

# E-Banking

## General Terms of Use (GTU)

### 1. Service offered

1.1 The e-banking service offered by the Neue Bank AG (hereinafter referred to as the “bank”) allows the account holder to inspect and transact his/their business relationships via e-banking and, where needed, to make this possibility available to an authorised person. The bank reserves the right to change the service offered at any time.

1.2 The exchange of data governed by these terms of use extends to all banking transactions based on separate contracts or conditions of business of the bank (e.g. General Terms and Conditions of Business). Within the scope of the services desired by the account holder via e-banking, the following provisions take precedence to the extent they contain deviating rules.

### 2. E-banking access

2.1 Technical access by the user to the services is via internet using any provider as desired by the user. In this regard and in the following, “user” means the account holder and persons authorised by the account holder to use e-banking.

2.2 Access to the e-banking services is granted after entry of the following authentication details:

- a) contract number
- b) password
- c) changing authorisation number in accordance with the matrix/security card made available by the bank or other means of authentication (hereinafter referred to as the “means of authentication”). The authentication details are dispatched to the mailing address provided by the account holder.

2.3 Anyone providing authentication in accordance with point 2.2 is deemed authorised to use e-banking in relation to the bank. The bank may allow the user to make queries and place orders within the framework and scope of the authorisations selected pursuant to the e-banking agreement, even without further verification.

2.4 Orders and instructions via e-banking are deemed authored, authorised, and sent by the account holder or the user acting on the account holder's behalf, irrespective of limitations to the internal arrangements between the account holder and the user acting on the account holder's behalf and notwithstanding any Commercial Register entries, publications, or arrangements on the bank's signature documents to the contrary. The bank is therefore deemed to have executed properly if, pursuant to a correct verification of authentication according to point 2.2, the bank complies with the messages, instructions, and orders it receives within the framework of the e-banking agreement.

2.5 Without reservation, the account holder recognises all transactions posted to his accounts and custody accounts referred to in the e-banking agreement as well as in any supplements that have been performed using e-banking in connection with his personal authentication or that of another user, especially without a written order.

### 3. Placing of orders

3.1 The user may use e-banking around the clock. The bank's execution of orders placed, especially of market and payment

orders, is however dependent on the operating hours of the bank and other involved institutions and systems, such as markets, settlement systems, and clearing systems. Product-specific dead-lines (cut-offs) and applicable lead time for execution (for financial instruments of issuers outside the EEA and North America, up to 48 hours or more) must in any event be taken into account. Trades placed outside the bank's business hours and exceeding CHF 250'000.00 or counter value will be sent to the execution venue on the following working day.

3.2 Orders are placed by sending the relevant data. After the data is received by the bank, the bank processes the order. A placed order may be revoked only if direct contact is made on time, i.e. before the order has been executed. If an order (e.g. payment or market order, etc.) was placed with the bank electronically, and if it is ascertainable after placement of the order that the order has not been executed by the bank in accordance with the order or only partially so, the user is required to complain immediately to the bank in this regard.

3.3 Before sending the data, the user must check all the data for completeness and correctness. The risk of misrouting or return arising from entry of incorrect or incomplete information is borne by the account holder.

3.4 The bank has the right, at any time and without providing reasons, to refuse to give information and accept instructions, orders, and messages via e-banking and to demand written authorisation.

3.5 The bank processes the orders, instructions, and messages it receives via e-banking in the context of the overall client relationship. It therefore reserves the right especially to refuse execution of orders because of lack of funds or insufficient credit limit.

3.6 The bank does not accept orders or instructions via e-mail, since neither integrity nor authenticity can be ensured by that means.

3.7 The account holder notes and agrees that no advice is given for market orders placed via e-banking. The bank does not check whether market orders placed via e-banking are compatible with any investment goal and associated investor profile agreed between the account holder and an authorised person or the bank.

3.8 The user checks all market orders for compatibility with the financial status of the account holder and, by placing the order, confirms that he is familiar with the practice and customs of market transactions, especially the structures and risks of the various types of transaction.

Otherwise, the user must consult a client advisor of the bank and obtain relevant clarification. If market orders are placed without having received prior relevant advice by the bank and without having studied the current sales documents, especially any public prospectuses, the user and/or the account holder bear the risk. The bank does not assume any liability for such orders.

3.9 The bank is entitled to refuse or cancel market orders if they are not in accordance with the relevant norms governing the transaction and market location in question.

3.10 The account holder is aware that e-banking is not suitable for speculating with equities and derivatives over the course of a day or for taking advantage of shortterm price fluctuations (day trading). The account holder accepts that securities bought via e-banking may, due to the way the system is set up, not be sellable again on the same day.

3.11 Any information available to the user by e-banking does not constitute (investment) advice, submission of an offer, or a request to conclude certain transactions with the bank, but rather serves information purposes exclusively (e.g. to facilitate the investment decisions made by the user independently).

#### **4. E-documents / electronic mail**

4.1 If "e-documents" is agreed, correspondence will be sent only via e-banking in the context of e-banking. However, the bank reserves the right to send notifications by other suitable means.

4.2 The user undertakes to regularly retrieve and store the electronic mail. It is at the bank's discretion how long it leaves the correspondence in the e-banking user's mailbox. In any case, it will be available for at least three months from the date of creation.

4.3 The user acknowledges that the documents in the electronic mailbox are deemed to have been delivered with legal effect and that any deadlines begin to run from the date of delivery. The account holder is liable for any damages and disadvantages resulting from delayed or uncollected correspondence in the electronic mailbox.

4.4 The account holder may instruct Neue Bank AG at any time to send correspondence in paper form only.

4.5 If the account holder no longer wishes to receive correspondence electronically and the bank is unable to deliver it physically (e.g. due to lack of knowledge of the current address), the bank is entitled to hold all client correspondence at the bank ("retained mail"). Legally effective delivery shall also apply to this correspondence. If the "electronic mail" form of delivery is terminated, correspondence will not be automatically sent by post in physical form to the user authorised to correspond electronically, unless the account holder has also designated this user as the recipient of the physical mail.

#### **5. Obligations of the user**

5.1 The user receives his contract number, his initial password, and the means of authentication from the bank by post. The user is required to keep the password and the means of authentication separate from each other, to keep them secret, and to protect them from misuse by unauthorised parties.

5.2 The user is required to change the initial password sent to him by the bank immediately after receiving it and to do so again later at regular intervals. In particular, the user may not record his password once he has changed it. The password may be between 12 and 65 characters (digits and/or letters). Passwords may not consist of easily determinable codes such as telephone numbers, birth dates, car numbers, names of persons close to the user, etc.

5.3 The obligation to keep the password and the means of authentication secret applies to every individual user separately. The bank is not liable for any losses arising from the fact that the user or other third parties misuse the authentication details of other users.

5.4 If there is a suspicion that an unauthorised party might have gained knowledge of the password or other authentication details of the user or if the means of authentication are no longer in the user's own possession, then the user is required to communicate this without delay to the bank during the usual business hours and to confirm it in writing immediately. The bank without delay arranges for the personal authentication details to be blocked. Any associated costs are borne by the account holder.

5.5 The user may and - in the event of risk of misuse - must however himself block his own access to e-banking at any time, also outside the bank's business hours, by entering a wrong password three times in a row or by having the bank block his authorisation (see point 6).

5.6 The user is required to minimize the security risks arising through use of the internet by employing appropriate security measures (especially password protection, antivirus programs, firewalls, etc.) corresponding to the current state of technology. The user also is required to take note of the security information provided on the websites of the services used or made available to him in other form and, where appropriate, to take the recommended security measures within a useful time period.

5.7 The user must without delay inform the bank of any recognisable malfunctions and irregularities.

#### **6. Exclusion of warranty and liability**

6.1 The account holder bears all risks arising from any disclosure of his authentication details or those of other users. The account holder bears all consequences of the authorised or improper use of these authentication details.

6.2 The bank is not liable for any losses and/or any loss of profits incurred by the account holder as a result of transmission errors, technical defects, interruptions of transmission, delays, omissions, malfunctions of any sort, or unlawful interference by third parties in telecommunication facilities or the internet as well as as a result of using the open network, through interruptions and time lags, especially in the processing of orders, due to network overload, malicious blockage of electronic access by third parties or inadequacies on the part of the network operator. The bank accordingly excludes all liability for any losses that may arise from the use of the internet and additional peripheral devices.

6.3 The bank assumes no liability for the correctness and completeness of the data, information, and messages it transmits. In particular, all information concerning accounts and custody accounts (balances, statements, transactions) and generally available information such as market prices and currency exchange rates are deemed preliminary and non-binding. Only the official bank statements and receipts and other documents prepared by the bank are legally binding, but not the statements, reports, and compilations printed out from the e-banking system. E-banking data do not constitute binding offers, unless they are expressly labelled as such.

5.4 Furthermore, the bank expressly excludes any liability for the user's terminal equipment as well as for technical access to e-banking. The bank also refuses all liability for any software it delivers e.g. by way of data carrier, download, etc., unless it receives a complaint within one week of delivery. All liability is excluded for any losses arising from and during the transport of software via internet. The bank also does not guarantee that the e-banking program meets the expectations and wishes in all points or that it works flawlessly in connection with other programs chosen by the user. The bank does not assume any liability for any losses or malfunctions during the operation of e-banking due to computer viruses in the user's system.

6.5 In its determination of security risks, the bank reserves the right at all times to interrupt e-banking for the protection of the account holder until the risks have been removed. The bank is also entitled to interrupt e-banking for other maintenance work.

6.6 The bank is expressly released from liability for losses suffered by the account holder as a result of malfunctions, interruptions referred to in point 5.5, especially in processing or in the case of overloaded IT systems of the bank, unless the bank is grossly negligent. The bank is in no event liable for loss of profit or consequential losses.

6.7 The bank cannot verify who receives and uses the means of authentication. Especially in the case of legal persons and/or delivery to a business address, it is the sole responsibility of the account holder to monitor receipt of the means of authentication and the use thereof. The account holder must bear the risks arising from manipulations of his computer or of another user's computer by unauthorised parties.

6.8 The bank assumes no liability for losses incurred by the account holder due to the account holder's lack of legal capacity or that of another user.

6.9 The bank assumes no liability for slight negligence. In particular, the bank excludes liability for slight negligence:

- for orders not executed or not executed on time and resulting losses;
- for losses caused by its assistants in the performance of their duties.

6.10 The bank assumes no liability for the failure to execute orders or the delayed execution of orders or the resulting losses, especially due to price losses, unless it is grossly negligent.

## 7. Blocking of e-banking access

7.1 The account holder may have his access or that of another user to the relevant e-banking services of the bank blocked. Access to the accounts and custody accounts via e-banking is automatically blocked if three attempts have been made to access the services with a wrong password and/or a wrong authentication number.

7.2 The bank is entitled to block the access of a user to individual or all services without providing reasons and without prior cancellation.

## 8. E-banking authorisations

8.1 The authorisation of users by the account holder to make use of e-banking persists until the bank receives a revocation in writing. It is expressly stipulated that a granted authorisation does not expire upon the death or loss of legal capacity of the account holder, but rather remains in effect until revoked in writing and notwithstanding any Commercial Register entries and publications to the contrary. This provision is subject to point 6.2.

8.2 The revocation or the amendment of the signature rights of a user on the account holder signature forms deposited at the bank do not bring any change concerning authorisation granted by the account holder to use e-banking, unless expressly indicated. Rather, such a change requires express revocation according to point 7.1.

## 9. Banking secrecy

The account holder notes that due to the design of the internet, its use as a transmission medium may result in client-specific data being transmitted in an uncontrolled manner to third countries, even if the sender and the recipient are located in the same country (e.g. Liechtenstein). Liechtenstein banking secrecy applies solely to data located in Liechtenstein. Foreign legal orders often have no protection of the account holder's or authorised persons' privacy comparable with the banking secrecy of the bank maintaining the account. Senders and recipients are transmitted without encryption over the internet. It may therefore be possible for third parties to draw conclusions about existing banking relationships. Likewise, the account holder accepts that information of the bank for which the user requests separate transmission via e-mail, text message, etc., is generally transmitted without encryption, so that banking secrecy is not preserved and/or cannot be guaranteed.

## 10. Security on the internet

10.1 When the e-banking system was developed, special attention was paid to the aspects of security. A multilevel security system was developed which also uses cryptographic procedures of a high standard. Because of encryption, unauthorised parties are as a general rule not able to see confidential user data. But despite the security precautions, which correspond to the most current level of technology, absolute security cannot be guaranteed on the side of either the bank or the user. The account holder notes that especially his computer workplace or that of another user may constitute a vulnerability for e-banking.

10.2 In particular, the account holder notes the following risks:

- The bank cannot guarantee either unrestricted access to the relevant services or unrestricted use of such services. Nor can the bank guarantee unrestricted availability of the internet.
- Insufficient knowledge of the system and lack of security precautions may facilitate unauthorised access (e.g. insufficient protection of data stored on the hard disk, file transfers, residual screen

images, etc.). It is the responsibility of the account holder and/or another user to obtain precise information on the requisite security precautions and to comply with them.

- By compiling traffic characteristics, the internet provider of the user has the possibility of tracing when the user entered into contact with whom.
- There is a latent danger that a third party gains unnoticed access to the user's computer during use of the internet (e.g. using trojans, viruses, etc.).
- There is a permanent danger that computer viruses may spread on the computer of the user during use of the internet as soon as the computer makes contact with the outside world, whether via computer networks or data carriers. Virus scanners may support the user's security precautions and are urgently recommended.

10.3 Beyond this, the importance of using software exclusively from trustworthy sources must be noted.

## 11. Cancellation/dissolution with immediate effect

The e-banking agreement is valid for an indefinite period and may at any time be cancelled in writing and with immediate effect by either party, without indicating reasons. The bank is however entitled to delete access to e-banking without cancellation if the e-banking services have not been used for a period of at least 12 months.

## 12. Reservation of legislative provisions

These General Terms of Use are subject to legislative provisions that may affect the operation and use of e-banking. In this regard, supplemental reference is made to the disclaimer on the bank website ([www.neuebank.li](http://www.neuebank.li)).

## 13. Partial invalidity

The invalidity, illegality, or lack of enforceability of individual or multiple provisions of the e-banking agreement and these General Terms of Use do not affect the validity of the other parts of the agreement. The provisions not applicable in this way are to be replaced by new provisions that are as close as possible in terms of their legal and economic purpose.

## 14. Foreign legal orders

The account holder notes that when using e-banking from a foreign country, the account holder and/or another user may in some cases be violating rules under the law of his domicile, such as import and export restrictions on encryption algorithms, or other foreign law, and/or the use of e-banking of the bank may be prohibited. It is the responsibility of the account holder and/or another user to obtain information in this regard. The bank refuses all liability in this regard.

## 15. Exclusion of certain persons

15.1 When using the e-banking service in a foreign country, the user must comply with any local restrictions (e.g. import and export restrictions for encryption algorithms). It is the responsibility of the user to obtain information on the relevant applicable (foreign) laws and regulations and to comply with them. The bank refuses all liability arising from such breaches of duty by the user.

15.2 The bank is entitled without prior notice to modify or limit the e-banking services for users in foreign countries.

## 16. Amendments

Amendments of e-banking provisions are notified to the account holder in writing or via e-banking itself. The amendments are deemed accepted as soon as an e-banking service is used again despite the amendments or if no written objection has been received by the bank without 30 days after their disclosure.

## 17. Client data

The account holder agrees that the bank may use his data for bank-internal statistical purposes.

#### 18. Integral part

In all other respects, the “General Terms and Conditions of Business” and the “General Provisions for Payment Services” of the bank shall apply. They constitute an integral part of the “General Terms of Use”. The versions currently in force are available at [www.neuebank.li](http://www.neuebank.li).

Subject to special agreements, the standard terms and conditions of the bank shall apply for orders placed by the customer.

The bank reserves the right to introduce fees at any time for provision of e-banking and to adjust such fees to market conditions.

#### 19. Place of jurisdiction and applicable law

The exclusive place of jurisdiction for all disputes arising from this legal relationship and the place of performance are Vaduz.

The bank is however authorised to assert its rights also at the place of residence/domicile of the account holder or a user or at any other competent court. Exclusively Liechtenstein law is applicable to this legal relationship.

The account holder hereby confirms receipt and acceptance of the General Terms of Use. The account holder expressly agrees to include all users referred to in the e-banking agreement in these contract terms, to instruct them accordingly, and to accept all violations by such users as enforceable against the account holder.

#### Legal information

Please note that a client relationship with Neue Bank AG may be deduced through the downloading, installation, and/or use of this application and the associated links to third parties (e.g. App Store/Google Play, network operators, device manufacturers). Bank client confidentiality can no longer be guaranteed due to the possible disclosure of your banking relationship and bank client information to third parties (e.g. should you lose your end device).

# Mobile Banking

## General Terms of Use

By accessing the information, services, and contents made available via the mobile banking application («App») of Neue Bank AG («Bank»), the User and/or the person(s) authorised by the User (hereinafter «User») declares that the User has understood and recognises these Terms of Use. Otherwise, use of the App shall not be permitted.

The following Terms of Use supplement other agreements concluded between the User and the Bank, especially the E-Banking Agreement and the General Terms of Use for E-Banking (including the duty of care referred to therein relating to the safekeeping and management of access data). All of these agreements constitute integral parts of these Terms of Use.

### 1. Addressees

The information, services, and contents (hereinafter «information») made accessible by using the App is addressed solely to Users residing or domiciled in the European Economic Area (without Croatia). In particular, the information accessible via the App is not intended for persons subject to a legal order that prohibits the publication of or access to such information (due to the nationality of the person, the person's residence, or other reasons). Persons to whom such restrictions apply are not permitted to access the information. This applies in particular to persons residing in the United States or Canada.

### 2. No offer/no advice

The information published in this App does not constitute investment advice, an invitation, an offer, or a recommendation to buy or sell investment instruments, to carry out certain transactions, or to conclude any other legal transaction. It is for information purposes only and in no way replaces personal advice by qualified specialists. If the User is interested in a specific investment product, the Bank recommends that before making the investment decision, the User carefully study the complete product documentation as well as the information brochure entitled «Risks in Securities Trading» published by the Liechtenstein Bankers Association and also to have a specialist of the User's choosing examine the consequences, including under tax law.

### 3. Personal data/Data security

The Bank does not use the App to collect any personal data, unless the User expressly makes the data available by way of a form or otherwise. In such cases, the Bank may use the personal information to market products and services that the Bank believes may be of interest to the User.

The App is based on the most recent security standards. Nevertheless, use of the App means that the User's data is transmitted via an open network accessible to everyone (internet). In some cases, the data may also circulate across borders, even if the sender and the recipient are located in the same country. This entails the risk that third parties may gain possession of certain data. The User assumes all risks that may arise from the transmission of such information or orders, especially those originating from transmission errors or misunderstandings. Through the use of the App, app providers (e.g. Apple, Google) gain possession of personal data that may be used by these companies. Please observe the data protection and business conditions of the relevant providers.

### 4. Access

Access to the information and functions of the App is granted to persons who have provided valid identification details for use of the App. Identification details are currently the contract number provided to the User by the Bank and the User-defined personal password. The Bank reserves the right to exchange or adjust the identification details at any time for objective reasons; the Bank communicates these changes to the User in advance in an appropriate manner. A person providing the valid identification details (self-identification) is considered by the Bank to be authorised to use the information and functions of the App. The Bank may thus, for example, allow that person to make or request queries and may accept orders and legally binding communications from that person within the scope of the services procured by the User without further verification of the person's authorisation; this also is the case if the person is not a person who is in fact authorised. Without reservation, the client recognises all transactions performed within the scope of the App's functions by way of the User's identification details or those of an authorised person. Similarly, all instructions, orders, and communications received by the Bank in this way are considered authored and authorised by the client.

### 5. Duty of care of the User

The Bank takes the measures customary in the banking industry to ensure the best possible security of the App. However, it is indispensable that the User fulfils the required duty of care to ensure effective protection from abuse.

This includes:

- Changing the password: The User is required to change the password regularly. The password may not be composed of easily determinable combinations (e.g. telephone number, date of birth, number plate, etc.);
- Confidentiality of identification details: The User is required to ensure that all identification details are kept confidential and are protected against abuse by unauthorised persons. In particular, the User must activate the lock code on the User's mobile end device (e.g. smartphone lock, screen lock) and log out by way of the «Logout» link after using the App. The identification details may not be stored unencrypted on the User's mobile end device or otherwise be recorded. The identification details may also not be given or made available to third parties (in particular no use permitted in connection with apps provided by third parties and no communication permitted to third parties requesting the User to divulge the identification details – the Bank will never ask the User to divulge the identification details outside the App);
- Change and blocking of identification details: The User is required to immediately change the identification details if there is reason to fear that unauthorised third parties have gained knowledge of one or more identification details of the User. If this is not possible, the User must contact the Bank to have access to the App blocked. In emergencies, access may also be blocked by entering a wrong password multiple times in E-Banking;
- Security measures: The User is required to minimise the risk of unauthorised access to the User's end device (e.g. via public electronic networks such as the internet) by employing suitable protection measures. In particular, operating systems and browsers must be kept up to date, e.g. the software updates and security patches made available or recommended by the provid-



ers must be installed immediately. The updates of the App made available by the Bank must also be downloaded and installed as soon as they are available. The usual security precautions for public electronic networks must also be taken, e.g. no malicious third-party software may be installed on the mobile end device. The User is in particular not permitted to run the App on a mobile end device whose security configuration has at least potentially been manipulated (e.g. by jailbreaking, especially unauthorised removal of usage restrictions on devices whose manufacturers have blocked certain functions by default). It is the responsibility of the User to continuously obtain information about the security precautions corresponding to the current state of technology as well as to read the security notices provided on the Bank's website ([www.neuebank.li](http://www.neuebank.li)) and to take the recommended security measures;

- Notification of the Bank: The User is required to immediately notify the Bank if there is reason to fear that unauthorised third parties have gained access to the end device.

## 6. Risks

Pursuant to the identification agreement set out in clause 4, the client shall bear all the consequences arising from the use – including abuse – of the User's identification details or those of a person authorised by the User (e.g. in the event of unauthorised access by third parties, unless the Bank has breached the duty of care customary in the banking industry. The client shall also bear the consequences arising from breach of the User's duty of care pursuant to clause 5. Public and private data networks for the exchange of information and data as well as the User's mobile end device are part of an overall system that is beyond the control of the Bank. They may become a vulnerability within the system. In particular, they may be vulnerable to access or intervention by unauthorised third parties, or transmission errors (e.g. during the transmission of a market order), delays, system interruptions, or system breakdowns may occur. Moreover, loss of the mobile end device may result in unauthorised access to the client's data. The client cannot derive any claims against the Bank from such occurrences.

## 7. External links

Clicking on a link may result in leaving the App. The Bank assumes no liability for the contents, products, services, or objects offered on the linked pages. Use of the links is at the User's own risk.

## 8. Warranty

The Bank is unable to warrant that access to the information and functions of the App is free from malfunction and interruption at all times. The Bank reserves the right to interrupt the information and functions temporarily in order to defend against security risks or perform maintenance. The client bears any losses arising from a malfunction or interruption, unless the Bank breached the care customary in the banking industry.

When displaying and transmitted the data, information, communications (hereinafter «data») transmitted as part of the services offered, the Bank applies the care customary in the banking industry. The Bank excludes any warranty or liability for the correctness, completeness, and timeliness of the data that goes beyond this. In particular, information pertaining to accounts and custody accounts (balances, statements, transactions, etc.) as well as generally available information such as market prices or foreign exchange rates are preliminary and non-binding, unless they are expressly labelled as binding. Similarly, the data contained in the services constitute binding offers only if they are labelled as such.

## Legal information

Please note that a client relationship with Neue Bank AG may be deduced through the downloading, installation, and/or use of this application and the associated links to third parties (e.g. App Store/Google Play, network operators, device manufacturers). Bank client confidentiality can no longer be guaranteed due to the possible disclosure of your banking relationship and bank client information to third parties (e.g. should you lose your end device).

The Bank excludes any warranty or liability for freedom from defects of the software, for the ability to run the software on the mobile end device of the User, or usability of the software in combination with the other applications of the User or with the network or system operator used by the User. If errors are found in the software, the User shall immediately refrain from accessing the information and functions and inform the Bank.

In areas where the Bank is responsible for providing its services with the care customary in the banking industry, the Bank as a rule is liable only for direct and immediate losses of the client. Liability for indirect or collateral losses of the client is excluded.

## 9. Copyright

All information and functions that can be accessed via the App are fully and exclusively the property of the Bank (in particular copyrights, trademarks, design rights, and other rights) unless otherwise specified. The Bank grants the client a non-exclusive, non-transferable, free-of-charge licence to download, install, and use the App within the scope of the information and functions. Any

publication in whole or in part, modification, linking, use, transmission, copying in whole or even in part of the App or of the information, functions, and logos is prohibited without prior written consent of the Bank.

## 10. Costs

The App and the information provided are free of charge. The User may, however, incur costs for data transfer. The Bank recommends that the User clarify this question with the User's internet or mobile network provider.

## 11. Changes and amendments

The Bank reserves the right to change these Terms of Use, the App, and the contents of the App or to discontinue the App. Changes are communicated to the User in an appropriate manner and shall be deemed approved within one month if no written objection is made.

## 12. Governing law and place of jurisdiction

Access to the App and these Terms of Use are subject exclusively to Liechtenstein law. If a legal relationship arises for the Bank due to use of the App, Liechtenstein law shall likewise be exclusively applicable. To the extent permitted by the law, the seat of the Bank is the regular place of jurisdiction and performance. However, the Bank is also entitled to take legal action against the User before any other competent court.