

# Terms and Conditions for Digital Banking

## 1. Digital Banking Services

1.1 The services offered by Bank Cler Ltd (hereinafter referred to as the "Bank") in Digital Banking (E-Banking, Mobile Banking and other services), the applicable terms and conditions and additional details are set out in product descriptions, service overviews and user manuals. These can be seen on the Bank's website and are also binding in addition to these Terms and Conditions for Digital Banking (hereinafter also referred to as "Terms and Conditions").

1.2 The data exchange provided for in these Terms and Conditions relates to banking business and also other legal transactions which, in general, are based on separate agreements or terms and conditions of business. Additional or special agreements or provisions can apply to individual digital services. In the event of contradictions in the area of application of the services requested by the customer, the following order of precedence applies:

- any special terms and conditions relating to the digital service in question
- these Terms and Conditions for Digital Banking
- agreements or terms and conditions of business as well as information and conditions relating to individual banking or other business or services set out elsewhere on the Bank's website
- general terms and conditions of business

In so far as special provisions and conditions exist for specific digital services that have to be accepted by the customer and/or users other than the customer (on this point see Clause 2.1), these may be communicated in electronic form by the Bank. The customer or, depending on the service, a user other than the customer, decides whether they wish to use the relevant service by electronically agreeing to the relevant provisions/conditions. Any conditions accepted by a user other than the customer are also binding on the customer. The Bank reserves the right to include new and/or supplementary provisions and conditions in existing agreements in other forms.

1.3 By using the "E-Documents" service or a similarly designated service (hereinafter referred to as "E-Documents"), the customer authorises the Bank to send correspondence relating to the corresponding accounts/custody accounts or any other banking products (particularly account and custody account statements, credit and debit advices, confirmations, interest, capital and other certificates, notifications of interest due, credit card statements as well as stock exchange trading and other statements,

notifications in connection with capital market events) to themselves and other users of Digital Banking in electronic form via Digital Banking and to make such correspondence available in Digital Banking. This applies to all products and services, i.e. also to such products and services in the context of the relevant banking relationship which are not accessible via Digital Banking.

The Bank is entitled to make documents as described above available electronically even in the absence of instructions from the customer. Existing instructions on custody or delivery by post will be replaced when the customer opts for the E-Documents service. The Bank reserves the right to restrict the availability of delivery of correspondence by post for certain accounts, custody accounts or other products. Customers will be informed of such changes in a suitable manner.

Even if the customer has opted for the E-Documents service, the Bank reserves the right to continue to send certain documents exclusively or additionally by post, particularly by reason of legal or regulatory requirements or, if in the Bank's judgement, this is shown to safeguard the Bank's interest.

Documents sent by electronic means in accordance with the customer's instructions have the same legal effect as documents sent by post. Users must check documents sent in this form for completeness and accuracy. A document is deemed to have been duly received by the customer at the time the document can be accessed in Digital Banking. The customer is responsible for taking note of the documents addressed to them or intended for them in good time. The customer acknowledges that after the maximum available memory capacity has been reached or after the end of a certain period of time, the Bank is entitled to delete notifications, whether opened or unopened, that the Bank has sent to users. Mail boxes forming part of Digital Banking are therefore not intended to enable customers to comply with any of their statutory retention obligations.

1.4 As part of the digital services, users have the possibility of receiving information on certain events by means of electronic communications (e.g. texts/SMS, email, etc.). By using such services, customers acknowledge that the notifications are made via unencrypted communication channels. See also Clause 8 "Security in Digital Banking/banking secrecy" on this point.

## 2. Access to Digital Banking

2.1 Access to Digital Banking is granted to users who authenticate themselves by inputting the means of identification as part of the selected user login process valid for these services. A user is deemed to be a person authorised by the customer (also referred to as "contractual partner" in contract documents) in the agreement for Digital Banking or in the framework of another agreement, e.g. a basic contract, for the use of Digital Banking (i.e. the customer themselves or a third party). The Bank reserves the right to restrict access to Digital Banking or to specific ranges of functions or functionalities to such users, other than the customer, who hold a bank power of attorney granted by virtue of signature documentation of the Bank. In so far as the customer is also a user, they are included in these conditions as a matter of principle even if mention is only made of a user or users. In so far as the customer is addressed specifically as the Bank's contractual partner (account holder, custody account holder and, if applicable, in different relationships) in these Terms and Conditions, the term "customer" is normally used.

2.2 The following are required as means of identification for the use of Digital Banking:

- a) the identification number sent to the user by the Bank
- and
- b) the user's personal password which the user may select
- and
- c) an additional means of identification provided by or accepted by the Bank (two-factor authentication)

The individual login processes and means of identification made available by the Bank are described on the Bank's website and in specific product or other documentation, as applicable. They can be amended or replaced in line with the state of the art as it changes over time, or for other reasons, or by new processes. Customers affected by such changes will be informed in an appropriate manner.

2.3 Any person who identifies themselves as described in Clause 2.2 is deemed by the Bank to be entitled to use Digital Banking. Thus within the scope and to the extent of the services and methods of availability selected by the customer in the "Agreement for Digital Banking" or in another authoritative agreement e.g. a basic contract, and irrespective of that person's legal relationship to the customer – if that person is not identical with the customer – and regardless of entries in the Commercial Register to the contrary, publications or rules in signature

documents, and without further examination of that person's authorisation and irrespective of the Bank's legal relationship to the customer, the latter may allow such persons to make enquiries, issue instructions, obtain documents electronically and use other functionalities in Digital Banking. The Bank is also authorised to take receipt of legally binding notifications and orders from them and to execute such orders. The Bank can withhold the use of specific functionalities e.g. for the issue of declarations of intent in legal matters which, by reason of legal or other provisions or in accordance with the Bank's rules, must originate from the customer or certain proxies or signatories, from the customer themselves and specific users.

2.4 The Bank has the right at any time and without stating reasons to refuse the provision of Digital Banking services and to require that the user prove their identity in another form (e.g. by signature or personal appearance).

2.5 The customer accepts without reservation all transactions posted in Digital Banking by themselves or another user or a third party, as the case may be, using their means of identification. Likewise, all instructions, orders, notifications and declarations of intent which reach the Bank by Digital Banking or are issued to the Bank in text form in the course of the use of functionalities specially provided for this purpose or by the selection of electronic buttons or comparable items are deemed to be given, composed or issued and authorised by the customer and electronically provided documents as lawfully retrieved from a user.

2.6 Unless expressly agreed otherwise, the purpose of communication channels (notifications) provided within the scope of Digital Banking is not the transmission of time-critical messages by the user or messages subject to a deadline. Payment or stock exchange orders and other orders relating to securities transactions, revocations of orders or powers of attorney, the blocking of credit cards and similar procedures may, depending on the transaction and the underlying agreement, only be communicated by users via the communication channels provided and agreed for this purpose either as part of or outside Digital Banking. The Bank is entitled to delete notifications, whether opened or unopened, sent to users after the maximum available memory capacity has been reached or within a certain period of time. Mail boxes forming part of Digital Banking are therefore not intended to enable customers to comply with any of their statutory retention obligations. (see also Clause 1.3).

### 3. The user's duties of care

- 3.1 All users undertake to change the initial password assigned by the Bank immediately after receipt and to change it regularly thereafter. Passwords should not consist of easily determined combinations (such as telephone numbers, dates of birth, car registration numbers, etc.).
- 3.2 Activation and/or verification codes for Digital Banking services supplied to users must be put into effect by users immediately and according to the instructions provided.
- 3.3 All users must ensure that all means of identification are kept secret and are protected against improper use by unauthorised persons. In particular, passwords must not be recorded or stored without protection on a terminal (such as a desktop computer, laptop, tablet or mobile telephone) or recorded elsewhere. Likewise, the means of identification must not be disclosed or otherwise made available to third parties. The Bank will never use email to request the user to enter their means of identification for Digital Banking in any data entry mask or to send it in any way to the Bank or to any other recipient. In order to reduce the security risk of manipulation by unauthorised third parties, when logging in via a web browser the user must ensure that the Internet address of Bank Cler Ltd is entered manually in the address bar and that the Bank's website is not accessed via links in search engines.
- 3.4 If there is cause for suspicion that unauthorised third parties have gained knowledge of one or more means of identification of a user, the user must change the relevant means of identification immediately. If this is not possible, the user must immediately request that access to the relevant services be blocked, or block access to the services themselves by taking the steps described on the Bank's relevant web pages or by proceeding in accordance with Clause 6.1 of these Terms and Conditions.
- 3.5 If there is cause for suspicion that unauthorised third parties have gained access to a user's terminal (e.g. in the event of loss or theft of the terminal), the user must contact the Bank by telephone without delay during the support times published on the Bank's web pages.
- 3.6 Users are responsible for the data collected about them and must therefore check all the data they enter for completeness and accuracy. Responsibility concerning data communicated by the user to the Bank remains with the user until this information is accepted for further processing by the Bank's

system. The customer is responsible for the consequences that can arise from erroneous entries.

### 4. Risks and liability

- 4.1 Should loss or other detriment occur, without the Bank or a user breaching its or their duty of care, the party (the Bank or the customer) in whose sphere of influence the cause of the loss or the act causing the loss lies, shall be liable as a matter of principle. In particular, the customer bears the risks which arise from the misuse of a user's means of identification as well as from technical malfunctions or manipulation of the hardware and/or software of a user and also from breaches of the duties of care by users or from interference by unauthorised third parties in the public and private data transmission networks.

In so far as the Bank is liable for the performance of services with its customary care, it is in principle only liable for the customer's direct and immediate losses. Liability for the customer's indirect losses is excluded.

- 4.2 The Bank accepts no guarantee for the accuracy and completeness of data displayed by the Bank in Digital Banking. In particular, information on bank accounts and custody accounts (balances, statements, transactions, etc.) as well as publicly accessible information such as stock-exchange prices and currency rates, are deemed to be unconfirmed and non-binding. Except for such information as is designated as binding, the information in the Bank's statements and documents sent to the customer and/or third parties nominated by the customer in paper or electronic form in accordance with the delivery instructions issued by the customer is authoritative. Data displayed in Digital Banking only constitutes binding offers if the data is expressly indicated as such.
- 4.3 The Bank does not arrange technical access to its services. This is the sole responsibility of the user. The customer particularly acknowledges that the Bank does not distribute the special software necessary for Internet access and for the use of Digital Banking, nor does the Bank support the user in respect of software or hardware problems unless corresponding support services have been expressly agreed. Consequently, the Bank accepts no guarantee for either network operators (providers) or for any necessary software.
- 4.4 Data communication is conducted over public telecommunications networks that are not specially protected (telephone, Internet, etc.). The Bank accepts no liability for losses arising from the use of

these networks. In particular, the Bank accepts no liability for losses incurred by the customer as a consequence of communication faults, technical defects, interruptions in the telephone network or the Internet, unlawful tampering with network installations, overloading in the networks, wilful blocking of electronic access by third parties, interruptions or other deficiencies on the part of the network operator.

- 4.5 In spite of all security measures, the Bank cannot accept any liability for users' terminals as this is not possible from a technical standpoint (see Clause 8 on security/ banking secrecy).
- 4.6 The Bank expressly excludes liability for software that may be recommended or supplied by the Bank as well as the consequences arising from its use or during the transfer of the software via the Internet.
- 4.7 When exercising its customary degree of care, the Bank accepts no liability for the consequences of faults and interruptions, in particular in the processing during the operation of Digital Banking services (e.g. caused by unlawful interference with its computer systems or those of third parties engaged by the Bank).
- 4.8 If security risks are detected, the Bank reserves the right at any time to disconnect access to Digital banking for the protection of users until such risks are averted. The Bank accepts no liability for any losses arising from such an interruption.
- 4.9 The Bank accepts no liability for orders and/or settlement instructions and losses (particularly losses caused by exchange rate movements) that are not executed on time provided that the Bank has exercised its customary degree of care.

## 5. Execution of orders and instructions

- 5.1 Stock exchange and payment orders may in principle be submitted at any time. However, such orders are not processed around the clock, nor are they processed immediately after their submission. Amongst other factors, processing depends on trading days and times of the relevant stock exchange and also on the working and processing times of processing departments and organisations.
- 5.2 Transactions can only be released when the Bank has received all transaction confirmations that it has required.

## 6. Blocking

- 6.1 Users can arrange for access to the services in Digital Banking to be blocked. Blocking can only be requested during the times stipulated in the Bank's website. The Bank can require additional confirmation of the block in writing. The user can also block access to the services in Digital Banking themselves at any time by entering an incorrect means of identification incorrectly enough times until the block is displayed. However, the Bank reserves the right to execute payment and securities orders pending at the time of the block.
- 6.2 The Bank can require that the customer provide a written request for the removal of a block instigated by a user.
- 6.3 The Bank is entitled to block access by users to individual or all Digital Banking services at any time without stating reasons and without prior termination of the corresponding agreement if this, in its own judgement, appears to be appropriate for objective reasons.

## 7. Provisions on power of attorney

Powers of attorney granted under the Bank's regulations governing signatures do not automatically authorise the use of Digital Banking services. Their use requires the issue of corresponding access, enquiry or other rights by the customer by means of a separate agreement. The Bank can make the use of all or specific services dependent in whole or in part on the existence of a Bank power of attorney granted under the Bank's regulations governing signatures or withhold the services from the customer themselves (see also Clause 2.1).

The entitlement of a user to use the Digital Banking services is valid until the customer issues a written cancellation to the Bank.

The deletion or amendment of the power of attorney or the signature rights of a user in accordance with a signature documentation lodged with the Bank, but not the deletion or amendment of a users' signature right in the Commercial Register, results in the revocation of all the rights granted to this person within the framework of Digital Banking. Simple enquiry rights remain unaffected thereby.

Authorisation to use Digital Banking services does not automatically lapse in the event of death and possible loss of legal capacity or bankruptcy of the customer, or of a user other than the customer.

## 8. Security in Digital Banking/banking secrecy

8.1 The customer acknowledges that the data used in Digital Banking services is transmitted via an open network which is accessible to everyone i.e. the Internet. The data is therefore transmitted by regular means and without controls across borders. This also applies to data transmission if the sender and recipient are located in Switzerland. Although the individual data packages are transmitted in an encrypted form, the sender and the recipient on the other hand remain unencrypted in each case. These can also be read by third parties. A third party may then be able to infer the existence of a banking relationship. By downloading, installing and using apps on terminals, points of contact can be created to third parties such as the operators of the app in question. It may therefore be possible to draw a conclusion on the existence of a customer relationship.

8.2 Special importance was attached to security during the development of Digital Banking and its ongoing enhancement, particularly by the use of a multi-step security system which, among other things, makes use of cryptographic procedures of a very high technical standard. In principle, because of the encryption, it is not possible for any unauthorised person to view confidential customer data. However, absolute security cannot be guaranteed either by the Bank or by the user, even with security precautions meeting the highest, most technically advanced standards. The customer acknowledges in particular that their terminal constitutes the weak link when accessing Digital Banking. Regular updates to the software (e.g. the operating system) of the terminals as well as security precautions such as the installation and regular updating of an antivirus program in particular are the responsibility of the user.

8.3 The customer acknowledges in particular the following specific risks:

- Insufficient knowledge of the system and the absence of system precautions may facilitate unauthorised access (for example, inadequate protection of data stored on storage media, file transfers and screen radiation, etc.). It is incumbent on the customer to obtain information in detail about the necessary security precautions and to place the users other than the customer under an obligation of compliance with the precautions.
- It is impossible to exclude the creation of a user profile by the user's Internet provider; this means that the relevant providers have the means of tracing when and with whom users are in contact.

- There is the constant risk that a third party may gain unnoticed access to the Client's terminal during Internet use (e.g. through a Java or ActiveX application).
- There is also the constant risk that when using the Internet, malware (such as computer viruses) will spread on a user's terminal if the terminal is in contact with other systems, be it via computer networks or other data carriers.
- It is expected that users will work only with software procured from a trustworthy source.
- Modifications to the operating system of the user's terminal (e.g. jail breaking, rooting) may facilitate unauthorised access.

## 9. Import and export restrictions

The customer acknowledges that by using Digital Banking from outside Switzerland they might, under certain circumstances, infringe the provisions of foreign law. It is the customer's responsibility to seek information on this point and to inform users other than the customer about this matter. The Bank accepts no liability in this respect. The customer acknowledges that there may be import and export restrictions regarding encryption algorithms, which, if applicable, may be infringed when using Digital Banking services in or from a country other than Switzerland. The customer is responsible for informing users other than themselves about this matter.

## 10. Customer/user data and marketing

Attention is drawn to the Bank's General Terms and Conditions of Business and Privacy Statement. These can be viewed on the Bank's website at [www.cler.ch/datenschutzerklaerung](http://www.cler.ch/datenschutzerklaerung).

## 11. Termination of the Agreement

Agreements for Digital Banking (including agreements concluded with a different designation) can be terminated in writing at any time by the customer and the Bank. Unless instructed to the contrary by a user, the Bank is entitled but not obliged to execute orders pending at the time of the termination. The Bank is entitled at its own discretion to cancel existing agreements for Digital Banking and thus access to Digital Banking services without prior notice or subsequent notification to the customer, if there has been no access made within one year from the conclusion of the agreement or Digital Banking has not been used for more than one year.

## 12. Reservation of particular statutory provisions

Any statutory or other provisions governing the operation and use of the Internet remain reserved and apply from the point in time when they come into force.

### 13. General terms and conditions of business

The Bank's General Terms and Conditions of Business also apply to the use of Digital Banking services (see also Clause 1.2).

### 14. Partial invalidity

The invalidity, illegality or unenforceability of one or more provisions of these Terms and Conditions do not affect the validity of the remaining parts of the agreement.

### 15. Amendment of the Terms and Conditions for Digital Banking and the services offered

The Bank may amend these Terms and Conditions at any time and/or restrict or extend the range of services offered in the area of digital services. It will notify the customer of such changes by an electronic display or notification within the framework of Digital Banking or in any other suitable way. Amendments will be deemed to be approved if the customer fails to object to the amendments to the Terms and Conditions and/or services within a period of one month following notification. The explicit acceptance of corresponding amendments by electronic or other means remains reserved if such amendments are presented correspondingly by the Bank, as well as amendments to the range of services without prior notification if such notification is impossible for objective reasons.

### 16. Mobile Banking

16.1 Mobile Banking enables Digital Banking to be used with a smartphone or another suitable mobile terminal via a corresponding app. The available functionalities correspond in principle with those of E-Banking.

16.2 The minimum technical requirements for the use of Mobile Banking are set out in corresponding product descriptions and service overviews that can be seen on or downloaded from the Bank's website; these descriptions and overviews are regularly updated.

Version April 2023