exclusion of any conflict of laws provisions.

The choice of law clause and the jurisdiction clause in accordance with this clause 10.5 shall not apply if and to the extent that the User is a consumer within the meaning of Swiss law or a consumer within the meaning of another legal system and that the User has a compulsory right to invoke the application of another law and/or the jurisdiction of another court under the relevant legal system.

11 Contact details of the Bank

The Bank, Cembra Money Bank Ltd., is a company limited by shares under Swiss law with its registered office in Zurich. It may be contacted at the following postal address, by email or by telephone.

Cembra Money Bank Ltd.
Bändliweg 20
8048 Zurich
Switzerland

Email: info@cembra.ch

Phone no. +41 (0)44 439 40 23

Further information on the Bank can be found on the following website: www.cembra.ch

V03/10.2024